ALJABAR

Suatu Pondasi Matematika

SUBIONO

2022

ALJABAR
Suatu Pondasi Matematika

Penulis:
Subiono

itspress

ALJABAR
Suatu Pondasi Matematika

Penulis : Subiono
Email : subiono2008@matematika.its.ac.id
Alamat : Departemen Matematika
Institut Teknologi Sepuluh Nopember
Sukolilo Surabaya, 60111
Indonesia

429 halaman; 30 cm

ISBN 978-623-318-091-7

Diterbitkan pertama kali oleh
ITS Press, Surabaya 2022
Anggota IKAPI dan APPTI

Dicetak oleh Percetakan ITS Press
Isi di luar tanggung jawab percetakan

Copyright

Kata Pengantar

AlhamdulIllahiRabbilalamin, segala puji hanyalah milikMu ya Allah yang telah memberikan "kebebasan bertanggung jawab" kepada manusia semasa hidupnya untuk suatu kebaikan dalam melaksanakan amanatMu di hamparan bumi yang dihuni beragam manusia. Sholawat dan Salam kepadaMu ya Nabi Muhammad beserta para keluarganya dan para pengikutnya sampai nanti di hari akhir.

Buku ini disusun dengan maksud untuk membantu dan mempermudah mahasiswa dalam mempelajari materi kuliah Aljabar. Isi bahasan dimulai dengan pendahuluan membahas dasar-dasar teori yang digunakan pada hampir seluruhan bahasan berikutnya. Selanjutnya bahasan dibagi dua : yaitu bagian pertama mengenai teori grup yang merupakan bahan materi kuliah Aljabar I dan Kapita Selekta I bidang Aljabar. Bagian kedua adalah Ring dan Lapangan yang merupakan materi kuliah Aljabar II dan Kapita Selekta II bidang Aljabar. Oleh karenanya tidak berlebihan bahwa, selain dari apa yang telah disebutkan, penyusunan buku ini juga dimaksudkan untuk menambah suatu bahan bacaan khususnya bagi para peminat Aljabar.

Dalam buku ini diberikan beberapa konsep pengertian dan sifat dari materi yang disajikan didahului contoh-contoh untuk mempermudah pemahaman pengertian dan sifat yang dibahas. Selain itu juga diberikan beberapa contoh aplikasi yang mungkin.

Topik bahasan disajikan dengan penekanan pada "matematika" tetapi tidaklah menjadikan para pemakai lain akan mengalami kesulitan dalam mempelajari buku ini, karena peletakan penekanan aspek matematika dibuat dengan porsi yang seimbang. Sehingga para peminat matematika tetap dapat menikmati dan menggunakan ilmunya terutama dalam Aljabar, begitu juga untuk para pemakai yang lainnya diharapkan mendapat tambahan wawasan untuk melihat matematika sebagai alat yang dibutuhkan terutama dalam kajian Aljabar untuk menyelesaikan masalah-masalah praktis yang dihadapinya.

Persiapan penulisan materi buku ini membutuhkan waktu yang agak lama, sejak penulis mengajarkan mata kuliah "Aljabar I", "Aljabar II" dan "Kapsel Aljabar" di Departemen Matematika FSAD-ITS, Surabaya. Beberapa materi disusun dari pengalaman mengajar tersebut. Selain itu juga dari kumpulan makalah penulis dan hasil-hasil dari pembimbingan skripsi dan tesis mahasiswa.

Penulis pada kesempatan ini menyampaikan keaktifan para pembaca dalam mengkaji buku ini untuk menyampaikan kritik dan saran guna perbaikan buku ini, sehingga pada versi yang mendatang "mutu buku" yang baik bisa dicapai. Kritik dan saran ini sangat penting karena selain alasan yang telah disebutkan tadi, penulis percaya bahwa dalam sajian buku ini masih kurang dari sempurnah bahkan mungkin ada suatu kesalahan dalam sajian

buku ini baik dalam bentuk redaksional, pengetikan dan materi yang menyebabkan menjadi suatu bacaan kurang begitu bagus.

Akhirnya, dengan segala kerendahan hati penulis memohon hanya kepadaMu ya Allah semoga penulisan ini bisa berlanjut untuk versi mendatang yang tentunya lebih "baik" dari Edisi yang tersedia saat ini dan semoga benar-benar buku yang tersaji ini bermanfaat bagi pembaca.

Surabaya, 1 Pebruari 2022

Penulis

Daftar Isi

Bab 1

Pendahuluan

Dalam bab pendahuluan ini dibahas beberapa gagasan matematika mendasar yang digunakan dalam bab-bab berikutnya. Pembahasan dimulai dari pengertian himpunan dan fungsi. Fungsi (pemetaan) satu-satu (injektif), pemetaan pada (surjektif) dan komposisi fungsi. Kesemuanya adalah konsep-konsep dasar yang sering muncul dan muncul kembali, sering dalam bentuk yang berbeda. Relasi ekivalen pada himpunan dan partisi juga sering digunakan, terutama dalam membangun struktur aljabar baru dari yang lama. Himpunan bilangan bulat dengan operasi penjumlahan dan perkalian biasa dan berbagai sifat utamanya berulang kali memberikan uraian yang mendasar dan konstruksi model untuk konsep aljabar umum. Sehubungan dengan bilangan bulat, induksi matematika adalah metode yang sangat berguna dan menjadi nyaman untuk suatu pembuktian yang penting. Dengan berlatar belakang pengetahuan ini perhitungan untuk menentukan koefisien binomial dan algoritma untuk mendapatkan pembagi persekutuan terbesar akan lebih mudah dilakukan. Himpunan bilangan kompleks dengan operasi sebagaimana biasa dilakukan juga memainkan peran penting. Matriks juga memberikan sejumlah contoh untuk menggambarkan gagasan aljabar baru, dan pengetahuan tentang sifat-sifatnya yang paling dasar akan berguna.

1.1 Himpunan dan Fungsi

Pada bagian ini dikenalkan notasi dasar untuk himpunan dan operasi pada himpunan, juga simbol-simbol untuk beberapa himpunan tertentu yang sangat penting. Selain itu dikenalkan terminologi untuk berbagai jenis pemetaan antara himpunan dan gagasan kardinalitas dari himpunan.

Himpunan mungkin sesuatu dari matematika yang paling fundamental. Secara intuisi, dapat dipikirkan bahwa suatu himpunan adalah sebagai kumpulan dari berbagai hal, dimana kumpulan ini dipandang sebagai suatu entitas tunggal. Himpunan dapat memuat bilangan, titik dalam bidang-xy, fungsi dan lain sebagainya, bahkan himpunan yang lain. Himpunan biasanya dinotasikan oleh huruf besar A, B, C atau huruf kaligrafis $\mathcal{F}, \mathcal{S}, \mathcal{T}$.

Definisi 1.1.1 Bila A adalah suatu himpunan dan x adalah suatu entitas di A ditulis $x \in A$. Dalam hal ini dikatakan bahwa x adalah suatu **elemen** dari A. Notasi $x \notin A$ menyatakan x bukan elemen A. ✓

Ada beberapa cara menyajikan himpunan.

1. Mendaftar elemen-elemen himpunan bila hanya sedikit banyaknya elemen dari himpunan. Atau, mendaftar sebagaian dari elemen-elemen dari himpunan dan berharap pembaca dapat petunjuk dari pola elemen yang telah didaftar. Misalnya, contoh-contoh berikut.

   (a) $\{1, 8, \pi, \text{Rabu}\}$

   (b) $\{0, 1, 2, \ldots, 40\}$

   (c) $\{\ldots, -6, -4, -2, 0, 4, 6, \ldots\}$.

2. Menjelaskan kriteria bagi entitas yang termuat dalam himpunan.

   (a) $\{x \mid x$ adalah bilangan riil dan $x > -2\}$

   (b) $\{a/b \mid a, b$ adalah bilangan bulat dan $b \neq 0\}$

   (c) $\{x \mid P(x)\}$.

Contoh 1.1.1 Beberapa himpunan yang sangat penting dalam aljabar yang memiliki nama dan simbol khusus adalah sebagai berikut:
Himpunan kosong, himpunan tanpa elemen.

$$\varnothing = \{\,\}.$$

Himpunan semua bilangan bulat

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}.$$

Himpunan semua bilangan rasional

$$\mathbb{Q} = \left\{ \frac{p}{q} \,\middle|\, p, q \in \mathbb{Z}, q \neq 0 \right\}.$$

Himpunan semua bilangan riil

$$\mathbb{R} = \{x \mid x \text{ adalah bilangan riil}\}.$$

Himpunan semua bilangan kompleks

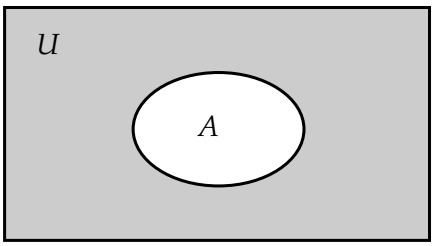
$$\mathbb{C} = \left\{ x + yi \mid x, y \in \mathbb{R}, i = \sqrt{-1} \right\}. \bullet$$

Contoh 1.1.2 Himpunan-himpunan lain yang mempunyai nama dan simbol khusus adalah:
Himpunan bilangan bulat genap (kelipatan dua)

$$2\mathbb{Z} = \{2n \mid n \in \mathbb{Z}\}.$$

Himpunan bilangan riil positip

$$\mathbb{R}^+ = \{x \in \mathbb{R} \mid x > 0\}. \bullet$$



Gambar 1.1: Diagram Venn A^C

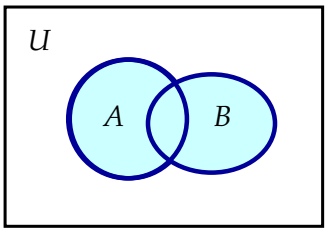
Definisi 1.1.2 Diberikan himpunan A, notasi himpunan A^C adalah **komplemen dari** A didefinisikan sebagai himpunan dari semua elemen-elemen di himpunan universal U yang tidak di A, yaitu

$$A^C = \{x \,|\, x \in U \text{ dan } x \notin A\}.$$

Secara diagram Venn himpunan A^C diberikan oleh Gambar 1.1. Diberikan dua himpunan A dan B, A adalah **himpunan bagian** (subset) dari B ditulis $A \subseteq B$ bila setiap elemen dari A adalah suatu elemen di B. Dua himpunan sama $A = B$, bila dan hanya bila $A \subseteq B$ dan $B \subseteq A$. **Gabungan** (union) dari A dan B adalah himpunan

$$A \cup B = \{x \,|\, x \in A \text{ atau } x \in B\}.$$

Digram Venn himpunan $A \cup B$ diberikan oleh Gambar 1.2. **Irisan** (intersection) dari A dan B



Gambar 1.2: Diagram Venn $A \cup B$

adalah himpunan

$$A \cap B = \{x \,|\, x \in A \text{ dan } x \in B\}.$$

Digram Venn himpunan $A \cap B$ diberikan oleh Gambar 1.3. Himpunan A **dikurangi** B adalah himpunan yang didefinisikan oleh

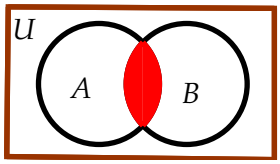
$$A - B = A \cap B^C = \{x \,|\, x \in A \;\text{ dan }\; x \notin B\}.$$

Digram Venn himpunan $A - B$ diberikan oleh Gambar 1.4. Sedangkan himpunan **beda simetrik** dari A dan B didefinisikan oleh

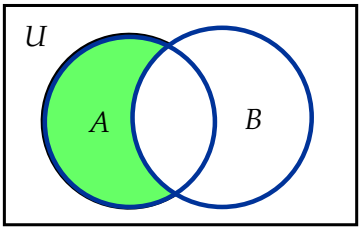
$$A \triangle B = (A \cap B^C) \cup (A^C \cap B) = \left\{x \,|\, x \in A \cap B^C \text{ atau } x \in A^C \cap B\right\}.$$

Digram Venn himpunan $A \triangle B$ diberikan oleh Gambar 1.5. **Produk Kartesian** dari A dan B adalah himpunan

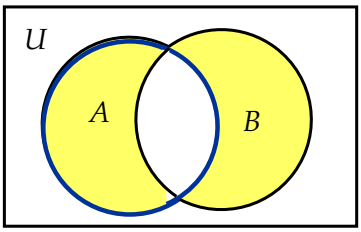
$$A \times B = \{(a, b) \,|\, a \in A, b \in B\}$$



Gambar 1.3: Diagram Venn $A \cap B$



Gambar 1.4: Digram Venn $A - B$



Gambar 1.5: Diagram Venn $A \triangle B$

yang juga dinamakan himpunan semua pasangan terurut dengan komponen pertama elemen di A dan komponen kedua elemen di B. Bila $A = B$, ditulis A^2 atau $A \times A$. Secara umum bila n adalah suatu bilangan bulat positip, maka n-pasangan terurut ditulis $(a_1, a_2, \ldots, a_n)$ mempunyai elemen pertama a_1, elemen kedua a_2,..., dan elemen ke-n a_n. Jadi

$$(a_1, a_2, \ldots, a_n) = (b_1, b_2, \ldots, b_n)$$

bila dan hanya bila $a_i = b_i, i = 1, 2, \ldots, n$. Hasil kali dari $A_1, A_2, \ldots, A_n$ adalah

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) | a_i \in A_i, i = 1, 2, \ldots, n\}$$

dan $A^n = A_1 \times A_2 \times \cdots \times A_n$ untuk $A_i = A$, $i = 1, 2, \ldots, n$. Banyaknya elemen dari A dinamakan **kardinalitas** dari A dan ditulis sebagai $|A|$. Walaupun notasi yang diberikan sama dengan notasi harga mutlak tetapi mempunyai arti yang berbeda. Misalnya $|-5| = 5 = |5|$, tetapi $|\{-5\}| = 1$. Bila himpunan A berhingga, maka kardinalitas dari himpunan A adalah suatu bilangan bulat taknegatif. ✓

Contoh 1.1.3 Bila himpunan bilangan riil dipandang sebagai himpunan universal, maka

$$\mathbb{Q}^C = \{x \mid x \in \mathbb{R} \text{ dan } x \notin \mathbb{Q}\}$$

adalah himpunan dari semua bilangan irrasional. ●

Proposisi 1.1.1 Diberikan himpunan A dan B berhingga, maka

1. $|A \cup B| = |A| + |B| - |A \cap B|$
2. $|A \times B| = |A| \cdot |B|$

Bukti

1. Karena $A \cup B = (A \triangle B) \cup (A \cap B)$, maka

$$\begin{aligned} |A \cup B| &= |A \triangle B| + |A \cap B| \\ &= (|A| - |A \cap B|) + (|B| - |A \cap B|) + |A \cap B| \\ &= |A| + |B| - |A \cap B| \end{aligned}$$

2. Misalkan $B = \{1, 2, \ldots, n\}$, didapat

$$A \times B = (A \times \{1\}) \cup (A \times \{2\}) \cup \cdots \cup (A \times \{n\}).$$

Terlihat bahwa $(A \times \{i\}) \cap (A \times \{j\}) = \emptyset, \forall i \neq j$. Jadi

$$\begin{aligned} |A \times B| &= |A \times \{1\}| + |A \times \{2\}| + \ldots + |A \times \{n\}| \\ &= \underbrace{|A| + |A| + \ldots + |A|}_{n} = |A| \cdot n. \end{aligned}$$

Terlihat bahwa $|A \times B| = |A| \cdot |B|$. ✓●

Contoh 1.1.4 Diberikan dua himpunan $\{1, 2\}$ dan $\{1, 2, 3\}$, didapat

$$\{1, 2\} \times \{1, 2, 3\} = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}$$

dan

$$\{1, 2, 3\} \times \{1, 2\} = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 1), (3, 2)\}.$$

Terlihat

$$\{1, 2\} \times \{1, 2, 3\} \neq \{1, 2, 3\} \times \{1, 2\}$$

sebab $(1, 3) \in \{1, 2\} \times \{1, 2, 3\}$, tetapi $(1, 3) \notin \{1, 2, 3\} \times \{1, 2\}$ dan

$$|\{1, 2\} \times \{1, 2, 3\}| = 2.3 = 6 = 3.2 = |\{1, 2, 3\} \times \{1, 2\}|. \quad ●$$

Contoh 1.1.5 Diberikan himpunan berikut

$$\begin{aligned} \{1, 2\} \times \{2, 3\} \times \{4, 5\} = \{&(1, 2, 4), (1, 2, 5), (1, 3, 4), (1, 3, 5), \\ &(2, 2, 4), (2, 2, 5)(2, 3, 4), (2, 3, 5)\} \end{aligned}.$$

Didapat $|\{1, 2\} \times \{2, 3\} \times \{4, 5\}| = 2 \cdot 2 \cdot 2 = 8$. ●

Contoh 1.1.6 Diberikan $\mathbb{P}$ adalah himpunan bilangan bulat positif dan

$$A = \{(a, b) \in \mathbb{P}^2 \,|\, a < b\}.$$

Bila $(x, y) \in A$ berakibat bahwa $x < y$ dan bila $(y, z) \in A$ berakibat bahwa $y < z$. Hal ini menunjukkan bahwa $x < y$ dan $y < z$, akibatnya $x < z$. Jadi $(x, z) \in A$.

Definisi 1.1.3 Suatu relasi diantara himpunan A dan B adalah suatu subset $\mathcal{R}$ dari $A \times B$. Dalam hal ini $(a, b) \in \mathcal{R}$ dibaca sebagai a berelasi dengan b dan ditulis sebagai $a\mathcal{R}b$.

Contoh 1.1.7 Relasi sama dengan: Diberikan himpunan A dan didefinisikan

$$\mathcal{R} = \{(a, a) \,|\, a \in A\} \subset A \times A.$$

Jadi $a_1\mathcal{R}a_2$ berarti bahwa $a_1 = a_2$. Misalkan T himpunan titik dan G himpunan garis dibidang. Didefinisikan $t\mathcal{R}g$ bila titik t terletak pada garis g. Suatu relasi $\mathcal{R}$ pada himpunan bilangan bulat $\mathbb{Z}$ didefinisikan oleh $m\mathcal{R}n$ bila $m - n$ adalah bilangan bulat genap. Bila A himpunan berhingga, maka banyaknya relasi pada A adalah $2^{|A|^2}$.

Contoh 1.1.8 Misalkan $X = \{a, b, c\}$. Himpunan $R = \{(a, b), (b, a), (a, c)\}$ adalah suatu relasi pada X.

Definisi 1.1.4 Diberikan dua himpunan A dan B, suatu **fungsi** atau **pemetan** dari A ke B adalah suatu aturan yang memasangkan setiap elemen di A dengan tepat hanya satu (tunggal) elemen di B. Dalam hal ini ditulis $\phi : A \to B$ untuk menunjukkan bahwa ϕ adalah suatu fungsi dari A ke B. Suatu pemetaan harus terdefinisi dengan baik, ini berarti bahwa bila ϕ terspesifikasi oleh suatu aturan yang memasangkan setiap elemen dari A dengan suatu elemen di B, aturan harus bermakna hanya tepat satu (tunggal) elemen di B. Bila $\phi : A \to B$ adalah suatu pemetaan dari A ke B, maka pasangan dari elemen $a \in A$ dengan elemen di B ditulis sebagai $\phi(a) = b$ dinamakan **image** dari a terhadap ϕ. Untuk himpunan bagian A' dari A, ditulis

$$\phi(A') = \{\phi(a) \,|\, a \in A'\}$$

yang dinamakan **image/range** dari A' terhadap ϕ. Berkaitan dengan apa yang telah dibahas, himpunan A dinamakan **domain** dari ϕ, ditulis $\mathrm{Dom}(\phi) = A$ sedangkan himpunan B dinamakan **kodomain** dari ϕ

Image atau **range** dari ϕ adalah himpunan semua nilai-nilai $\phi(a)$ ditulis $\mathrm{Im}(\phi) = \{f(a) \,|\, a \in A\}$. Notasi $\phi(A)$ juga sering digunakan untuk menyatakan $\mathrm{Im}(\phi)$, jadi $\phi(A) = \mathrm{Im}(\phi)$. Himpunan $\mathrm{Im}(\phi)$ adalah subset dari B.

Contoh 1.1.9 Pemetaan $\phi : \mathbb{Z} \to \{0, 1\}$ didefinisikan oleh aturan

$$\phi(n) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{bila } n \text{ genap} \\ 1 & \text{bila } n \text{ ganjil} \end{cases}$$

adalah terdefinisi secara baik, tetapi pemetaan $\psi : \mathbb{Z} \to \{0, 1\}$ yang didefinisikan oleh aturan

$$\psi(n) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{bila } n \text{ genap} \\ 1 & \text{bila } n \text{ kelipatan3} \end{cases}$$

tidak terdefinisi secara baik, sebab $\psi(6) = \psi(2.\,3) = 0$ juga $\psi(6) = \psi(3.\,2) = 1$. Terlihat bahwa pasangan dari $6 \in \mathbb{Z}$ tidak tunggal di $\{0, 1\}$.

Contoh 1.1.10 Tunjukkan bahwa $f : \mathbb{R} - \{1\} \to \mathbb{R}$ yang didefinisikan oleh

$$f(x) = \frac{x^2+2}{x-1}, \ \forall x \in \mathbb{R} - \{1\}$$

adalah suatu fungsi.

Jawab
Pilih sebarang $x \in \mathbb{R} - \{1\}$, maka $x^2 + 2$ dan $x - 1$ keduanya adalah bilangan riil. Lagipula, karena $x \neq 1$, maka $x - 1$ tidak sama dengan nol. Jadi $(x-1)^{-1}$ ada sebagai bilangan riil. Dengan demikian $(x^2+2)/(x-1) \in \mathbb{R}$. Pilih $x_1, x_2 \in \mathbb{R} - \{1\}$ dan misalkan $x_1 = x_2$. Didapat

$$x_1^2 + 2 = x_2^2 + 2, \ \ x_1 - 1 = x_2 - 1 \ \text{ dan } \ (x_1-1)^{-1} = (x_2-1)^{-1}.$$

Jadi

$$\frac{x_1^2+2}{x_1-1} = \frac{x_2^2+2}{x_2-1},$$

dengan demikian $f(x_1) = f(x_2)$. Jadi f terdefinisi secara baik. ●

Pembahasan berkaitan dengan himpunan dan fungsi dapat dilakukan dalam SAGE dengan menggunakan perintah-perintah sebagai berikut.

```
# Membuat himpunan A dan B
A=Set([1,2])
B=Set([1,2,3])
print"A =",A;print"B =",B
```

```
A = {1, 2}
B = {1, 2, 3}
```

```
# Operasi himpunan

C=A.union(B);D=A.intersection(B)
print("C =",C,", adalah gabungan dari A dan B")
print("D =",D,", adalah irisan dari A dan B")
```

```
C = {1, 2, 3} , adalah gabungan dari A dan B
D = {1, 2} , adalah irisan dari A dan B
```

```
# Himpunan bagian

da=D.issubset(A)
```

```
db=D.issubset(B)
ab=A.issubset(B)
ba=B.issubset(A)
pretty_print(html("Apakah $D\\subset A$ ? $%s$"%latex(da)))
pretty_print(html("Apakah $D\\subset B$ ? $%s$"%latex(db)))
pretty_print(html("Apakah $A\\subset B$ ? $%s$"%latex(ab)))
pretty_print(html("Apakah $B\\subset A$ ? $%s$"%latex(ba)))
```

Apakah $D \subset A$? True
Apakah $D \subset B$? True
Apakah $A \subset B$? True
Apakah $B \subset A$? False

```
# A-B, B-A

A-B;B-A
pretty_print(html("$A-B=%s$"%latex(A-B)))
pretty_print(html("$B-A=%s$"%latex(B-A)))
```

$A - B = \{\}$
$B - A = \{3\}$

```
# Kardinalitas

carA=A.cardinality()
carB=B.cardinality()
pretty_print(html("$|A|=%s$"%latex(carA)))
pretty_print(html("$|B|=%s$"%latex(carB)))
```

$|A| = 2$
$|B| = 3$

```
# Membuat A x B dan B x A

AxB=Set([(a,b) for a in A for b in B])
BxA=Set([(b,a) for a in A for b in B])

pretty_print(html("$A\\times B=%s$"%latex(AxB)))
pretty_print(html("$B\\times A=%s$"%latex(BxA)))
```

$A \times B = \{(1,2),(1,3),(2,3),(2,2),(1,1),(2,1)\}$
$B \times A = \{(1,2),(3,2),(2,2),(3,1),(1,1),(2,1)\}$

```
# Cek apakah AxB = BxA

pretty_print(html("Apakah $A\\times B=B\\times A$? $%s$"%latex(AxB==BxA)))
```

Apakah $A \times B = B \times A$? False

```
# Cek apakah |C|=|A|+|B|-|D|

C.cardinality()==A.cardinality() + B.cardinality()
 - D.cardinality()
```

True

```
# Cek apakah |AxB|=|BxA| dan |AxB|=|A|.|B|

a=AxB.cardinality()==BxA.cardinality()
b=AxB.cardinality()==A.cardinality()*B.cardinality()
print("Apakah |AxB| = |BxA|?",a)
print("Apakah |AxB| = |A|.|B|?",b)
```

Apakah |AxB| = |BxA|? True
Apakah |AxB| = |A|.|B|? True

```
# Membuat himpunan P={1,2,3,4,5,6}

P=Set([1..6])
pretty_print(html("Himpunan $P=%s$"%latex(P)))
```

Himpunan $P = \{1, 2, 3, 4, 5, 6\}$

```
# Membuat AA subset PxP dengan (x,y) di AA bila x<y,
# AA adalah suatu relasi di P

PxP=Set([(x,y) for x in P for y in P])
AA=Set([(x,y) for (x,y) in PxP if x<y])

pretty_print(html("Himpunan $P\\times P=%s$"%latex(PxP)))
pretty_print(html("Himpunan $A=\\{(x,y)\\in P\\times P\\,
                        |\\,x<y\\}=%s$"%latex(AA)))
```

Himpunan $P = \{1, 2, 3, 4, 5, 6\}$

```
# Mendefinisikan fungsi phi : Z -> {0,1}
# phi(n)=0 bila n genap
# phi(n)=1 bila n ganjil

def phi(x):
if  mod(x,2)==0:
return 0
else:
return 1
phi(10);phi(-11)
```

```
0
1
```

Contoh 1.1.11 Misalkan pemetaan $\phi : \mathbb{Z} \to \mathbb{Z}$ diberikan oleh $\phi(n) = 2n$, $\forall n \in \mathbb{Z}$. Maka untuk setiap dua bilangan bulat m dan n, bila $\phi(m) = \phi(n)$ berakibat $m = n$.

Contoh 1.1.12 Bila pemetaan $\chi : \mathbb{Z} \to \mathbb{Z}$ yang diberikan oleh $\chi(n) = n^2$, $\forall n \in \mathbb{Z}$. Maka untuk setiap dua bilangan bulat m dan n, bila $\chi(m) = \chi(n)$ berakibat $m = \pm n$.

Definisi 1.1.5 Suatu pemetaan $\phi : A \to B$ dinamakan **satu-satu** bila $a_1 \neq a_2$ di A selalu berakibat $\phi(a_1) \neq \phi(a_2)$ atau ekivalen bila $\phi(a_1) = \phi(a_2)$ berakibat $a_1 = a_2$.

Contoh 1.1.11 adalah pemetaan satu-satu sedangkan Contoh 1.1.12 bukan.

Contoh 1.1.13 Misalkan pemetaan $\phi : \mathbb{Z} \to 2\mathbb{Z}$ diberikan oleh $\phi(n) = 2n$, $\forall n \in \mathbb{Z}$. Maka untuk sebarang $m \in 2\mathbb{Z}$ dan karena m genap, maka dapat dipilih $n = \frac{m}{2} \in \mathbb{Z}$ sehingga $\phi(n) = 2n = m$. Dalam hal ini $\phi(\mathbb{Z}) = 2\mathbb{Z}$.

Contoh 1.1.14 Misalkan pemetaan $\phi : \mathbb{R} \to \mathbb{R}^+$ diberikan oleh $\phi(x) = e^x$, $\forall x \in \mathbb{R}$. Maka untuk sebarang $y \in \mathbb{R}^+$ dan karena $y > 0$, maka dapat dipilih $x = \ln y \in \mathbb{R}$ sehingga $\phi(x) = e^x = e^{\ln y} = y$. Jadi dalam hal ini $\phi(\mathbb{R}) = \mathbb{R}^+$.

Definisi 1.1.6 Suatu pemetaan $\phi : A \to B$ dinamakan **pada** bila untuk setiap y di B ada suatu $x \in A$ sehingga $\phi(x) = y$. Dalam kasus ini $\phi(A) = B$. Bila pemetaan ϕ adalah satu dan pada dinamakan pemetaan **satu-satu pada** (**bijektif**).

Dalam Contoh 1.1.13 dan 1.1.14 adalah pemetaan pada, sedangkan dalam Contoh 1.1.12 bukan petaan pada.

Definisi 1.1.7 Diberikan dua pemetaan $\phi : A \to B$ dan $\chi : B \to C$. Didefinisikan pemetaan **komposisi** $\chi \circ \phi : A \to C$ oleh

$$\chi \circ \phi(a) \stackrel{\text{def}}{=} \chi(\phi(a)), \ \forall a \in A.$$

Contoh 1.1.15 Misalkan $\phi : \mathbb{Z} \to 2\mathbb{Z}$ diberikan oleh $\phi(n) = 2n$, $\forall n \in \mathbb{Z}$ dan misalkan $\chi : 2\mathbb{Z} \to 10\mathbb{Z}$ diberikan oleh $\chi(m) = 5m$, $\forall m \in 2\mathbb{Z}$. Didapat

$$\chi \circ \phi(n) = \chi(\phi(n)) = \chi(2n) = 5 \cdot 2n = 10n.$$

Catatan bahwa, pemetaan ϕ, χ dan $\chi \circ \phi$ adalah pemetaan satu-satu pada. ●

Contoh 1.1.16 Misalkan $\phi : \mathbb{R} \to \mathbb{R}$ dan $\chi : \mathbb{R} \to \mathbb{R}$ diberikan oleh $\phi(x) = 2x$ dan $\chi(x) = x^2$ untuk semua x di $\mathbb{R}$. Komposisi $\chi \circ \phi : \mathbb{R} \to \mathbb{R}$ dan $\phi \circ \chi : \mathbb{R} \to \mathbb{R}$ diberikan oleh $\chi \circ \phi(x) = \chi(\phi(x))$ dan $\phi \circ \chi(x) = \phi(\chi(x))$ untuk semua $x \in \mathbb{R}$. Didapat, $\chi(\phi(x)) = \chi(2x) = (2x)^2 = 4x^2$ dan $\phi(\chi(x)) = \phi(x^2) = 2x^2$. Terlihat bahwa $\chi \circ \phi \neq \phi \circ \chi$. Perlu diperhatikan bahwa, walaupun ϕ satu-satu pada tak-satupun dari pemetaan $\chi, \chi \circ \phi$ dan $\phi \circ \chi$ adalah satu-satu pada. ●

Berikut ini diberikan bahwa komposis dari dua pemetaan menghasilkan pemetaan lagi.

Teorema 1.1.1 Bila $\phi : A \to B$ dan $\chi : B \to C$ keduanya adalah pemetaan, maka komposisi $\chi \circ \phi$ juga merupakan pemetaan dari A ke C.

Bukti
Komposisi $\chi \circ \phi$ adalah suatu relasi dari A ke C dan $\text{Dom}(\chi \circ \phi) \subseteq A$ juga $\text{Im}(chi \circ \phi) \subseteq C$. Diberikan sebarang $a \in A$, karena $A = \text{Dom}(\phi)$, maka ada tunggal $b \in B$ sehingga $b = \phi(a)$. Tetapi $B = \text{Dom}(\chi)$, jadi ada tunggal $c \in C$ sehingga $c = \chi(b)$. Maka dari itu

$$c = \chi(b) = \chi(\phi(a)) = (\chi \circ \phi)(a).$$

Terlihat bahwa $a \in \text{Dom}(\chi \circ \phi)$. Jadi $A \subseteq \text{Dom}(\chi \circ \phi)$. Karena $\text{Dom}(\chi \circ \phi) \subseteq A$, maka $\text{Dom}(\chi \circ \phi) = A$.

Misalkan bahwa $(a, y) \in \chi \circ \phi$ dan $(a, z) \in \chi \circ \phi$, maka ada $b \in B$ sehingga $(a, b) \in \phi$ dan $(b, y) \in \chi$. Juga ada $\beta \in B$ sehingga $(a, \beta) \in \phi$ dan $(\beta, z) \in \chi$. Karena ϕ adalah pemetaan, maka $b = \beta$. Didapat $(b, y) \in \chi$ dan $(b, z) \in \chi$. Karena χ adalah pemetaan, maka haruslah $y = z$. Jadi bila $(a, y) \in \chi \circ \phi$ dan $(a, z) \in \chi \circ \phi$ berakibat bahwa $y = z$. Hal ini menunjukkan bahwa $\chi \circ \phi$ adalah suatu pemetaan. ✓

Teorema 1.1.2 Diberikan tiga pemetaan $\phi : A \to B$, $\chi : B \to C$ dan $\psi : C \to D$. Maka

(1) Assosiatif : $\psi \circ (\chi \circ \phi) = (\psi \circ \chi) \circ \phi$.

(2) Bila ϕ dan χ keduanya adalah satu-satu, maka $\chi \circ \phi$ satu-satu.

(3) Bila ϕ dan χ keduanya adalah pada, maka $\chi \circ \phi$ pada.

Bukti

(1) Untuk sebarang $x \in A$, didapat

$$\begin{aligned} \psi \circ (\chi \circ \phi)(x) &= \psi((\chi \circ \phi)(x)) \\ &= \psi(\chi(\phi(x))) \\ &= (\psi \circ \chi)(\phi(x)) \\ &= (\psi \circ \chi) \circ \phi(x). \end{aligned}$$

Terlihat bahwa $\psi \circ (\chi \circ \phi) = (\psi \circ \chi) \circ \phi$.

(2) Diberikan sebarang $x, y \in A$ yang memenuhi $\chi \circ \phi(x) = \chi \circ \phi(y)$, ditunjukkan bahwa $x = y$. Didapat $\chi(\phi(x)) = \chi(\phi(y))$. Karena χ satu-satu, maka haruslah $\phi(x) = \phi(y)$. Juga karena ϕ satu-satu, maka haruslah $x = y$. Dengan demikian $\chi \circ \phi$ adalah satu-satu.

(3) Diberikan sebarang $z \in C$, karena χ pada dapat dipilih $y \in B$ yang memenuhi $\chi(y) = z$. Tetapi ϕ adalah pada, maka dapat dipilih $x \in A$ yang memenuhi $\phi(x) = y$. Sehingga didapat $\chi(y) = \chi(\phi(x)) = z$ atau $(\chi \circ \phi)(x) = z$. Jadi bila diberikan sebarang $z \in C$ selalu dapat dipilih $x \in A$ yang memenuhi $(\chi \circ \phi)(x) = z$. Hal ini berarti bahwa $\chi \circ \phi$ adalah pada.

Definisi 1.1.8 Untuk sebarang himpunan $A \neq \varnothing$ didefinisikan suatu pemetaan **identitas** $\rho_0 : A \to A$ oleh $\rho_0(x) = x$, $\forall x \in A$.

Proposisi 1.1.2 Misalkan A adalah sebarang himpunan tak-kosong dan $\rho_0 : A \to A$ adalah pemetaan identitas. Maka

(1) ρ_0 adalah satu-satu pada.

(2) Untuk sebarang himpunan B dan sebarang pemetaan $\phi : A \to B$, didapat $\phi \circ \rho_0 = \phi$.

(3) Untuk sebarang pemetaan $\phi : B \to A$, didapat $\rho_0 \circ \phi = \phi$

Bukti

(1) Diberikan sebarang $y \in A$ (kodomain) dan karena ρ_0 pemetaan identitas, maka dapat dipilih $x \in A$ (domain) yaitu $x = y$ sehingga $\rho_0(x) = x = y$. Jadi ρ_0 adalah pada. Selanjutnya bila $a, b \in A$ (domain) yang memenuhi $\rho_0(a) = \rho_0(b)$. Didapat $a = b$. Jadi ρ_0 adalah satu-satu. Dengan demikian ρ_0 adalah satu-satu pada.

(2) Diberikan sebarang $a \in A$, didapat $\phi \circ \rho_0(a) = \phi(\rho_0(a)) = \phi(a)$. Terlihat bahwa $\phi \circ \rho_0 = \phi$.

(3) Diberikan sebarang $b \in B$, didapat $\rho_0 \circ \phi(b) = \rho_0(\phi(b)) = \phi(b)$. Terlihat bahwa $\rho_0 \circ \phi = \phi$.

Contoh 1.1.17 Misalkan $\phi : \mathbb{Z} \to 3\mathbb{Z}$ didefinisikan oleh $\phi(n) = 3n$, $\forall n \in \mathbb{Z}$. Selanjutnya perhatikan bahwa pemetaan $\chi : 3\mathbb{Z} \to \mathbb{Z}$ yang didefinisikan oleh $\chi(m) = \frac{m}{3}$, $\forall m \in 3\mathbb{Z}$. Maka $\chi \circ \phi(n) = \chi(\phi(n)) = \frac{3n}{3} = n$. Terlihat bahwa $\chi \circ \phi$ adalah pemetaan identitas pada $\mathbb{Z}$. Juga, $\phi \circ \chi(m) = \phi(\chi(m)) = \phi(\frac{m}{3}) = 3\frac{m}{3} = m$. Terlihat bahwa $\phi \circ \chi$ adalah pemetaan identitas.

Definisi 1.1.9 Misalkan $\phi : A \to B$. Maka pemetaan ϕ dikatakan **mempunyai invers** bila ada suatu pemetaan $\phi^{-1} : B \to A$ sedemikian hingga $\phi^{-1} \circ \phi$ adalah pemetaan identitas pada A dan $\phi \circ \phi^{-1}$ adalah pemetaan identitas pada B. Pemetaan ϕ^{-1} dinamakan **invers** dari ϕ.

Teorema 1.1.3 Misalkan $\phi : A \to B$ mempunyai invers. Maka

(1) Ada dengan tunggal invers ϕ^{-1} terhadap ϕ.

(2) Invers dari ϕ^{-1} adalah ϕ, yaitu $(\phi^{-1})^{-1} = \phi$.

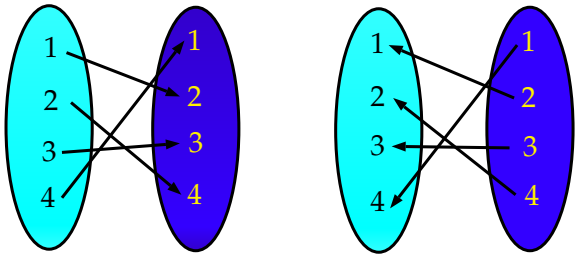
Bukti

(1) Misalkan ada dua pemetaan $\chi : B \to A$ dan $\psi : B \to A$ dengan $\chi \circ \phi = \psi \circ \phi = \rho_0^A$ dan ρ_0^A pemetaan identitas pada A dan $\phi \circ \chi = \phi \circ \psi = \rho_0^B$, ρ_0^B adalah pemetaan identitas pada B. Maka

$$\chi = \chi \circ \rho_0^B = \chi \circ (\phi \circ \psi) = (\chi \circ \phi) \circ \psi = \rho_0^A \circ \psi = \psi.$$

(2) Jelas dari definisi invers. ✓

Contoh 1.1.18 Misalkan $\phi : \{1,2,3,4\} \to \{1,2,3,4\}$ didefinisikan oleh $\phi(1) = 2, \phi(2) = 4, \phi(3) = 3, \phi(4) = 1$ atau diberikan oleh sebelah kiri Gambar 1.6. Maka ϕ^{-1} didefinisikan oleh



Gambar 1.6: Diagram Fungsi

$\phi^{-1}(1) = 4, \phi^{-1}(2) = 1, \phi^{-1}(3) = 3, \phi^{-1}(4) = 2$, atau diberikan oleh sebelah kanan Gambar 1.6.

Contoh 1.1.19 Misalkan $\phi : \mathbb{R} \to \mathbb{R}^{\geq}$, dengan $\mathbb{R}^{\geq} = \{x \in \mathbb{R} \mid x \geq 0\}$ adalah himpunan bilangan riil tak-negatif dan $\phi(x) = |x|$, $\forall x \in \mathbb{R}$. Perlu diperhatikan bahwa pemetaan ϕ adalah pada, tetapi tidak satu-satu. Sebab $\phi(-2) = \phi(2) = 2$. Juga pemetaan ϕ tidak mempunyai invers sebab pasangan dari $2 \in \mathbb{R}^{\geq}$ terhadap ϕ^{-1} tidak tunggal, yaitu $\phi^{-1}(2) = -2$ dan $\phi^{-1}(2) = 2$.

Contoh 1.1.20 Misalkan $\phi : \mathbb{Z} \to \mathbb{Z}$ didefinisikan oleh $\phi(n) = 5n$, $\forall n \in \mathbb{Z}$. Catatan bahwa pemetaan ϕ satu-satu tetapi tidak pada. Sebab $7 \neq 5n$ untuk setiap $n \in \mathbb{Z}$ dan pemetaan ϕ tidak punya invers sebab $6 \in \mathbb{Z}$ (kodomain) tidak punya kawan di domain $\mathbb{Z}$, yaitu $\phi^{-1}(6)$ tidak terdefinisi.

Teorema 1.1.4 Misalkan $\phi : A \to B$ dan $\chi : B \to C$ adalah dua pemetaan. Maka

(1) pemetaan ϕ mempunyai invers bila dan hanya bila ϕ satu-satu pada.

(2) Bila masing-masing ϕ dan χ mempunyai invers, maka $\chi \circ \phi$ mempunyai invers dan $(\chi \circ \phi)^{-1} = \phi^{-1} \circ \chi^{-1}$.

Bukti

(1) ($\Rightarrow$) Misalkan $\phi^{-1} : B \to A$ ada. Maka untuk sebarang $a, b \in A$ dan $\phi(a) = \phi(b)$ didapat

$$a = \phi^{-1}(\phi(a)) = \phi^{-1}(\phi(b)) = b.$$

Terlihat bahwa pemetaan ϕ adalah pada. Selanjutnya, diberikan sebarang $b \in B$, maka $\phi(\phi^{-1}(b)) = b$. Jadi dapat dipilih $a = \phi^{-1}(b)$ di A yang memenuhi $\phi(a) = b$. Jadi ϕ adalah

pada. Dengan demikian ϕ adalah satu-satu pada.
($\Leftarrow$) Misalkan ϕ adalah satu-satu pada. definisikan pemetaan $\tau : B \to A$ sebagai berikut. Untuk sebarang $b \in B$, $\tau(b)$ adalah elemen $a \in A$ yang memenuhi $\phi(a) = b$ (sebab ϕ adalah pada). Dan, karena ϕ satu-satu, maka hanya ada tepat satu $a \in A$. Jadi τ terdefinisi secara baik. Selanjutnya, dari definisi τ didapat $\phi(\tau(b)) = b$ untuk sebarang $b \in B$, juga $\tau(\phi(a)) = a$. Jadi $\tau = \phi^{-1}$ dengan demikian ϕ punya invers.

(2) Asumsikan bahwa maasing-masing ϕ dan χ mempunyai invers. Maka dari (1) ϕ dan χ adalah satu-satu pada. Dengan menggunakan Teorema 1.1.2 $\chi \circ \phi$ adalah satu-satu pada. Lagi, dengan menggunakan hasil (1) $\chi \circ \phi$ mempunyai invers. Sehingga didapat

$$(\phi^{-1} \circ \chi^{-1}) \circ (\chi \circ \phi) = \phi^{-1} \circ (\chi^{-1} \circ \chi) \circ \phi = \phi^{-1} \circ \rho_0^B \circ \phi = \phi^{-1} \circ \phi = \rho_0^A.$$

Terlihat bahwa $\phi^{-1} \circ \chi^{-1} = (\chi \circ \phi)^{-1}$.

Definisi 1.1.10 Diberikan dua himpunan A dan B, maka A dan B mempunyai **kardinalitas yang sama**, yaitu $|A| = |B|$ bila dan hanya bila ada suatu pemetaan satu-satu pada $\phi : A \to B$.

Contoh 1.1.21 Dua himpunan berhingga mempunyai kardinalitas sama bila dan hanya bila banyaknya elemen kedua himpunan tersebut sama. Juga, $|\mathbb{Z}| = |2\mathbb{Z}| = |n\mathbb{Z}|$ untuk sebarang bilangan bulat $n \geq 1$, sebab pemetaan $\phi : \mathbb{Z} \to n\mathbb{Z}$ didefinisikan oleh $\phi(x) = nx$, $\forall x \in \mathbb{Z}$ adalah pemetaan satu-satu pada.

Latihan

Latihan 1.1.1 Tentukan apakah pemetaan yang berikut ini pemetaan satu-satu atau bukan dan berikan alasannya.

1. $\phi : \mathbb{R} \to \mathbb{R}$, dengan $\phi(x) = 5x + 3$, $\forall x \in \mathbb{R}$.
2. $\phi : \mathbb{R} \to \mathbb{R}$, dengan $\phi(x) = e^x$, $\forall x \in \mathbb{R}$.
3. $\phi : \mathbb{R} \to \mathbb{R}$, dengan $\phi(x) = x^3$, $\forall x \in \mathbb{R}$.
4. $\phi : \mathbb{Z} \to \mathbb{Z}$, dengan $\phi(n) = n^2$, $\forall n \in \mathbb{Z}$.
5. $\phi : \mathbb{Q}^* \to \mathbb{Q}^*$, dengan $\mathbb{Q}^*$ adalah himpunan semua bilangan rasional tak-nol dan $\phi(n/m) = m/n$, $\forall n/m \in \mathbb{Q}^*$.
6. $\phi : \mathbb{R}^+ \to \mathbb{R}^+$, dengan $\mathbb{R}^+$ adalah himpunan semua bilangan riil positip dan $\phi(x) = x^4$, $\forall x \in \mathbb{R}$.
7. $\phi : \mathbb{Z} \times \mathbb{Z}^* \to \mathbb{Q}$, dengan $\mathbb{Z}^*$ adalah himpunan semua bilangan bulat tak-nol dan $\phi(m, n) = m/n$, $\forall x \in \mathbb{R}$.

Latihan 1.1.2 Tentukan apakah pemetaan berikut pada atau tidak, jelaskan jawaban saudara.

1. $\phi : \mathbb{R}^+ \to \mathbb{R}$, dengan $\phi(x) = \ln x$, $\forall x \in \mathbb{R}^+$.
2. $\phi : \mathbb{R} \to \mathbb{R}$, dengan $\phi(x) = x^2 - 4$, $\forall x \in \mathbb{R}$.

3. $\phi : \{1,2,3,4\} \to \{1,2,3,4\}$, ϕ adalah sebarang pemetaan satu-satu.

Latihan 1.1.3 Apakah pemetaan berikut mempunyai invers atau tidak, berikan alasannya.

1. $\phi : \mathbb{R} \to \mathbb{R}$, dengan $\phi(x) = |x+1|,\ \forall x \in \mathbb{R}$.

2. $\phi : \mathbb{R} \to \mathbb{R}$, dengan $\phi(x) = (5x+3)/2,\ \forall x \in \mathbb{R}$.

3. Diberikan pemetaan
$$\phi : \{1,2,3,\ldots,n\} \to \{1,2,3,\ldots,n\},$$
dengan $\phi(i) = i+2$ untuk $1 \le i \le n-2$ dan $\phi(n-1) = 1, \phi(n) = 2$.

Latihan 1.1.4 Diberikan dua pemetaan $\phi : A \to B$ dan $\chi : B \to C$. Tunjukkan bahwa

(a) Bila $\chi \circ \phi$ adalah pada, maka χ harus juga pada.

(b) Bila $\chi \circ \phi$ adalah satu-satu, maka ϕ harus juga satu-satu.

Latihan 1.1.5 Tunjukkan bahwa bila himpunan A adalah berhingga dan $|A| = n$, maka $|A \times A| = n^2$.

Latihan 1.1.6 Tunjukkan bila $|A| = |B|$ dan $|C| = |D|$, maka $|A \times C| = |B \times D|$.

1.2 Relasi Ekivalen dan Partisi

Gagasan relasi ekivalen pada himpunan memainkan peran penting dalam berbagai konstruksi dalam aljabar. Seperti yang akan terlihat di bagian ini. Relasi ekivalen pada himpunan menentukan partisi dari himpunan menjadi potongan-potongan yang tidak tumpang tindih, dan sebaliknya setiap partisi tersebut menentukan relasi ekivalen pada himpunan tersebut.

Contoh 1.2.1 Pada himpunan $\mathbb{Z}$, diberikan relasi $\sim$ didefinisikan oleh kondisi $a \sim b$ bila dan hanya bila $a - b$ dapat dibagi oleh 5 untuk setiap $a, b \in \mathbb{Z}$. Perlu diperhatikan bahwa, relasi $\sim$ mempunyai sifat berikut:

1. Untuk setiap bilangan bulat a, didapat $a - a = 0$, jadi $a - a$ dapat dibagi oleh 5. Dengan demikian $a \sim a$.

2. Untuk setiap $a, b \in \mathbb{Z}$, $a - b = -(b - a)$. Jadi bila $a \sim b$ yang berarti bahwa $a - b$ dapat dibagi 5, maka juga $b - a$ dapat dibagi 5. Dengan demikian $b \sim a$.

3. Untuk $a, b, c \in \mathbb{Z}$, bila $a \sim b$ dan $b \sim c$, maka $a - b = 5n$ dan $b - c = 5m$ untuk beberapa $m, n \in \mathbb{Z}$. Didapat
$$a - c = (a - b) + (b - c) = 5n + 5m = 5(n + m),$$
terlihat bahwa $a \sim c$.

Selanjutnya diambil $8 \in \mathbb{Z}$, diselidiki himpunan semua bilangan bulat x yang memenuhi $x \sim 8$, yaitu $[8]_\sim = \{x \in \mathbb{Z} \mid x \sim 8\} \subset \mathbb{Z}$. Perhatikan bahwa $8 - 3 = 5$. Jadi $8 \sim 3$ dan berdasarkan sifat (3), maka $x \sim 3$. Juga berdasarkan sifat (2), maka $3 \sim 8$. Jadi bila $x \sim 3$, maka $x \sim 8$. Jadi $x \sim 8$ bila dan hanya bila $x \sim 3$ atau bila dan hanya bila $x - 3 = 5k$ atau ekivalen $x = 2 + 5k$ untuk beberapa bilangan bulat k. Dengan demikian $[8]_\sim = 3 + 5\mathbb{Z}$ adalah himpunan semua bilangan bulat yang dapat diungkapkan sebagai jumlah dari 3 dan kelipatan 5. ●

Contoh 1.2.2 Bila $P(\mathbb{Z})$ adalah himpunan dari semua himpunan bagian dari $\mathbb{Z}$ dan relasi pada $P(\mathbb{Z})$ didefinisikan sebagai berikut: diberikan sebarang $S, T \in P(\mathbb{Z})$, $S \sim T$ bila dan hanya $|S| = |T|$. Tetapi $|S| = |T|$, berarti bahwa ada pemetaan $\phi : S \to T$ dengan ϕ adalah satu-satu pada. Selanjutnya dibahas sifat dari relasi $\sim$:

1. Untuk sebarang $S \in P(\mathbb{Z})$, pilih ϕ pemetaan identitas pada S. Sebagaimana telah dibahas pemetan ini adalah satu-satu pada. Jadi $S \sim S$.

2. Untuk sebarang $S, T \in P(\mathbb{Z})$, bila $S \sim T$ dapat dipilih pemetaan satu-satu pada $\phi : S \to T$. Maka dengan menggunakan Teorema 1.1.3 dan 1.1.4 pemetaan invers $\phi^{-1} : T \to S$ adalah satu-satu pada. Jadi $T \sim S$.

3. Untuk sebarang $S, T, U \in P(\mathbb{Z})$, bila $S \sim T$ dan $T \sim U$, maka dapat dipilih pemetaan satu-satu pada $\phi : S \to T$ dan $\chi : T \to U$. Dengan menggunakan Teorema 1.1.4 didapat pemetaan komposisi $\chi \circ \phi : S \to U$ adalah satu-satu pada. Dengan demikian $S \sim U$. ●

Berikut ini kita ulangi lagi pembahasan tentang Relasi pada Definisi 1.1.3, disini dibahas himpunan $A = B$ dan dikaitkan dengan pengertian suatu relasi yang khusus yang dinamakan relasi ekivalen.

Definisi 1.2.1 Suatu **relasi** pada suatu himpunan tak-kosong S adalah himpunan bagian $\mathcal{R} \subset S \times S$. Bila $\mathcal{R}$ adalah suatu relasi pada S penulisan $a\mathcal{R}b$ mempunyai arti $(a, b) \in \mathcal{R}$. Jadi $\mathcal{R}$ adalah suatu **relasi ekivalen** bila tiga kondisi berikut dipenuhi, yaitu untuk semua $a, b, c \in S$

1. **Refleksif** $a\mathcal{R}a$.

2. **Simetri** Bila $a\mathcal{R}b$, maka $b\mathcal{R}a$.

3. **Transitif** Bila $a\mathcal{R}b$ dan $b\mathcal{R}c$, maka $a\mathcal{R}c$.

Bila $\mathcal{R}$ adalah relasi ekivalen pada S, maka untuk sebarang $a \in S$, **klas ekivalen** dari a adalah himpunan $[a]_\mathcal{R} \stackrel{\text{def}}{=} \{b \in S \mid a\mathcal{R}b\}$. ✓

Relasi yang diberikan dalam Contoh 1.2.1 dan 1.2.2 adalah relasi ekivalen.

Contoh 1.2.3 Diberikan $S \neq \emptyset$, relasi sama dengan $=$ didefinisikan oleh himpunan bagian $\{(x, x) \mid x \in S\} \subset S \times S$ adalah suatu relasi ekivalen. ●

Berikut ini diberikan beberapa sifat penting dari relasi ekivalen yang sering digunakan dalam pengkonstruksian secara aljabar.

Teorema 1.2.1 Misalkan $\sim$ adalah suatu relasi ekivalen pada suatu himpunan tak-kosong S dan $a, b \in S$ adalah sebarang elemen di S. Maka

(1) $a \in [a]_\sim$.

(2) Bila $a \in [b]_\sim$, maka $[a]_\sim = [b]_\sim$.

(3) $[a]_\sim = [b]_\sim$ bila dan hanya bila $a \sim b$.

(4) Salah satu $[a]_\sim = [b]_\sim$ atau $[a]_\sim \cap [b]_\sim = \emptyset$

Bukti

(1) Dari sifat refleksif, maka $a \sim a$. Jadi $a \in [a]_\sim$.

(2) Bila $a \in [b]_\sim$. Maka dari definisi klas ekivalen didapat $b \sim a$. Dari sifat simetri didapat $a \sim b$. Selanjutnya bila $x \in [a]_\sim$, maka $a \sim x$. Dengan sifat transitif, maka $b \sim x$. Jadi $x \in [b]_\sim$. Terlihat bahwa $[a]_\sim \subseteq [b]_\sim$. Dengan cara yang sama, bila $y \in [b]_\sim$, maka $b \sim y$. Dengan menggunakan sifat transitif didapat $a \sim y$ dan $y \in [a]_\sim$. Jadi $[b]_\sim \subseteq [a]_\sim$. Dengan demikian $[a]_\sim = [b]_\sim$.

(3) ($\Rightarrow$) Misalkan $[a]_\sim = [b]_\sim$. Dari (1) didapat $b \in [b]_\sim$. Jadi $b \in [a]_\sim$, hal ini berarti bahwa $a \sim b$.
($\Leftarrow$) Misalkan $a \sim b$. Maka $b \in [a]_\sim$. Dengan menggunakan hasil (2) didapat $[a]_\sim = [b]_\sim$.

(4) Andaikan bahwa $[a]_\sim \cap [b]_\sim \neq \emptyset$. Hal ini berarti bahwa ada beberapa $c \in [a]_\sim$ dan $c \in [b]_\sim$. Dengan menggunakan hasil (2), maka $[c]_\sim = [a]_\sim$ dan $[c]_\sim = [b]_\sim$. Jadi $[a]_\sim = [b]_\sim$. ✓

Hasil Teorema 1.2.1 bagian (4) menyatakan bahwa dua klas ekivalen, maka kalau tidak sama pasti irisan keduanya kosong dan sebaliknya kalau irisannya tidak kosong pasti keduanya sama. Hal ini berarti bahwa relasi ekivalen adalah suatu partisi yang membagi klas ekivalen berbeda kedalam klas yang saling asing (irisannya kosong). Relasi ekivalen sangat berguna dalam pengkontruksian secara aljabar. Pada contoh berikut, bukannya memulai dengan relasi ekivalen tetapi mempartisi himpunan. Dimulai dengan mempartisi satu himpunan dan menggunakan partisi untuk mendefinisikan relasi ekivalen.

Contoh 1.2.4 Diberikan himpunan bilangan riil $\mathbb{R}$, misalkan $[1] = \{x \in \mathbb{R} \mid 0 \leq x - 1 < 1\}$. Himpuna $[1]$ adalah interval $[1, 2) \subset \mathbb{R}$. Dengan cara yang sama, untuk sebarang bilangan bulat n, misalkan $[n] = \{x \in \mathbb{R} \mid 0 \leq x - n < 1\} = [n, n + 1)$. Catatan bahwa, untuk sebarang bilangan bulat $i \neq j$ didapat $[i] \cap [j] = \emptyset$ dan untuk setiap bilangan riil $x \in \mathbb{R}$, $x \in [n]$ dimana n adalah bilangan bulat terbesar sehingga $n \leq x$. Jadi $\mathbb{R}$ dibagi kedalam klas yang saling asing. Bila didefinisikan suatu relasi $\sim$ pada $\mathbb{R}$ oleh $x \sim y$ bila dan hanya bila $x \in [n]$ dan $y \in [n]$, maka dapat ditunjukkan bahwa $\sim$ adalah suatu relasi ekivalen pada $\mathbb{R}$. ●

Definisi 1.2.2 Misalkan S adalah himpunan tak-kosong. Suatu **partisi** dari S terdiri dari suatu himpunan koleksi $\mathcal{K} = \{P_i \mid P_i \subseteq S\}$ dari himpunan bagian tak-kosong dari S yang memenuhi

(1) $S = \bigcup_i P_i$.

(2) Untuk sebarang P_i dan P_j dalam himpunan koleksi $\mathcal{K}$, maka salah satu yang terjadi $P_i = P_j$ atau $P_i \cap P_j = \emptyset$.

Himpunan bagian P_i dalam koleksi $\mathcal{K}$ dinamakan **sel** dari partisi.

Sekarang sampai pada Teorema utama yang menghubungkan relasi ekivalen dengan partisi, generalisasi dari apa yang telah dibahas dalam Contoh 1.2.4.

Teorema 1.2.2 Misalkan S adalah himpunan tak-kosong

(1) Diberikan relasi ekivalen $\sim$ pada S, koleksi dari klas ekivalen terhadap $\sim$ adalah suatu partisi.

(2) Diberikan suatu partisi $\{P_i\}$ dari S, ada suatu relasi ekivalen pada S yang mempunyai klas ekivalen adalah tepat merupakan sel dari partisi.

Bukti

(1) Diberikan suatu relasi ekivalen $\sim$ pada S. Dari Teorema 1.2.1 bagian (1) didapat $a \in [a]_\sim$ untuk setiap $a \in S$. Dengan menggunakan Teorema 1.2.1 bagian (4) didapat $S = \bigcup_{a \in S} [a]_\sim$.

(2) Diberikan suatu partisi $\{P_i\}$ didefinisikan suatu relasi $\sim$ oleh: $a \sim b$ bila dan hanya bila $a \in P_i$ dan $b \in P_i$. Dari Definisi 1.2.2 bagian (1) didapat sebarang $a \in S$ berada pada beberapa sel dalam partisi, tentunya a berada pada sel yang sama dengan dirinya sendiri. Jadi $a \sim a$. Bila $a \sim b$, maka a dan b berada pada sel yang sama dalam partisi. Hal ini sama artinya b dan a berada pada sel yang sama dalam partisi. Jadi $b \sim a$. Bila $a \sim b$ dan $b \sim c$, maka a dan b berada pada sel yang sama P_i juga b dan c berada pada sel yang sama P_j. Karena $b \in P_i \cap P_j$, maka dengan menggunakan Definisi 1.2.2 bagian (2) didapat $P_i = P_j$. Jadi a dan c berada pada sel yang sama, dengan demikian $a \sim c$. Selanjutnya diberikan $a \in S$, misalkan $a \in P_i$. Maka $x \in [a]_\sim$ bila dan hanya bila $a \sim x$ atau bila dan hanya bila a dan x berda pada sel yang sama dalam partisi atau dengan kata lain bila dan hanya bila $x \in P_i$. Jadi $[a]_\sim = P_i$.

Definisi 1.2.3 Misalkan $\sim$ adalah suatu relasi ekivalen pada S himpunan semua klas ekivalen pada S terhadap $\sim$ dinotasikan oleh $S/\sim$. Khususnya, masing-masing elemen dari $S/\sim$ adalah himpunan bagian dari S. Didefinisikan suatu pemetaan $\phi : S \to S/\sim$ oleh $\phi(x) = [x]_\sim, \forall x \in S$. Pemetaan ϕ dinamakan pemetaan ***kanonik*** dari S ke $S\sim$.

Contoh 1.2.5 Misalkan $S = \{1, 2, 3, 4\}$ dan $\sim$ adalah relasi ekivalen pada S yang diberikan oleh $1 \sim 3, 2 \sim 4$ dan pasangan lain yang berelasi diberikan oleh sifat refleksif dan simetri. Maka ada dua elemen di $S/\sim$ yaitu $\{1, 3\}$ dan $\{2, 4\}$ sehingga didapat $\phi(1) = \phi(3) = \{1, 3\}$ dan $\phi(2) = \phi(4) = \{2, 4\}$.

Latihan

Latihan 1.2.1 Tentukan apakah relasi berikut adalah relasi ekivalen pada himpunan yang diberikan. Bila ya, uraikan klas ekivalennya.

1. Dalam $\mathbb{R}$, $a \sim b$ bila dan hanya bila $|a| = |b|$.
2. Dalam $\mathbb{R}$, $a \sim b$ bila dan hanya bila $a \leq b$.
3. Dalam $\mathbb{Z}$, $a \sim b$ bila dan hanya bila $a - b$ adalah genap.

4. Dalam $\mathbb{R}$, $a \sim b$ bila dan hanya bila $|a - b| \leq 1$.
5. Dalam $\mathbb{Z}$, $a \sim b$ bila dan hanya bila $a = b +$ beberapakelipatandari 3.
6. Dalam $\mathbb{R} \times \mathbb{R} - \{(0,0)\}$, $(x_1, y_1) \sim (x_2, y_2)$ bila dan hanya bila $x_1 y_2 = x_2 y_1$.
7. Dalam $\mathbb{R} \times \mathbb{R}$, $(x_1, y_1) \sim (x_2, y_2)$ bila dan hanya bila $x_1^2 + y_1^2 = x_2^2 + y_2^2$.
8. Dalam $\mathbb{R} \times \mathbb{R}$, $(x_1, y_1) \sim (x_2, y_2)$ bila dan hanya bila $3y_1 - 5x_1 = 3y_2 - 5x_2$. ✓

Latihan 1.2.2 Dalam $\mathbb{R}$, diberikan interval $(n, n+2]$ dimana n adalah bilangan bulat genap. Tunjukkan bahwa koleksi dari interval-interval tersebut adalah suatu partisi dari $\mathbb{R}$. Selanjutnya uraikan relasi ekivalen yang ditentukan oleh partisi tersebut. ✓

Latihan 1.2.3 Dalam bidang $\mathbb{R} \times \mathbb{R}$ terangkan mengapa pendefinisian $(x_1, y_1) \sim (x_2, y_2)$ bila dan hanya bila $x_1 y_2 = x_2 y_1$ tidak memberikan relasi ekivalen. ✓

Latihan 1.2.4 Diberikan sebarang bilangan bulat n yang tetap. Didefinisikan relasi pada $\mathbb{Z}$, $a \sim b$ bila dan hanya bila $a - b$ dapat dibagi oleh n. Tunjukkan relasi tersebut adalah relasi ekivalen pada $\mathbb{Z}$ dan uraikan klas ekivalennya. ✓

Latihan 1.2.5 Misalkan $\phi : S \to T$ adalah sebarang pemetaan dan didefinisikan suatu relasi $\sim$ pada S oleh $a \sim b$ bila dan hanya bila $\phi(a) = \phi(b)$. Tunjukkan bahwa $\sim$ adalah suatu relasi ekivalen. ✓

1.3 Sifat-sifat dari $\mathbb{Z}$

Pada bagian ini dibahas beberapa sifat dasar bilangan bulat, banyak yang akan menjadi penting kemudian dalam mengidentifikasi contoh berbagai jenis struktur aljabar, dimana $\mathbb{Z}$ akan memainkan peran penting bagi suatu model dasar. Bahasan dimulai dengan sifat relasi urutan biasa pada $\mathbb{Z}$ kemudian beralih ke sifat-sifat yang melibatkan operasi yang sudah dikenal penjumlahan, pengurangan, perkalian, dan pembagian. Akhirnya, diperkenalkan struktur aljabar baru terkait erat dengan bilangan bulat, yang disebut bilangan bulat mod n untuk setiap bilangan bulat $n > 1$.

Terurut Secara Baik dan Induksi

Elemen-elemen himpunan bilangan bulat positip $\mathbb{N}$ dapat ditulis dalam urutan menaik dengan tanda pertaksamaan berulang, yaitu

$$1 < 2 < 3 < 4 < 5 < \cdots$$

Misalkan $S \subset \mathbb{N}$ dengan $S \neq \emptyset$ dan $n \in \mathbb{N}$. Dari bilangan bulat berikut $1, 2, 3, \ldots, n$ dapat dipilih satu yang merupakan elemen terkecil yang berada di S. Secara intuisi didapat aksiomatik berikut.

Aksiomatik 1 (Prinsip Keterurutan Secara Baik dalam $\mathbb{N}$)
Setiap himpunan bagian $S \subset \mathbb{N}$ dengan $S \neq \emptyset$ mempunyai suatu elemen terkecil di S, yaitu elemen pertama di S setelah elemen-elemennya diurutkan secara menaik. ☑

Sering dalam membuktikan beberapa teorema atau membangun beberapa struktur diinginkan memilih elemen positip terkecil dari himpunan tak-kosong yang diberikan. Prinsip keterurutan secara baik menyatakan bahwa elemen tersebut dijamin ada. Terkait erat dengan prinsip keterurutan secara baik ada prinsip lain yaitu induksi matematika, yang sama pentingnya dalam bukti dan konstruksi. Digunakan prinsip keterutan secara baik untuk membuktikan prinsip dari induksi matematika sebagaimana diberikan berikut.

Teorema 1.3.1 (**Prinsip dari Induksi Matematika**) Misalkan $P(n)$ adalah pernyataan tentang suatu bilangan bulat positip n sedemikian hingga

(1) $P(1)$ adalah benar.

(2) Bila $P(k)$ adalah benar, maka $P(k+1)$ adalah benar.

Maka $P(n)$ adalah benar untuk semua bilangan bulat positip n.

Bukti Dibuktikan melalui kontradiksi. Andaikan ada bilangan bulat positip n yang memenuhi $P(n)$ tidak benar. Maka dari itu ada himpunan semua bilangan bulat positip

$$S = \{n > 0 \,|\, P(n)\text{tidak benar}\}.$$

Selanjutnya menggunakan prinsip keterutan secara baik, maka S harus mempunyai suatu elemen terkecil misalkan m. Berikutnya dari asumsi (1) m tidak akan sama dengan 1, sebab $P(1)$ benar. Jadi $m-1$ tetap positip. Karena $m-1 < m$ dan m adalah bilangan bulat positip terkecil dengan $P(m)$ tidak benar (sebab $m \in S$) dan $P(m-1)$ adalah benar (sebab $m-1 \notin S$) dengan menggunakan asumsi (2), maka $P(m) = P((m-1)+1)$ adalah benar. Hal ini bertentangan dengan kenyataan bahwa $P(m)$ tidak benar. Dengan demikian haruslah $P(n)$ benar untuk semua bilangan bulat positip. ✓

Contoh 1.3.1 Buktikan bahwa untuk setiap bilangan bulat positip n, maka

$$1 + 3 + 5 + 7 + \cdots + (2n-1) = n^2.$$

Bukti menggunakan prinsip induksi matematika. Untuk $n = 1$ didapat $1 = 1^2$ benar. Misalkan benar untuk $n = k$, didapat

$$1 + 3 + 5 + 7 + \cdots + (2k-1) = k^2 \text{ benar}$$

Selanjutnya ditunjukkan bahwa untuk $n = k+1$ akan didapat

$$1 + 3 + 5 + 7 + \cdots + (2k-1) + (2(k+1)-1) = (k+1)^2.$$

Hal ini dilakukan sebagai berikut

$$\underbrace{1 + 3 + 5 + 7 + \cdots + (2k-1)}_{=k^2} + (2(k+1)-1) = k^2 + 2k + 1 = (k+1)^2.$$

Terlihat benar bahwa

$$1 + 3 + 5 + 7 + \cdots + (2k-1) + (2(k+1)-1) = (k+1)^2. \quad ●$$

Contoh 1.3.2 Buktikan bahwa untuk setiap bilangan bulat $n \geq 0$, suatu himpunan S dengan $|S| = n$ mempunyai himpunan bagian sebanyak 2^n. Untuk membuktikan ini, $n = 0$ dikeluarkan dulu dari bukti induksi. Untuk $n = 0$ dibuktikan sebagai berikut. Himpunan yang tidak mempunyai anggota adalah himpunan kosong. Jadi $S = \emptyset$ dan banyaknya himpunan bagian adalah S sendiri. Jadi benar bahwa $2^0 = 1$. Selanjutnya untuk $n = 1$, maka $S = \{x\}$ dan himpunan bagian dari S adalah: $\emptyset$ dan S sendiri. Jadi banyaknya himpunan bagian dari S adalah $2^n = 2^1 = 2$. Asumsikan benar bahwa himpunan dengan k elemen mempunyai sebanyak 2^k himpunan bagian. Misalkan S sebarang himpunan dengan $|S| = k + 1$ dan a sebarang elemen di S. Selanjutnya misalkan $T = S - \{a\}$. Himpunan T mempunyai elemen sebanyak k. Jadi T memenuhi asumsi yaitu mempunyai sebanyak 2^k himpunan bagian. Himpunan bagian dari S yang tidak memuat a adalah T mempunyai 2^k himpunan bagian. Jadi S mempunyai sebanyak $2^k + 2^k = 2^{k+1}$ himpunan bagian. ●

Contoh 1.3.3 Untuk sebarang bilangan riil x, y dan sebarang bilangan bulat $n \geq 1$ didapat

$$x^{n+1} - y^{n+1} = (x - y)(x^n + x^{n-1}y + \cdots + xy^{n-1} + y^n).$$

Sebagai langkah dasar induksi $n = 1$ didapat $x^2 - y^2(x - y)(x + y)$ adalah jelas benar. Untuk langkah induksi berikutnya, asumsikan bahwa benar

$$x^k - y^k = (x - y)\left(x^{k-1} + x^{k-2}y + \cdots + xy^{k-2} + y^{k-1}\right).$$

Maka didapat

$$\begin{aligned}(x - y)\left(x^k + x^{k-1}y + \cdots + xy^{k-1} + y^k\right) &= (x - y)\left[x(x^{k-1} + x^{k-2}y + \cdots + y^{k-1}) + y^k\right] \\ &= x\underbrace{(x - y)\left(x^{k-1} + x^{k-2}y + \cdots + y^{k-1}\right)}_{=x^k - y^k} + (x - y)y^k \\ &= x\left(x^k - y^k\right) + (x - y)y^k \\ &= x^{k+1} - y^{k+1}.\end{aligned}$$

Terlihat bahwa

$$x^{k+1} - y^{k+1} = (x - y)\left(x^k + x^{k-1}y + \cdots + xy^{k-1} + y^k\right),$$

sebagaimana yang diinginkan. ●

Teorema 1.3.2 Prinsip Induksi (Versi Modifikasi) Misalkan $P(n)$ adalah suatu pernyataan yang bergantung pada bilangan bulat positip n yang memenuhi

(1) $P(1)$ adalah benar.

(2) Bila $P(k)$ benar untuk semua k dengan $1 \leq k < m$, maka $P(m)$ adalah benar.

Maka $P(n)$ adalah benar untuk semua bilangan bulat positip n.

Bukti Misalkan bahwa $Q(n)$ adalah pernyataan bahwa $P(k)$ benar untuk semua k dimana $1 \leq k \leq n$. Ditunjukkan dengan menggunakan prinsip induksi matematika (Teorema 1.3.1) bahwa $Q(n)$ benar untuk semua bilangan bulat positip n. Karena $Q(n)$ berakibat $P(n)$, maka hal ini berakibat $P(n)$ benar untuk semua bilangan bulat positip n. Sebagai langkah dasar, $Q(1)$

adalah pernyataan $P(1)$, adalah benar dari asumsi (1). Untuk langkah induksi berikutnya, asumsikan bahwa $Q(m)$ benar dan dibuktikan bahwa $Q(m+1)$ benar. Disini $Q(m+1)$ adalah pernyataan $P(k)$ benar untuk semua k dimana $1 \leq k \leq m+1$. Untuk $1 \leq k \leq m$, $P(k)$ mengikuti $Q(m)$. Sedangkan untuk $k = m+1$ dengan menggunakan asumsi (2), maka $P(m+1)$ adalah benar.

Dalam Teorema 1.3.1 pernyataan (1) dan (2) dapat diganti sebagai berikut. Diasumsikan untuk beberapa bilangan bulat positip n_0:

(1') $P(n_0)$ adalah benar.

(2') Bila $P(k)$ adalah benar untuk semua k, dengan $n_0 \leq k < m$, maka $P(m)$ adalah benar.

Maka $P(n)$ benar untuk semua $n \geq n_0$.

Contoh 1.3.4 Misalkan bahwa $P(n)$ adalah pernyataan bahwa

$$2n + 1 \leq 2^n \qquad (n \in \mathbb{N}).$$

Pernyataan $P(1)$ dan $P(2)$ adalah salah sebab

$$2(1) + 1 \not\leq 2^1 \quad \text{dan} \quad 2(2) + 1 \not\leq 2^2.$$

Apapun itu, $P(3)$ adalah benar sebab

$$2(3) + 1 = 7 \leq 2^3 = 8.$$

Misalkan bahwa $P(k)$ adalah benar untuk semua $k \geq 3$, didapat

$$2k + 1 \leq 2^k \quad (\text{bila } k \geq 3)$$

Hal ini berakibat bahwa

$$2(k+1) + 1 = 2k + 3 = 2k + 1 + 2 \leq 2^k + 2 \leq 2^k + 2^k = 2^{k+1} \quad (k \geq 3).$$

Terlihat bahwa $P(k+1)$ adalah benar. Akibatnya $P(n)$ adalah benar untuk $n \geq 3$. Atau pernyataan

$$2n + 1 \leq 2^n$$

berlaku untuk semua $n \in \mathbb{N}$, dengan $n \geq 3$.

Contoh 1.3.5 Diberikan dua bilangan riil x dan y, dengan mengalikan bentuk $(x+y)$ berulang kedalam bentuk pangkat didapat:
$(x+y)^2 = x^2 + 2xy + y^2$
$(x+y)^3 = x^3 + 3x^2y + 3xy^2 + y^3$
$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$.
Hal ini menjadi rumit setelah beberapa saat untuk menghitung semua pangkat dari $(x+y)$.

Untuk menyelesaikan masalah tersebut diberikan teorema berikut.

Teorema 1.3.3 (**Binomial**) Diberikan sebarang dua bilangan riil x dan y, maka untuk setiap bilangan bulat $n \geq 1$ didapat

$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \binom{n}{2}x^{n-2}y^2 + \cdots + \binom{n}{n-2}x^2y^{n-2} + \binom{n}{n-1}xy^{n-1} + y^n,$$

dimana **koefisien binomial** diberikan oleh

$$\binom{n}{r} \stackrel{\text{def}}{=} \frac{n!}{r!(n-r)!}$$

untuk $0 \leq k \leq n$.

Bukti Untuk $n = 1$, benar bahwa $x + y = x^1 + y^1$. Asumsikan pernyataan benar untuk k. Didapat

$$\begin{gathered}(x+y)^{k+1} = (x+y)(x+y)^k = \\ (x+y)\left[x^k + \binom{k}{1}x^{k-1}y + \binom{k}{2}x^{k-2}y^2 + \cdots + \binom{k}{k-2}x^2y^{k-2} + \binom{k}{k-1}xy^{k-1} + y^k\right] = \\ x^{k+1} + \binom{k}{1}x^ky + \binom{k}{2}x^{k-1}y^2 + \cdots + \binom{k}{k-2}x^3y^{k-2} + \binom{k}{k-1}x^2y^{k-1} + xy^k + \\ x^ky + \binom{k}{1}x^{k-1}y^2 + \binom{k}{2}x^{k-2}y^3 + \cdots + \binom{k}{k-2}x^2y^{k-1} + \binom{k}{k-1}xy^k + y^{k+1} = \\ x^{k+1} + [\binom{k}{1} + 1]x^ky + [\binom{k}{2} + \binom{k}{1}]x^{k-1}y^2 + \cdots + [\binom{k}{r} + \binom{k}{r-1}]x^{k-r+1}y^r + \cdots + y^{k+1}.\end{gathered}$$

Untuk melengkapi bukti bahwa

$$(x+y)^{k+1} = x^{k+1} + \binom{k+1}{1}x^ky + \binom{k+1}{2}x^{k-1}y^2 + \cdots + \binom{k+1}{k-1}x^2y^{k-1} + \binom{k+1}{k}xy^k + y^{k+1}$$

cukup dibuktikan **Identitas Pascal**

$$\binom{k}{r} + \binom{k}{r-1} = \binom{k+1}{r}$$

sebagaimana berikut.

$$\begin{aligned}\binom{k}{r} + \binom{k}{r-1} &= \frac{k!}{r!(k-r)!} + \frac{k!}{(r-1)!(k-r+1)!} \\ &= \frac{k!(k-r+1) + rk!}{r!(k-r+1)!} \\ &= \frac{(k+1)!}{(k-r+1)!} \\ &= \binom{k+1}{r}.\end{aligned}$$

Lengkap sudah bukti. ✓

Contoh 1.3.6 (**Segitiga Pascal**)
Identitas Pascal yang telah dibuktikan mendasari konstruksi dari **Segitiga Pascal** yang sangat dikenal:

							1											baris ke − 0
						1			1									baris ke − 1
					1			2			1							baris ke − 2
				1			3			3			1					baris ke − 3
			1			4			6			4			1			baris ke − 4
		1			5			10			10			5			1	baris ke − 5
1	k	$\binom{k}{2}$	$\binom{k}{3}$		$\cdots$		$\cdots$		$\cdots$			$\binom{k}{k-3}$	$\binom{k}{k-1}$	k	1	baris ke−k		

Algorithma Pembagian

Kita semua sudah akrab sejak Sekolah Dasar dengan proses pembagian, yaitu diberikan bilangan bulat a selalu dapat direpresentasikan sebagai jumlah dari suatu kelipatan bilangan bulat lain yang diberikan yaitu $b \geq 1$ ditambah suatu sisa yang lebih kecil dari b. Hal ini akan terlihat pada teorema berikut yang dijamin oleh prinsip keterutan secara baik.

Contoh 1.3.7 Berikut ini penyajian hasil dari proses pembagian dari beberapa pasang bilangan bulat.
Untuk 84 dan 60 didapat $84 = 1 \cdot 60 + 24$.
Untuk 924 dan 105 didapat $924 = 8 \cdot 105 + 84$.
Untuk -10 dan 3 didapat $-10 = -4 \cdot 3 + 2$.
Masing-masing kasus bilangan yang pertama merupakan kelipatan dari bilangan yang kedua tambah suatu bilangan bulat yang lebih kecil dari bilangan yang kedua.

Teorema 1.3.4 (**Algorithma Pembagian**) Misalkan a adalah sebarang bilangan bulat dan b juga sebarang bilangan bulat tetapi $b \geq 1$. Maka ada dengan tunggal bilangan bulat q dan r yang memenuhi

(1) $a = qb + r$

(2) $0 \leq r < b$.

Bukti Misalkan $P = \{a - kb \,|\, k \in \mathbb{Z} \text{ dan } a - kb \geq 0\}$. Bila $a \geq 0$, maka $a \in P$ (sebab $a = a - 0 \cdot b$). Bila $a < 0$, maka $a - 2a \cdot b > 0$. Jadi $a - 2a \cdot b \in P$, dengan demikian $P \neq \emptyset$. Gunakan aksiomatik keterurutan secara baik dari bilangan bulat positip didapat: Ada $r \in P$ dengan r adalah elemen terkecil. Karena $r \in P$, maka $r = a - qb$ untuk beberapa $q \in \mathbb{Z}$ atau $a = qb + r$ (memenuhi (1)) dan $r \geq 0$. Tinggal menunjukkan bahwa $r < b$. Andaikan $r \not< b$ yang berarti $r \geq b$, didapat

$$0 \leq r - b = (a - qb) - b = a - \underbrace{(q+1)}_{k} b \in P,$$

tetapi $(r - b) < r$, ini menunjukkan bahwa ada bilangan bulat positip yang lebih kecil dari r berada di P. Hal ini bertentangan bahwa r adalah elemen terkecil di P. Jadi haruslah $r < b$. Dengan demikian (2) dipenuhi, yaitu r memenuhi $0 \leq r < b$. Tinggal menunjukkan bahwa

q dan r tunggal. Misalkan q_1 dan r_1 adalah bilangan bulat yang memenuhi $a = q_1 b + r_1$. Didapat

$$a = qb + r = q_1 b + r_1,$$

dimana $0 \leq r < b$ dan $0 \leq r_1 < b$. Maka $r_1 - r = qb - q_1 b = b(q - q_1)$, sebagai akibat

$$|r_1 - r| = |b(q - q_1)| = |b|\,|q - q_1| = b|q - q_1|. \tag{1.1}$$

Tambahkan dua pertidaksamaan $-b < -r \leq 0$ dan $0 \leq r_1 < b$, didapat

$$-b < r_1 - r < b, \quad \text{atau} \quad |r_1 - r| < b.$$

Berdasarkan Persamaan 1.1, maka $b|q - q_1| < b$. Sehingga didapat

$$0 \leq |q - q_1| < 1.$$

Karena $|q - q_1|$ adalah bilangan bulat positip taknegatip dan memenuhi $0 \leq |q - q_1| < 1$, maka haruslah $q - q_1 = 0$ atau $q = q_1$. Dengan demikian didapat $q_1 b + r_1 = qb + r$, yaitu $r_1 = r$. Jadi terbukti bahwa q dan r adalah tunggal.

Bilanga q dalam Teorema 1.3.4 dinamakan **hasil bagi** sedangkan r dinamakan **sisa** pada pembagian a dibagi oleh b.

Akibat 1.3.1 Bila $a, b \in \mathbb{Z}$ dengan $b \neq 0$, maka ada tunggal bilangan bulat q dan r yang memenuhi

$$a = qr + b, \quad 0 \leq r < |b|.$$

Bukti Mengikuti bukti Teorema 1.3.4, cukup dibuktikan untuk kasus b adalah negatif. Maka $|b| > 0$ atau $|b| \geq 1$. Dengan demikian menurut Teorema 1.3.4 ada dengan tunggal bilangan bulat q_1 dan r yang memenuhi

$$a = q_1|b| + r, \quad 0 \leq r < |b|.$$

Karena $|b| = -b$, maka bisa diplih $q = -q_1$, sehingga didapat

$$a = q_1|b| = (-q)(-b) + r = qb + r, \quad 0 \leq r < |b|.$$

Definisi 1.3.1 Diberikan dua bilangan bulat a dan b, dengan $a \neq 0$ dikatakan bahwa a adalah **pembagi** dari b ditulis $a|b$, bila $b = ac$ untuk beberapa bilangan bulat c. Bila a tidak membagi b, maka ditulis $a \nmid b$. Catatan bahwa dibolehkan bahwa $a \leq 0$ dalam definisi ini.

Beberapa akibat langsung dari Definisi 1.3.1 diberikan dalam teorema berikut.

Teorema 1.3.5 Diberikan $a, b, c \in \mathbb{Z}$. Maka

1. $a|0, 1|a, a|a$,
2. $a|\pm 1$ bila dan hanya bila $a = \pm 1$,
3. bila $a|b$, maka $ac|bc$,
4. bila $a|b$ dan $b|c$, maka $a|c$,

5. $a|b$ dan $b|a$ bila dan hanya bila $a = \pm b$,

6. bila $c|a$ dan $c|b$, maka $c|(ax + by)$ untuk setiap $x, y \in \mathbb{Z}$.

Bukti Sebagai latihan.

Definisi 1.3.2 Diberikan dua bilangan bulat a dan b, suatu bilangan bulat d yang memenuhi kondisi $d|a$ dan $d|b$ dinamakan suatu **pembagi persekutuan** dari a dan b.

Contoh 1.3.8 Dua bilangan bulat 252 dan 180 mempunyai pembagi persekutuan positip: $1, 2, 3, 4, 6, 9, 12, 18$ dan 36. Tidak ada bilangan bulat positip yang lebih besar dari 36 yang merupakan pembagi persekutuan dari 252 dan 180.

Pada pembahasan berikutnya akan sering tertarik untuk mencari pembagi persekutuan terbesar dari dua bilangan bulat.

Definisi 1.3.3 Diberikan dua bilangan bulat a dan b keduanya taknol, **pembagi persekutuan terbesar** dari a dan b adalah suatu bilangan bulat $d \geq 1$ yang memenuhi

(1) $d|a$ dan $d|b$.

(2) Untuk sebarang bilangan bulat c, bila $c|a$ dan $c|b$, maka $c|d$.

Dalam hal ini ditulis $d = \text{fpb}(a, b)$.

Secara ringkas, fpb(a, b) adalah bilangan bulat terbesar di dalam himpunan dari semua pembagi persekutuan terbesar dari a dan b.

Suatu pertanyaan yang wajar adalah apakah bilangan bulat a dan b bisa mempunyai pembagi-pembagi persekutuan terbesar yang berbeda. Untuk menjawab pertanyaan ini, misalkan ada dua bilangan bulat positip d dan d_1 yang merupakan fpb(a, b). Maka berdasarkan Definisi 1.3.3 bagian (2) didapat $d|d_1$ juga $d_1|d$. Dengan demikian, berdasarkan Teorema 1.3.5 bagian (5), maka $d = \pm d_1$. Karena d dan d_1 keduanya adalah bilangan bulat positip, maka $d = d_1$. Jadi bila fpb(a, b) ada, maka keberadaannya adalah tunggal.

Algorithma pembagian beserta aplikasi yang lain dari prinsip keterurutan secara baik, menjamin keujudan dari fpb(a, b), sebagaimana diberikan oleh teorema berikut.

Teorema 1.3.6 Misalkan a dan b adalah bilangan bulat keduanya taknol. Maka

(1) $d = \text{fpb}(a, b)$ ada (exist).

(2) Ada bilangan bulat u dan v yang memenuhi $d = ua + vb$.

Bukti Misalkan $S = \{xa + yb | x, y \in \mathbb{Z} \text{ dan } xa + yb \geq 1\}$. Karena $S \neq \emptyset$ sebab $aa + bb \in S$ dan $S \subseteq \mathbb{N}$. Dengan menggunakan prinsip keterurutan secara baik S mempunyai elemen terkecil d. Karena $d \in S$ didapat $d = sa + tb$ untuk beberapa $s, t \in \mathbb{Z}$ dan $d \geq 1$. Bila k adalah suatu pembagi persekutuan dari a dan b, maka $a = uk$ dan $b = vk$ untuk beberapa $u, v \in \mathbb{Z}$. Didapat $d = sa + tb = (su + tv)k$, yaitu k membagi d. Selanjutnya ditunjukkan bahwa $d = \text{fpb}(a, b)$, hanya diperlukan d pembagi persekutuan dari a dan b. Gunakan algoritma pembagian didapat $a = qd + r$ dengan $0 \leq r = a - qd = a - q(sa + tb) = (1 - qs)a + (-qt)b < d$. Karena d elemen terkecil di S, maka tidak akan $r \geq 1$. Jadi haruslah $r = 0$. dengan demikian $a = qd$ atau d adalah pembagi dari a. Dengan cara yang sama dapat ditunjukkan bahwa d juga pembagi dari b. Dengan demikian sudah terbukti bahwa $d = \text{fpb}(a, b)$.

Teorema 1.3.6 bagian (1) menjamin keujudan dari fpb(a,b), sedangkan pada bagian (2) menyatakan bahwa fpb(a,b) dapat diungkapkan sebagai suatu **kombinasi linier** dari a dan b yaitu $ua + vb$. Mungkin pada awal yang terlihat saat ini kurang menarik, namun nanti pada kenyataannya ternyata **sangat berguna**.

Contoh 1.3.9 Apa yang diberikan dalam contoh ini menggambarkan bagaimana menghitung faktor persekutuan terbesar untuk kasus sederhana. Faktor persekutan terbesar dari 84 dan 60 didapat dengan berulang kali menerapkan algoritma pembagian, sebagai berikut:

$$\begin{aligned} 84 &= 1 \cdot 60 + 24 \\ 60 &= 2 \cdot 24 + 12 \\ 24 &= 2 \cdot 12 + 0. \end{aligned}$$

Dari persamaan ke-3 terlihat bahwa $12|12$ dan $12|24$. Sehingga berakibat pada persamaan ke-2 yaitu $12|60$. Dan karena $12|24$ dan $12|60$, maka persamaan ke-1 berakibat $12|84$. Jadi 12 adalah pembagi persekutuan dari 84 dan 60. Bila selain 12, d' juga pembagi persekutuan dari 84 dan 60, maka dari persamaan pertama $d'|60$ dan $d'|24$. Sehingga dari persamaan kedua berakibat $d'|24$ dan $d'|12$. Jadi $12 = \text{fpb}(86, 60)$. ●

Proposisi 1.3.1 (**Algorithma Euclide**) Untuk sebarang pasangan bilngan bulat a dan $b \geq 1$ dapat dilakukan penghitungan fpb(a,b) dengan melakukan algoritma pembagian secara berulang sebagai berikut:

$$\begin{aligned} a &= q_1 b + r_1 && \text{dimana } 0 \leq r_1 < b \\ b &= q_2 r_1 + r_2 && \text{dimana } 0 \leq r_2 < r_1 \\ r_1 &= q_3 r_2 + r_3 && \text{dimana } 0 \leq r_3 < r_2, \\ &\vdots \end{aligned}$$

berhenti ketika diperoleh sisa pembagian sama dengan nol:

$$\begin{aligned} r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} && \text{dimana } 0 \leq r_{n-1} < r_{n-2} \\ r_{n-2} &= q_n r_{n-1} + r_n && \text{dimana } 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Sisa pembagian terakhir taknol $r_n = \text{fpb}(a,b)$. Metoda perhitungan fpb(a,b) ini dinamakan **Algorithma Euclide**.

Bukti Hasil akhir sisa pembagian adalah nol, dengan menggunakan prinsip keterutan secara baik berakibat bahwa himpunan semua sisa yang positip harus mempunyai suatu elemen terkecil. Karena barisan sisa pembagian positip $r_1 > r_2 > r_3 > \cdots$ adalah barisan turun, maka sisa pembagian positip terkecil adalah sisa pembagian terakhir, yang mana sisa pembagian berikutnya adalah nol. Dalam hal ini r_n adalah sisa pembagian positip yang terakhir, maka

$$\begin{aligned} \text{fpb}(a,b) = \text{fpb}(b,r_1) = \text{fpb}(r_1,r_2) = \cdots = \text{fpb}(r_{i-1},r_i) = \cdots &= \text{fpb}(r_{n-2},r_{n-1}) \\ &= \text{fpb}(r_{n-1},r_n) \\ &= r_n. \end{aligned}$$

✓

Contoh 1.3.10 Hitung fpb(924, 105). Perhitungan dilakukan sebagai berikut:

$$\begin{aligned} 924 &= 8 \cdot 105 + 84 \\ 105 &= 1 \cdot 84 + 21 \\ 84 &= 4 \cdot 21 + 0. \end{aligned}$$

Jadi fpb(924, 105) = 21. Dari persamaan kedua didapat $21 = 105 - 84$. Dari persamaan yang pertama didapat $84 = 924 - 8 \cdot 105$. Gabungkan hasil pertama dengan kedua didapat

$$21 = 105 - (924 - 8 \cdot 105) = \boxed{-1} \cdot 924 + \boxed{9} \cdot 105.$$

Terihat bahwa fpb adalah sebagai suatu kombinasi linier $\boxed{u} \cdot 924 + \boxed{v} \cdot 105$ dimana $u = -1$ dan $v = 9$.

Catatan, bilangan bulat u dan v yang memenuhi fpb$(a, b) = ua + vb$ adalah tidak tunggal. Misalnya, bila $a = 90$ dan $b = 252$, maka

$$\text{fpb}(90, 252) = 18 = (3)90 + (-1)252.$$

dan

$$\text{fpb}(90, 252) = 18 = (3 + 252)90 + (-1 - 90)252 = (255)90 + (-91)252.$$

Teorema Dasar Aritmatika

Konsekuensi lain yang penting dari algoritma pembagian dan prinsip keterutan secara adalah setiap bilangan bulat $n > 1$ dapat ditulis sebagai produk dari bilangan prima, yaitu bilangan bulat yang tidak dapat ditulis sebagai produk dengan cara taktrivial.

Contoh 1.3.11 Misalkan dihitung fpb(385, 48) sebagai berikut:

$$\begin{aligned} 385 &= 8 \cdot 48 + 1 \\ 48 &= 48 \cdot 1 + 0. \end{aligned}$$

Terlihat bahwa fpb(385, 48) = 1, dengan kata lain bilangan bulat positip yang terbesar dan hanya satu bilangan ini yaitu 1 yang bisa membagi 385 dan 48.

Definisi 1.3.4 Dua bilangan bulat a dan b dikatakan **prima relatif** bila fpb$(a, b) = 1$ dengan kata lain pembagi persekutuan positip dari a dan b hanya bilangan bulat 1. Suatu bilangan bulat $p > 1$ dinamakan **prima** bila pembagi positipnya adalah 1 dan dirinya sendiri.

Proposisi berikut sebagai akibat dari Teorema 1.3.6 bagian (2).

Proposisi 1.3.2 Misalkan a dan b adalah prima relatif dan c adalah suatu bilangan bulat. Maka

(1) Sebarang pembagi persekutuan dari a dan bc adalah suatu pembagi persekutuan dari a dan c.

(2) Bila a membagi bc, maka a membagi c.

(3) Bila a dan c adalah prima relatif, maka a dan bc prima relatif.

Bukti Misalkan fpb$(a,b) = 1$ dan misalkan $d \mid a$ dan $d \mid bc$. Maka, dengan menggunakan Teorema 1.3.6 didapat $1 = sa + tb$ untuk suatu bilangan bulat s dan t, juga $a = dx$ dan $b = dy$ untuk suatu bilangan bulat x dan y. Dengan demikian didapat

$$c = c \cdot 1 = c(sa + tb) = acs + bct = dxcs + dyt = d(xcs + yt),$$

terlihat bahwa $d|c$ sebagaimana dibutuhkan untuk membuktikan (1). Misalkan bahwa $a|bc$, maka $bc = ad'$ untuk suatu bilangan bulat d' dan

$$c = c \cdot 1 = c(sa + tb) = acs + bct = acs + ad't = a(cs + d't),$$

terlihat bahwa $a \mid c$ sebagaimana diharapkan bukti bagian (2). Dari (1), d adalah pembagi persekutuan dari a dan bc dan juga pembagi persekutuan dari a dan c. Bila a dan c adalah prima relatif, maka fpb$(a,c) = 1 = d$. Hal ini berakibat juga fpb$(a,bc) = 1$. Jadi a dan bc adalah prima relatif. ✓

Sebagai akibat langsung adalah kesimpulan penting berikut.

Akibat 1.3.2 (**Lemma Euclide**) Misalkan b dan c adalah bilangan bulat. Bila p adalah prima dan $p|bc$, maka $p|b$ atau $p|c$.

Bukti Jika $p|b$, maka tidak ada yang perlu dibuktikan. Jika tidak $p|b$, maka fpb$(p,b) = 1$. Hal ini berakibat bahwa $1 = xp + yb$ untuk suatu bilangan bulat x dan y. Dari $1 = xp + yb$ didapat $c = xpc + ybc$. Jelas bahwa $p|xpc$ dan $p|ybc$ (hipotisis bahwa $p|bc$). Jadi $p|c$. ✓

Contoh 1.3.12 Adalah sangat penting dalam Lemma Euclid bahwa p adalah prima. Misalkan sebagai mana diketahui bahwa 6 membagi $3 \cdot 4 = 12$ tetapi $6 \nmid 3$ dan $6 \nmid 4$. ●

Untuk membuktikan Teorema Fundamental Aritmatika dibutuhkan Lemma Euclide dalam suatu bentuk yang lebih umum, sebagaimana kesimpulan berikut.

Akibat 1.3.3 Misalkan $b_1, b_2, \ldots, b_r$ adalah bilangan bulat. Bila p adalah prima dan $p \mid b_1, b_2, \ldots, b_r$, maka $p|b_i$ untuk beberapa i, dengan $1 \leq i \leq r$.

Bukti Digunakan induksi matematika pada r. Untuk $r = 1$, jelas dipenuhi. Kasus $r = 2$ adalah Lemma Euclide. Selanjutnya misalkan pernyataan benar untuk $r = k$ dan $p|(b_1, b_2, \ldots, b_k)b_{k+1}$. Gunakan Akibat 1.3.2 (Lemma Euclide), didapat salah satu dari $p|b_{k+1}$ hal ini sebagaimana diinginkan atau $p|b_1, b_2, \ldots, b_k$, dengan menggunakan hipotesis induksi $p|b_i$ untuk beberapa i, dengan $1 \leq i \leq k$. ✓

Teorema 1.3.7 (Fundamental Aritmatika) Misalkan n adalah suatu bilangan bulat dengan $n > 1$. Maka

(1) n adalah salah satu dari prima atau suatu produk dari prima.

(2) Faktorisasi dari n dalam suatu produk dari prima adalah tunggal, kecuali untuk urutan primanya. Yaitu, bila

$$n = p_1 p_2 \cdots p_r \text{ dan } n = q_1 q_2 \cdots q_s,$$

yang mana p_i dan q_j adalah prima, maka $r = s$ dan, bila perlu dengan melakukan pengurutan kembali didapat $p_i = q_i$ untuk semua i.

Bukti Untuk membuktikan (1) dan (2) digunakan induksi matematika pernyataan benar untuk $n \geq 2$.

(1) Untuk $n = 2$, pernyataan (1) dipenuhi, sebab 2 adalah prima. Untuk membuktikan (1) dipenuhi untuk n, asumsikan bahwa (1) benar untuk sebarang bilangan bulat k dengan $2 \leq k < n$. Bila n adalah prima adalah sebagaimana diinginkan. Bila n bukan prima, pilih bilangan bulat u dan v dengan $1 < u, v < n$ yang memenuhi $uv = n$. Dengan hipotesis induksi masing-masing u dan v salah satu dari prima atau bisa dituliskan sebagai produk dari prima. Didapat, $n = uv$ dapat dituliskan sebagai produk dari prima.

(2) Untuk $n = 2$, pernyataan (2) jelas dipenuhi, sebab 2 adalah prima yang tidak bisa dituliskan sebagai produk prima yang lainnya yang lebih besar dari 2. Jadi untuk membuktikan n memenuhi pernyataan (2) diasumsikan (2) dipenuhi untuk sebarang k dimana $2 \leq k < n$. Misalkan

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

Terlihat bahwa $p_1 \mid n$, maka $p_1 \mid q_1 q_2 \cdots q_s$. Dengan menggunakan Akibat 1.3.3 didapat $p_1 \mid q_i$ untuk beberapa i dengan $1 \leq i \leq s$. Bila diperlukan, dilakukan pengurutan kembali pada q_i sehingga q_j ini menjadi q_1. Dengan demikian didapat $p_1 \mid q_1$. Karena q_1 prima haruslah $p_1 = q_1$. Selanjutnya misalkan $k = n/p_1 = n/q_1 < n$, didapat

$$k = p_2 \cdots p_r = q_2 \cdots q_s.$$

Lakukan lagi proses hipotesis induksi secara berulang. Dengan demikian didapat banyaknya bilangan prima pada masing-masing faktor harus sama, yaitu $r - 1 = s - 1$, akibatnya $r = s$. Jadi $p_i, 2 \leq i \leq r$ dan $q_j, 2 \leq j \leq r$ harus sama kecuali hanya pada urutannya. ✓

Terema Fundamental Aritmatika yang baru saja dibuktikan berakibat bahwa diberikan sebarang bilangan bulat $n > 1$, maka n dapat ditulis sebagai produk

$$p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

dimana p_i adalah bilangan prima berbeda untuk masing-masing i dan, p_i ini dan pangkat-pangkatnya a_i adalah tunggal. Bila bilangan-bilangan bulat dituliskan dalam cara tersebut, maka mudah untuk memperoleh pembagi persekutuan terbesaranya, sebagaimana diberikan oleh contoh berikut.

Contoh 1.3.13 Sebagaimana telah dibahas dalam Contoh 1.3.10, fpb$(924, 105) = 21$. Tetapi $924, 105$ dan 21 dapat difaktorkan kedalam bentuk pangkat dari bilangan prima sebagai berikut:

$$924 = 2^2 \cdot 3^1 \cdot 7^1 \cdot 11^1 \qquad 105 = 3^1 \cdot 5^1 \cdot 7^1 \qquad 21 = 3^1 \cdot 7^1.$$

Sekedar untuk membandingkan, ditulis lagi

$$924 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1 \qquad 105 = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^0$$
$$21 = 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0.$$

Terlihat bahwa yang mana saja pangkat pada bilangan prima dalam faktorisasi 21 lebih kecil dari pangkat pada bilangan prima yang sama dalam faktorisasi dari 924 dan 105. Sebaliknya, bila diambil pangkat-pangkat yang lebih besar, maka didapat bilangan

$$2^2 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 4620.$$

Sebagaiman telah diketahui bahwa 21 adalah pembagi persekutuan terbesar dari 924 dan 105, sebaliknya 4620 adalah kelipatan persekutuan terkecil dari 924 dan 105.

Definisi 1.3.5 Diberikan dua bilangan bulat n dan m keduanya taknol, **kelipatan persekutuan terkecil** dari n dan m adalah bilangan bulat $l \geq 1$ yang memenuhi

(1) $n|l$ dan $m|l$.

(2) Untuk sebarang bilangan bulat k, bila $n|k$ dan $m|k$, maka $l|k$.

Dalam hal ini ditulis $l = \text{kpk}(n, m)$.

Proposisi 1.3.3 Diberikan

$$n = p_1^{a_1} p_2^{a_2} \cdot p_k^{a_k} \text{ dan } m = p_1^{b_1} p_2^{b^2} \cdots p_k^{b^k},$$

dimana p_i bilangan prima berbeda dan $a_i, b_i \geq 0$, maka

(1) $\text{fpb}(n, m) = p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$, dimana $c_i = \min\{a_i, b_i\}$,

(2) $\text{kpk}(n, m) = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$, dimana $d_i = \max\{a_i, b_i\}$,

(3) $\text{kpk}(n, m) \cdot \text{fpb}(n, m) = nm$.

Bukti Sebagai latihan.

Bilangan Bulat modulo n

Untuk mengakhiri bagian ini dibahas kembali topik relasi ekivalen. Yaitu relasi ekivalen yang khusus pada $\mathbb{Z}$ yang mana sifat-sifat $\mathbb{Z}$ ini telah dibahas sebelumnya.

Definisi 1.3.6 Misalkan $n > 0$ adalah sebarang bilangan bulat tetapi tetap. Untuk sebarang dua bilangan bulat a dan b adalah **kongruen mod** n ditulis

$$a \equiv b \mod n$$

bila $n|(a - b)$.

Proposisi 1.3.4

(1) Relasi kongruen $\mod n$ adalah suatu relasi ekivalen pada $\mathbb{Z}$

(2) Relasi ekivalen tersebut mempunyai tepat sebanyak n klas ekivalen yaitu

$$n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}.$$

(3) Bila $a \equiv b \mod n$ dan $c \equiv d \mod n$, maka

$$a + c \equiv b + d \mod n \qquad ac \equiv bd \mod n.$$

(4) Bila a dan n prima relatif, maka

$$ab \equiv ac \mod n \text{ berakibat } b \equiv c \mod n.$$

Bukti

(1) Untuk semua $a, b, c \in \mathbb{Z}$ didapat $a \equiv a \mod n$ sebab $n|0 = (a - a)$. Selanjutnya, bila $a \equiv b \mod n$, maka $n|(a - b) = -(b - a)$. Jadi $b \equiv a \mod n$. Berikutnya, bila $a \equiv b \mod n$ dan $b \equiv c \mod n$, maka $n|(a - b)$ dan $n|(b - c)$. Jadi $n|((a - b) + (b - c)) = (a - c)$. Terlihat bahwa $n|(a - c)$ atau $a \equiv c \mod n$.

(2) Untuk sebarang $a \in \mathbb{Z}$, misalkan $[a]_n$ adalah klas ekivalen dari $a \in \mathbb{Z}$. Dengan menggunakan algoritma pembagian didapat $a = qn + r$ untuk beberapa $q, r \in \mathbb{Z}$ dengan $0 \leq r < n$. Terlihat bahwa $a \equiv r \mod n$. Jadi $[a]_n = [r]_n$. Jadi hanya ada n klas ekivalen yaitu:

$$0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}.$$

Semuanya berbeda, sebab untuk r dan s dengan $0 \leq r, s < n$ didapat $n|(r - s)$ bila dan hanya bila $r = s$.

(3) Bila $a \equiv b \mod n$ dan $c \equiv d \mod n$, maka $n|(a - b)$ dan $n|(c - d)$. Didapat

$$n|((a - b) + (c - d)) = (a + c) - (b + d).$$

Terlihat bahwa $a + b \equiv b + d \mod n$. Juga

$$n|(c - b) \Rightarrow n|(ac - bd).$$

Terlihat bahwa $ac \equiv bd \mod n$.

(4) Bila a dan n prima relatif dan $ab \equiv ac \mod n$, maka

$$n|(ab - ac) = a(b - c),$$

berdasarkan Proposisi 1.3.2 bagian (2), maka $n|(b - c)$. Jadi $b \equiv c \mod n$.

Contoh 1.3.14 Diberikan himpunan klas kongruen mod 5, yaitu

$$\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]\}.$$

Proposisi 1.3.4 menjamin bahwa bila $[r_1]_5 = [r_2]_5$ dan $[s_1]_5 = [s_2]_5$, maka $[r_1 + s_1] = [r_2 + s_2]$. Dengan demikian bahwa dapat didefinisikan operasi tambah oleh $[r]_5 + [s]_5 = [r + s]_5$. Dengan cara yang sama didapat $[r_1 s_1]_5 = [r_2 s_2]_5$. Dengan demikian dapat didefinisikan operasi perkalian oleh $[r]_5[s]_5 = [rs]_5$. Hasil operasi tambah dan perkalian pada $\mathbb{Z}_5$ diberikan oleh tabel berikut.

Tabel 1: Penjumlahan mod 5

+	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

Tabel 2: Perkalian mod 5

×	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Definisi 1.3.7 Untuk sebarang $n > 0$, misalkan

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$$

adalah himpunan klas kongruen mod n. Sebagaimana pada contoh sebelumnya, Proposisi 1.3.4 menjamin bahwa operasi **penjumlahan** dan **perkalian** mod n

$$[r]_n + [s]_n = [r+s]_n \text{ dan } [r]_n[s]_n = [rs]_n$$

adalah terdefinisi secara baik di $\mathbb{Z}_n$, karena bila $[r_1]_n = [r_2]_n$ dan $[s_1]_n = [s_2]_n$ di $\mathbb{Z}_n$, maka

$$[r_1]_n + [s_1]_n = [r_1 + s_1]_n = [r_2 + s_2]_n = [r_2]_n + [s_2]_n$$

dan

$$[r_1]_n[s_1]_n = [r_1 s_1]_n = [r_2 s_2]_n = [r_2]_n[s_2]_n.$$

Himpunan $\mathbb{Z}_n$ dengan operasi tersebut dinamakan **bilangan bulat mod** n.

Proposisi berikut kumpulan beberapa sifat dasar dari tambah dan perkalian dalam bilangan bulat modulo n.

Proposisi 1.3.5 Untuk setiap $[r]_n, [s]_n$ dan $[t]_n$ di $\mathbb{Z}_n$ didapat

(1) Komutatif
$[r]_n + [s]_n = [s]_n + [r]_n \qquad [r]_n[s]_n = [s]_n[r]_n.$

(2) Assosiatif
$[r]_n + ([s]_n + [t]_n) = ([r]_n + [s]_n) + [t]_n \qquad [r]_n([s]_n[t]_n) = ([r]_n[s]_n)[t]_n.$

(3) Distributif
$[r]_n([s]_n + [t]_n) = [r]_n[s]_n + [r]_n[t]_n.$

(4) Identitas
$[0]_n + [r]_n = [r]_n = [r]_n + [0]_n \qquad [1]_n[r]_n = [r]_n[1]_n.$

Bukti

(1) Komutatif

$$[r]_n + [s]_n = [r+s]_n = [s+r]_n = [s]_n + [r]_n,$$
$$[r]_n[s]_n = [rs]_n = [sr]_n = [s]_n[r]_n.$$

(2) Assosiatif

$$\begin{aligned}[r]_n + ([s]_n + [t]_n) &= [r]_n + ([s+t]_n) \\ &= [r + (s+t)]_n = [(r+s)+t]_n \\ &= ([r+s]_n) + [s]_n \\ &= ([r]_n + [s]_n) + [t]_n,\end{aligned}$$

$$[r]_n([s]_n[t]_n) = [r]_n([st]_n) = [r(st)]_n = [(rs)t]_n = ([rs]_n)[t]_n = ([r]_n[s]_n)[t]_n.$$

(3) Distributif

$$\begin{aligned}[r]_n([s]_n + [t]_n) &= [r]_n([s+t]_n) \\ &= [r(s+t)]_n \\ &= [rs + rt]_n \\ &= [rs]_n + [rt]_n \\ &= [r]_n[s]_n + [r]_n[t]_n.\end{aligned}$$

(4) Identitas

$$\begin{aligned}[0]_n + [r]_n &= [0 + r]_n \\ &= [r]_n \\ &= [r + 0]_n \\ &= [r]_n + [0]_n\end{aligned}$$

$$[1]_n[r]_n = [1 \cdot r]_n = [r]_n = [r \cdot 1]_n = [r]_n[1]_n.$$ ✓

Contoh 1.3.15 Diberikan $\mathbb{Z}_{10} = \{[0]_{10}, [1]_{10}, \ldots, [9]_{10}\}$, misalkan himpunan bagian

$$\begin{aligned}\mathbb{U}(10) &= \{[n]_{10} \in \mathbb{Z}_{10} \mid \text{fpb}(n, 10) = 1\} \\ &= \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}\end{aligned}$$

Tabel hasil perkalian mod 10 untuk $\mathbb{U}_{10}$ diberikan sebagai berikut:

Tabel 3 Perkalian dalam $\mathbb{U}(10)$

$\times$	$[1]_{10}$	$[3]_{10}$	$[7]_{10}$	$[9]_{10}$
$[1]_{10}$	$[1]_{10}$	$[3]_{10}$	$[7]_{10}$	$[9]_9$
$[3]_{10}$	$[3]_{10}$	$[9]_{10}$	$[1]_{10}$	$[7]_{10}$
$[7]_{10}$	$[7]_{10}$	$[1]_{10}$	$[9]_{10}$	$[3]_{10}$
$[9]_{10}$	$[9]_{10}$	$[7]_{10}$	$[3]_{10}$	$[1]_{10}$

Hasil penghitungan Tabel 3, memperlihatkan bahwa bila $[r]_{10}, [s]_{10} \in \mathbb{U}(10)$, maka $[r]_{10}[s]_{10} \in \mathbb{U}(10)$. Alasan ini bisa dilihat pada proposisi berikutnya. Juga, didapat bahwa untuk sebarang $[r]_{10} \in \mathbb{U}(10)$ ada suatu $[s]_{10} \in \mathbb{U}(10)$ sedemikian hingga $[r]_{10}[s]_{10} = [1]_{10}$. Alasannya adalah bila $\text{fpb}(r, 10) = 1$, maka menurut Teorema 1.3.6 kita mempunyai $rs + 10t = 1$ untuk beberapa bilangan bulat s dan t. Hal ini berarti bahwa $rs \equiv 1 \mod 10$ atau $[rs]_{10} = [r]_{10}[s]_{10} = [1]_{10}$. ●

Definisi 1.3.8 Diberikan $\mathbb{Z}_n$ dan

$$\mathbb{U}(n) = \{[u]_n \in \mathbb{Z}_n \,|\, \text{fpb}(u,n) = 1\} \subset \mathbb{Z}_n.$$

Elemen-elemen di $\mathbb{U}(n)$ dinamakan **unit mod n**.

Proposisi 1.3.6 Untuk sebarang $[r]_n, [s]_n \in \mathbb{U}(n)$ didapat $[r]_n[s]_n \in \mathbb{U}(n)$.

Bukti Bila $[r]_n, [s]_n \in \mathbb{U}(n)$, maka $\text{fpb}(n,s) = \text{fpb}(n,r) = 1$. Dengan menggunakan Proposisi 1.3.2 bagian (3) kita mendapatkan $\text{fpb}(n,rs) = 1$. Dengan demikian $[rs]_n \in \mathbb{U}(n)$ atau $[r]_n[s]_n \in \mathbb{U}(n)$.

Proposisi 1.3.7 Untuk sebarang $[r]_n \in \mathbb{U}(n)$ ada suatu $[s]_n \in \mathbb{U}(n)$ yang memenuhi

$$[r]_n[s]_n = [1]_n.$$

Bukti Bila $[r]_n \in \mathbb{U}(n)$, maka $\text{fpb}(n,r) = 1$. Dengan menggunakan Teorema 1.3.6 didapat $rs + nt = 1$ untuk suatu bilangan bulat s dan t. Tetapi hal ini berakibat bahwa $rs \equiv 1 \mod n$ atau $[rs]_n = [1]_n$. Tetapi sebagaimana telah diketahui $[rs]_n = [r]_n[s]_n$, dengan demikian didapat $[r]_n[s]_n = [1]_n$.

Dari pembahasan Proposisi 1.3.6 dan 1.3.7 didapat kesimpulan berikut.

Akibat 1.3.4 Himpunan $\mathbb{U}(n)$ terhadap operasi perkalian memenuhi:

1. **Tertutup**, $[a]_n[b]_n \in \mathbb{U}(n),\ \forall [a]_n, [b]_n \in \mathbb{U}(n)$.
2. **Asosiatif**, untuk sebarang $[a]_n, [b]_n, [c]_n \in \mathbb{U}(n)$ berlaku:
$$([a]_n[b]_n)[c]_n = [a]_n([b]_n[c]_n).$$
3. Ada $[1]_n \in \mathbb{U}(n)$ memenuhi:
$$[1]_n[a]_n = [a]_n \text{ dan } [a]_n[1]_n = [a]_n,\ \forall [a]_n \in \mathbb{U}(n).$$
4. Untuk sebarang elemen $[r]_n \in \mathbb{U}(n)$ ada $[s]_n \in \mathbb{U}(n)$ yang memnuhi:
$$[r]_n[s]_n = [1]_n = [s]_n[r]_n.$$
5. Untuk sebarang $[a]_n, [b]_n \in \mathbb{U}(n)$ berlaku $[a]_n[b]_n = [b]_n[a]_n$.

Bukti
Berdasarkan Proposisi 1.3.6, maka $\mathbb{U}(n)$ terhadap operasi perkalian adalah tertutup. Selanjutnya, karena $\text{fpb}(1,n) = 1$, maka $[1]_n \in \mathbb{U}(n)$ dan memenuhi

$$[1]_n[a]_n = [1.a]_n = [a]_n \text{ dan } [a]_n[1]_n = [a.1]_n = [a]_n,\ \forall [a]_n \in \mathbb{U}(n).$$

Sifat asosiatif, jelas dipenuhi sebab untuk sebarang $[a]_n, [b]_n, [c]_n \in \mathbb{U}(n)$ berlaku:

$$([a]_n[b]_n)[c]_n = ([ab]_n)[c]_n = [(ab)c]_n = [a(bc)]_n = [a]_n([bc]_n) = [a]_n([b]_n[c]_n).$$

Berdasarkan Proposisi 1.3.7, setiap elemen $[r]_n \in \mathbb{U}(n)$ ada $[s]_n \in \mathbb{U}(n)$ yang memenuhi $[r]_n[s]_n = [1]_n = [s]_n[r]_n$. Akhirnya, juga untuk sebarang $[a]_n, [b]_n \in \mathbb{U}(n)$ berlaku:

$$[a]_n[b]_n = [ab]_n = [ba]_n = [b]_n[a]_n.$$

Latihan

Latihan 1.3.1 Dengan menggunakan induksi matematika pada n buktikan pernyataan berikut.

1. $1 + 2 + 3 + \cdots + n = n(n+1)/2$ untuk $n \geq 1$.
2. $1^2 + 2^2 + 3^2 + \cdots + n^2 = n(n+1)(2n+1)/6$ untuk $n \geq 1$.
3. $1^3 + 2^3 + 3^3 + \cdots + n^3 = n^2(n+1)^2/4$ untuk $n \geq 1$.
4. Bila $0 \leq x \leq y$, maka $x^n \leq y^n$ untuk $n \geq 0$.
5. $n < 2^n$ untuk $n \geq 0$.

Latihan 1.3.2 **Barisan Fibonacci** : $1, 1, 2, 3, 5, 8, 13, \ldots$ didefinisikan oleh

$$F_1 = F_2 + 1,\ F_{n+2} = F_{n+1} + F_n \text{ untuk } n \geq 1.$$

1. Tunjukkan bahwa $(F_{n+1})^2 - F_n F_{n+2} = (-1)^n$.
2. Tunjukkan bahwa $F_{n+1}F_{n+2} - F_n F_{n+3} = (-1)^n$.
3. Tunjukkan bahwa $F_n < 2^n$ untuk $n \geq 1$.

Latihan 1.3.3 Bila $a, r \in \mathbb{R}$ dan $r \neq 1$, tunjukkan bahwa untuk $n \geq 1$ memenuhi

$$a + ar + ar^2 + \cdots + ar^n = a(1 - r^{n+1})/(1 - r).$$

Latihan 1.3.4 Misalkan $P(n)$ adalah pernyataan tentang bilangan bulat positip dan n_0 adalah sebarang bilangan bulat positip. Asumsikan

(1) $P(n_0)$ adalah benar.

(2) Bila $P(k)$ benar untuk semua k dengan $n_0 \leq k < m$, maka $P(m)$ benar.

Dengan menggunakan prinsip keterurutan secara baik, tunjukkan bahwa $P(n)$ adalah benar untuk semua $n \geq n_0$.

Latihan 1.3.5 Tunjukkan bahwa tiga pernyataan prinsip berikut adalah saling ekivalen satu dengan yang lainnya.

(a) Prinsip keterurutan secara baik.

(b) Prinsip induksi matematika.

(c) Prinsip modifikasi induksi matematika.

Latihan 1.3.6 Tunjukkan bahwa untuk $0 \geq r \leq n$, maka

$$\binom{n}{r} = \binom{n}{n-r}$$

Latihan 1.3.7 Misalkan p adalah bilangan prima dan

$$(1+a)^p = 1 + c_1 a + c_2 a^2 + \cdots + c_{p-1} a^{p-1} + a^p,$$

dengan $a \in \mathbb{R}$. Tunjukkan bahwa $p | c_i$ untuk semua i, dengan $1 \leq i \leq p-1$.

Latihan 1.3.8 Dalam Contoh 1.3.7, bila $p = 11$, maka dapatkan $c_1, c_{10}, c_2, c_9, c_4, c_6$.

Latihan 1.3.9 Gunakan Algoritma Euclide untuk menghitung kpk(52, 135) dan tulis hasilnya sebagai kombinasi linier dari 52 dan 135.

Latihan 1.3.10 Misalkan a dan b adalah prima relatif. Tunjukkan bahwa untuk sebarang bilangan bulat n ada bilangan bulat x dan y yang memenuhi $n = xa + yb$.

Latihan 1.3.11 Tunjukkan bahwa bila $a = a'd$ dan $b = b'd$, dimana $d = \text{kpk}(a, b)$, maka $\text{kpk}(a', b') = 1$.

Latihan 1.3.12 Tunjukkan bahwa $\text{kpk}(a, b) = ab$ bila dan hanya bila $\text{fpb}(a, b) = 1$.

Latihan 1.3.13 Dapatkan fpb(9750, 59400) dan kpk(9750, 59400).

Latihan 1.3.14 Tunjukkan bahwa untuk sebarang bilangan bulat $n^3 \equiv n \mod 6$.

Latihan 1.3.15 Tunjukkan bahwa untuk sebarang bilangan bulat n bila tidak didapat $n \equiv 0 \mod 5$, maka didapat $n^4 \equiv 1 \mod 5$.

Latihan 1.3.16 Tunjukkan bahwa untuk sebarang bilangan bulat n, berlaku bahwa $n^5 \equiv n \mod 5$.

Latihan 1.3.17 Tunjukkan bahwa n adalah bilangan prima bila dan hanya bila dalam $\mathbb{Z}_n$, $[r]_n[s]_n = [0]_n$ selalu berakibat $[r]_0 = [0]_n$ atau $[s]_n = [0]_n$.

Latihan 1.3.18 Tunjukkan bahwa bila $\text{fpb}(n, r) = 1$, maka ada suatu bilangan bulat s yang memenuhi $\text{fpb}(n, s) = 1$ dan $rs \equiv 1 \mod n$.

Latihan 1.3.19 Bila $\text{fpb}(m, n) = 1$, maka tunjukkan bahwa untuk sebarang pasangan dua bilangan bulat a dan b ada suatu bilangan bulat x yang memenuhi $x \equiv a \mod m$ dan $x \equiv b \mod n$.

Latihan 1.3.20 (**Teorema Sisa Pembagian China**)

(a) Bila $m_1, m_2, \ldots, m_s$ adalah bilangan bulat yang lebih besar 1 sedemikian hingga sebarang dua dari bilangan tersebut adalah prima relatif, dan bila $a_1, a_2, \ldots, a_s$ adalah sebarang bilangan bulat, tunjukkan bahwa ada suatu bilangan bulat x yang memenuhi $x \equiv a_i \mod m_i$ untuk semua i, dengan $1 \leq i \leq s$. (Gunakan Latihan 1.3.19).

(b) Tunjukkan bahwa bila x dan x' keduanya memenuhi kongruen dalam bagian (a), maka $x \equiv x' \mod M$ dimana $M = m_1 m_2 \cdots m_s$.

1.4 Bilangan Kompleks

Pemahaman mengenai bilangan kompleks akan merupakan suatu yang esensial. Sebagaimana akan terlihat pada bahasan berikut. Dibutuhkan bilangan kompleks untuk mendapatkan semua penyelesaian persamaan polinomial. Ketika diberikan persamaan $x^2 - 2 = 0$, atau $x^2 = 2$ penyelesaiannya adalah $\sqrt{2}$ dan $-\sqrt{2}$. Ini benar, sebab $(\sqrt{2})^2 = (-\sqrt{2}) = 2$. Selanjutnya diberikan persamaan $x^2 + 1 = 0$ atau $x^2 = -1$ dengan cara yang sama penyeaiannya adalah $\sqrt{-1}$ dan $-\sqrt{-1}$. Sebab $(\sqrt{-1})2 = -1$ dan $(-\sqrt{-1})^2 = -1$. Bila $\sqrt{-1}$ dianggap suatu bilangan, dan ditulis $i = \sqrt{-1}$. Didapat $i^2 = -1$ dan $-i^2 = -1$. Dengan demikian dapat dikombinasikan i dengan bilangan yang lain misalnya $2i, i/3, -1 + i$ dan $(1 + \sqrt{2}i)/2$. Berikut ini diberikan pernyataan dari apa yang baru saja dibahas.

Definisi 1.4.1 Himpunan dari **bilangan kompleks** dinotasikan oleh $\mathbb{C}$, didifinikan sebagai

$$\mathbb{C} = \{a + bi \,|\, a, b \in \mathbb{R} \text{ dan } i^2 = -1\}.$$

Bila $z = a + bi$ adalah bilangan kompleks, maka a dinamakan **bagian riil** dari z dan b dinamakan **bagian imajiner** dari z. ✓

Setiap bilangan riil a adalah bilangan kompleks dengan bagian imajinernya adalah nol, jadi $a = a + 0 \cdot i$. Dengan demikian didapat

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Contoh 1.4.1 Bagian riil dari $4i$ adalah 0 sedangkan bagian imajinernya adalah 4. Bagian riil dari $(1 + \sqrt{2}i)/2$ adalah $1/2$ sedangkan bagian imajinernya adalah $\sqrt{2}/2$. ●

Contoh 1.4.2 Memperlakukan $a + bi$ sebagai bilangan, sehingga dapat dilakukan operasi penjumlahan dan perkalian. Asumsikan dengan hukum-hukum yang biasa berlaku pada operasi tersebut dan ingat $i^2 = -1$, maka didapat

$$\begin{aligned} (4 + 2i) - (1 - 3i) &= (4 - 1) + (2 - (-3))i = 3 + 5i \\ (4 + 2i)(1 - 3i) &= 4 - 12i + 2i - 6i^2 = 10 - 10i. \end{aligned}$$

definisi berikut adalah pernytaan yang lebih tepat.

Definisi 1.4.2 Diberikan dua bilangan kompleks $z = a + bi$ dan $w = c + di$, diddefinisikan tambah dan perkalian dari z dan w oleh

$$\begin{aligned} z + w &= (a + bi) + (c + di) = (a + c) + (b + d)i \in \mathbb{C} \\ zw &= (a + bi)(c + di) = (ac - bd) + (ad + bc)i \in \mathbb{C}. \end{aligned}$$

Tentunya disini, operasi pada a, b, c dan d adalah operasi sebagaimana biasa dilakukan pada bilangan riil. ✓

Bila digunakan operasi yang telah didefinisikan tersebut pada bilangan riil, maka bilangan kompleks dengan bagian imajiner nol, $z = a + 0 \cdot i$ dan $w = c + 0 \cdot i$ didapat $z + w = a + c$ dan $zw = ac$. Tambah dan perkalian bilangan kompleks adalah sama seperti tambah dan perkalian pada bilangan riil. Dengan kata lain, operasi penjumlahan dan perkalian pada bilangan kompleks adalah perluasan dari operasi yang berkaitan pada bilangan riil. Pengurangan dapat dilakukan dalam cara yang sama:

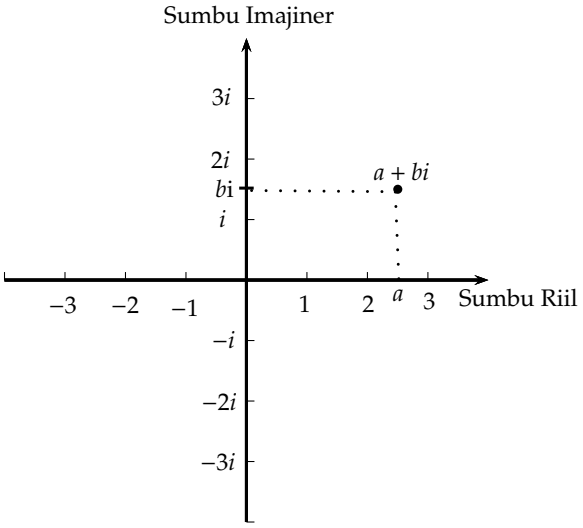
$$z - w = (a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{C}.$$

Catatan bahwa, $z - w = 0 = 0 + 0 \cdot i$ bila dan hanya bila $a - c = 0$ dan $b - d = 0$ atau bila dan hanya bila $a = c$ dan $b = d$ yang berarti bahwa $z = w$. Selanjutnya dilakukan pembagian pada $\mathbb{C}$ sebagaimana sesuai yang dilakukan pada pembagian di $\mathbb{R}$. Ingat bahwa untuk sebarang pasangan bilangan riil $a, b \neq 0$ pembagian a/b dapat dilihat sebagai perkalian dari $a \cdot 1/b$. Dengan begitu dibutuhkan dulu $1/w$ dengan w adalah bilangan kompleks taknol.

Contoh 1.4.3 Apakah $w = 1/(1 + 2i)$ adalah suatu bilangan kmpleks? Untuk menghitung sebagai suatu bilangan kompleks harus dapat dituliskan dalam bentuk $a + bi$. Hal ini dapat dilakukan sebagai berikut:

$$w = \frac{1}{1+2i} = \frac{1}{(1+2i)} \cdot \frac{1-2i}{(1-2i)} = \frac{1-2i}{1+4} = \frac{1}{5} - \frac{2}{5}i,$$

karena $1/5$ dan $-2/5$ adalah bilangan riil, maka w adalah bilangan kompleks. ●



Gambar 1.7: Bidang kompleks $\mathbb{C}$

Contoh yang baru dibahas, mengisyaratkan bagaimana kasus pembagian yang lain dilakukan.

Contoh 1.4.4 Misalkan dihitung $w = (3 - 2i)/(5 + 3i)$.

$$w = \frac{3-2i}{5+3i} = \frac{3-2i}{(5+3i)} \cdot \frac{5-3i}{(5-3i)} = \frac{9-19i}{34} = \frac{9}{34} - \frac{9}{34}i. \quad ●$$

Dalam dua contoh terakhir, telah dihitung $(1+2i)(1-2i) = 1^2+2^2$ dan $(5+3i)(5-3i) = 5^2+3^2$. Ungkapan a^2+b^2 mempunyai arti geometris sebagai mana diberikan pada bahasan berikut.

Definisi 1.4.3 Seperti halnya bilangan riil dapat disajikan sebagai suatu titik pada suatu garis, jadi suatu bilangan kompleks dapat disajikan sebagai titik pada suatu bidang yang dinamakan **bidang kompleks**. Bilangan kompleks $z = a + bi$ disajikan sebagai titik dengan koordinat (a, b) sebgai mana diberikan dalam Gambar 1.7. Dalam hal ini sumbu-x dinamakan **sumbu riil** dan sumbu-y dinamakan **sumbu imajiner**.

Suatu hal yang berkaitan dengan representasi geometri dari definisi yang telah dibahas adalah: pada bilangan riil, misalkan -2, maka nilai mutlaknya adalah $|-2| = 2$. Ini mempunyai arti bahwa jarak titik -2 dari pusat 0 pada garis riil adalah 2. Diperluas pengertian ini pada nilai mutlak $|a + bi|$ adalah jarak dari titik (a, b) dari titik pusat $(0, 0)$ dalam bidang kompleks.

Definisi 1.4.4 Untuk sebarang bilangan kompleks $z = a+bi$, nilai mutlak dari z didifinisikan oleh

$$|z| = |a + bi| \stackrel{\text{def}}{=} \sqrt{a^2 + b^2}.$$

Perlu diperhatikan bahwa, nilai mutlak ini adalah bilangan riil taknegatif.

Gunakan definisi ini pada suatu bilangan riil $a = a+0\cdot i$ didapat $\sqrt{a^2}$ yang sama dengan nilai mutlak sebagaimana biasanya, yaitu sama dengan a bila $a \geq 0$ dan $-a$ bila $a < 0$.

Contoh 1.4.5 Dari definisi, $|i| = |(1 + i)/\sqrt{2}| = |(-1 + \sqrt{3}i)/2| = 1$. Titik $(0, 1), (1/\sqrt{2}, 1/\sqrt{2})$ dan $(-1/2, \sqrt{3}/2)$ semuanya terletak pada lingkaran satuan di bidang kompleks.

Definisi 1.4.5 Untuk sebarang bilangan kompleks $z = a + bi$ didefinisikan **kompleks konjuget** atau singkatnya **konjuget** dari z oleh

$$\overline{z} = \overline{a + bi} \stackrel{\text{def}}{=} a - bi.$$

Gunakan definisi ini pada bilangan riil $a = a+0\cdot i$ didapat $a-0\cdot i = a$. Jadi sebarang bilangan riil mempunyai konjuget dirinya sendiri.

Proposisi 1.4.1

(1) Bila $z = a + bi$ sebarang bilangan kompleks, maka

$$z\overline{z} = |z|^2 = |\overline{z}|^2.$$

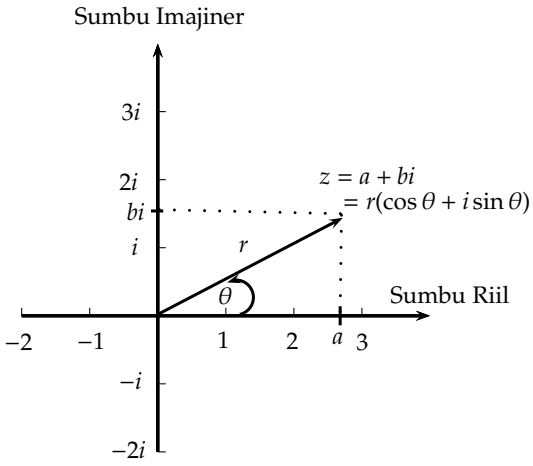
(2) Bila $w = c + di$ sebarang bilangan kompleks, maka

$$\frac{z}{w} = \frac{z\overline{w}}{|w|^2}.$$

Bukti

(1) $(a + bi)(a - bi) = a^2 + b^2 = a^2 + (-b)^2$

(2) $\dfrac{a + bi}{c + di} = \dfrac{(a + bi)}{(c + di)} \cdot \dfrac{(c - di)}{(c - di)} = \dfrac{ac + bd}{c^2 + d^2} + \dfrac{bc - sd}{c^2 + d^2} i.$



Gambar 1.8: Koordinat Polar dari $\mathbb{C}$

Berikutnya digunakan koordinat kutub (polar) dari titik dalam bidang untuk menyajikan bilangan kompleks untuk memfasilitasi penghitungan dalam menyelesaikan persamaan polinomial. Gambar garis dari tititik asal $(0,0)$ ke titik (a,b) yang merepresentasikan bilangan kompleks $z = a + bi$ sebagaimana diberikan dalam Gambar 1.8.

Bila r adalah panjang segmen garis tersebut, maka didapat $r^2 = a^2 + b^2 = |z|^2$ dan $r = |z|$. Misalkan bahwa θ adalah sudut dari sumbu riil positip ke garis, maka didapat

$$a = r\cos\theta \quad \text{dan} \quad b = r\sin\theta$$
$$z = r\cos\theta + i\sin\theta \; = \; r(\cos\theta + i\sin\theta).$$

Definisi 1.4.6 Misalkan z adalah suatu bilangan kompleks. maka representasi $z = a+bi$ dinamakan **representasi Cartesian** dari z, sedangkan $z = r(\cos\theta+i\sin\theta)$ dinamakan **representasi kutub** dari z.

Catatan, r adalah selalu bilangan riil taknegatif. Jadi, representasi dari -2 adalah $2(\cos\pi + i\sin\pi)$

Contoh 1.4.6 Representasi kutub dari beberapa bilangan kompleks sebagaimana berikut:

$$i = 1(\cos\tfrac{\pi}{2} + i\sin\tfrac{\pi}{2}) \qquad -i = 1(\cos\frac{3\pi}{2} + i\sin\tfrac{3\pi}{2})$$
$$\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i = 1(\cos\frac{\pi}{4} + i\sin\tfrac{\pi}{4}) \qquad 1 + i = \sqrt{2}(\cos\frac{\pi}{4} + i\sin\tfrac{\pi}{4}).$$

Penulisan bilangan kompleks dalam bentuk kutub memberikan kemudahan dalam berbagai penghitungan, sebagaimana terlihat pada beberapa proposisi berikut.

Proposisi 1.4.2 Diberikan dua bilangan kompleks dalam representasi kutub $z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$ dan $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$, maka

$$z_1 z_2 = r_1 r_2(\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)).$$

Bukti

$$\begin{aligned} z_1z_2 &= r_1r_2(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2) \\ &= r_1r_2((\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2)) \\ &= r_1r_2(\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_1)). \end{aligned}$$

Akibat 1.4.1 Diberikan suatu bilangan kompleks $z = r(\cos\theta + i\sin\theta)$, maka

$$z^2 = r^2(\cos 2\theta + i\sin 2\theta).$$

Bukti Gunakan Proposisi 1.4.2 didapat

$$\begin{aligned} z^2 &= r^2(\cos\theta + \theta) + i\sin(\theta+\theta)) \\ &= r^2(\cos 2\theta + i\sin 2\theta). \end{aligned}$$

Akibat 1.4.2 (**Formula De Moivre**) Diberikan sebarang bilangan kompleks $z = r(\cos\theta + i\sin\theta)$, maka untuk bilangan positip n didapat

$$z^n = r^n(\cos n\theta + i\sin n\theta)$$

Bukti Digunakan induksi matematika, untuk $n = 1$ jelas. Selanjutnya, misalkan benar untuk k dengan $1 < k < n$, maka

$$\begin{aligned} z^{k+1} &= z^kz = r^k(\cos k\theta + i\sin k\theta)\, r(\cos\theta + i\sin\theta) \\ &= r^{k+1}(\cos k\theta + i\sin k\theta)(\cos\theta + i\sin\theta) \quad \text{(gunakan Proposisi 1.4.2)} \\ &= r^{k+1}(\cos(k+1)\theta + i\sin(k+1)\theta). \end{aligned}$$

Terlihat bahwa untuk $n = k+1$ benar bahwa

$$z^{k+1} = r^{k+1}(\cos(k+1)\theta + i\sin(k+1)\theta),$$

dengan demikian untuk bilangan bulat $n > 0$ benar bahwa

$$z^n = r^n(\cos n\theta + i\sin n\theta).$$

Contoh 1.4.7 Diberikan $z = 1 - \sqrt{3}i$, untuk menghitung z^8, lakukan hal berikut:

1. Jadikan z kedalam bentuk kutub. Didapat $r^2 = |z|^2 = 1^2 + (\sqrt{3})^2 = 4$ atau $r = 2$. Jadi z dapat ditulis sebagai $z = 2(\frac{1}{2} - \frac{\sqrt{3}}{2}i)$ dan dicari sudut θ dengan $0 \le \theta \le 2\pi$ yang memenuhi $\cos\theta = \frac{1}{2}$ dan $\sin\theta = -\frac{\sqrt{\sqrt{3}}}{2}$, didapat $\theta = \dfrac{5\pi}{3}$ dan $z = 2\left(\cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3}\right)$.
2. Gunakan formula De Moivre, didapat

$$\begin{aligned} z^8 &= 2^8\left(\cos\frac{40\pi}{3} + i\sin\frac{40\pi}{3}\right) \\ &= 256\left(\cos(12\pi + \frac{4\pi}{3}) + i\sin(12\pi + \frac{4\pi}{3})\right) \\ &= 256\left(\cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3}\right) \\ &= 256\left(-\frac{1}{2} - \frac{\sqrt{3}}{2}i\right) \\ &= -126 - 128\sqrt{3}i. \end{aligned}$$

Contoh 1.4.8 Hitung $\sqrt{i}$. Misalkan $z = \sqrt{i}$ didapat $z^2 = i$. Ubah z kedalam bentuk kutub $z = r(\cos\theta + i\sin\theta)$, didapat

$$\begin{aligned} r^2(\cos 2\theta + i\sin 2\theta) = z^2 &= i \\ &= 1(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}). \end{aligned}$$

Jadi $r^2 = 1$ atau $r = 1$ dan $2\theta = \frac{\pi}{2} + 2\pi k$, atau $\theta = \frac{\pi}{4} + \pi k$ untuk beberapa bilangan bulat k. Tetapi diinginkan $0 \le \theta \le 2\pi$, dengan demikian $k = 0, 1$. Sehingga didapat $\theta = \frac{\pi}{4}$ dan $\theta = \frac{5\pi}{4}$. Jadi nilai dari $z^2 = i$ yang memenuhi adalah

$$z_1 = 1\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right) = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$$

dan

$$z_2 = 1\left(\cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4}\right) = -\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i.$$

Contoh 1.4.9 Dapatkan penyelesaian dari $z^3 + 8i = 0$. Dalam hal ini dicari bilangan kompleks $z = r(\cos\theta + i\sin\theta)$ yang memenuhi

$$z^3 = r^3(\cos 3\theta + i\sin 3\theta) = -8i = 8\left(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2}\right).$$

Didapat $r^3 = 8$ atau $r = 2$ dan $3\theta = \frac{3\pi}{2} + 2\pi k$ atau $\theta = \frac{\pi}{2} + \frac{2\pi}{3}k$, dengan $k = 0, 1, 2$. Dengan demikian nilai-nilai θ adalah $\theta = \frac{\pi}{2}, \frac{7\pi}{6}, \frac{11\pi}{6}$. Jadi nilai z yang memenuhi adalah

$$z_1 = 2(\cos\frac{\pi}{2} + i\sin\frac{\pi}{2}) = 2(0 + i) = 2i,$$

$$z_2 = 2(\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}) = 2(0 + i) = 2(-\frac{\sqrt{3}}{2} - \frac{1}{2}i) = -\sqrt{3} - i$$

dan

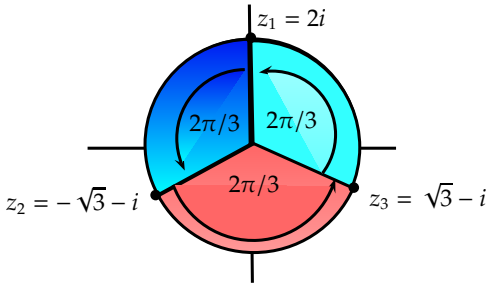
$$z_3 = 2(\cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6}) = 2(0 + i) = 2(\frac{\sqrt{3}}{2} - \frac{1}{2}i) = \sqrt{3} - i$$

Gambar 1.9 menyatakan bahwa tiga penyelesaian dari $z^3 + 8i = 0$ terletak pada lingkaran jari-jari 2 dengan pusat $(0, 0)$.

Latihan

Latihan 1.4.1 Pada latihan berikut ungkapkan bilangan kompleks dalam bentuk $a + bi$, dimana $a, b \in \mathbb{R}$.

1. $(2 + 3i) + (7 - 5i)$	2. $3i - (4 - 2i)$	3. $(4 - i) - (2 - 3i)$
4. i^7	4. i^{12}	6. i^{17}
7. i^{32}	8. i^{38}	9. $(-i)^5$
10. $(3 + 2i)(2 + 5i)$	11. $(5 - 2i)(3 + 4i)$	12. $(1 + i)^9$
13. $(1 + i)/i$	14. $(2 + i)/(1 - i)$	15. $i/(1 + 3i)$



Gambar 1.9: Penyelesaian dari $z^3 + 8i = 0$

Latihan 1.4.2 Hitung $|2 - 3i|, |1 + i|, |\sqrt{2} - \sqrt{3}i|$.

Latihan 1.4.3 Ungkapkan bilangan kompleks berikut dalam bentuk kutub $r(\cos\theta + i\sin\theta)$.

1. $1 - i$ 2. $-1 - i$ 3. $-1 + \sqrt{3}i$.

Latihan 1.4.4 Dapatkan semua penyelesaian dari persamaan berikut.

1. $z^3 = 1$ 2. $z^4 = 1$ 3. $z^4 = -1$
4. $z^3 = -8$ 5. $z^3 = -i$ 6. $z^3 = -125i$.

Latihan 1.4.5 Dengan menggunakan ekspasi deret dari e^x, $\cos x$ dan $\sin x$ tunjukkan **formula Euler** $e^{ix} = \cos x + i\sin x$.

Latihan 1.4.6 Dengan menggunakan formula Euler pada latihan sebelumnya, tunjukkan formula De Moivre.

1.5 Matriks

Untuk mengakhiri bab pendahuluan ini ditinjau ulang bahasan matriks. Beberapa macam pengertian matriks memberikan suatu hal yang penting sebagaimana diperlukan pada bahasan bab berikutnya.

Contoh 1.5.1 Suatu matriks berukuran 2×2 adalah susunan persegi dari empat bilangan bulat, misalnya

$$A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} \quad \text{atau} \quad B = \begin{bmatrix} -1 & 2 \\ 0 & -4 \end{bmatrix}.$$

Suatu matriks berukuran 2×3 adalah susunan persegi panjang dengan dua baris dan tiga kolom dari enam bilangan bulat, misalnya.

$$C = \begin{bmatrix} 1 & -1 & 0 \\ 0 & 3 & 7 \end{bmatrix} \quad \text{atau} \quad D = \begin{bmatrix} 2 & 1 & -1 \\ -1 & 0 & 5 \end{bmatrix}.$$

Dua matriks yang mempunyai bentuk sama dapat dilakukan operasi penjumlahan. Operasi penjumlahan dilakukan pada elemen-elemen yang seletak. Jadi

$$A + B = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} + \begin{bmatrix} -1 & 2 \\ 0 & -4 \end{bmatrix} = \begin{bmatrix} 1 + (-1) & 2 + 2 \\ 3 + 0 & 4 + (-4) \end{bmatrix} = \begin{bmatrix} 0 & 4 \\ 3 & 0 \end{bmatrix}$$

dan

$$C+D=\begin{bmatrix}1 & -1 & 0\\ 0 & 3 & 7\end{bmatrix}+\begin{bmatrix}2 & 1 & -1\\ -1 & 0 & 5\end{bmatrix}=\begin{bmatrix}1+2 & -1+1 & 0+(-1)\\ 0+(-1) & 3+0 & 7+5\end{bmatrix}=\begin{bmatrix}3 & 0 & -1\\ -1 & 3 & 12\end{bmatrix}.$$

Dua matriks yang tidak mempunyai bentuk yang sama tidak dapat ditambahkan satu dengan yang lainnya.

Definisi 1.5.1 Suatu matriks A berukuran $n \times m$ adalah susunan dari elemen-elemen dalam n baris dan m kolom. Ditulis $A = \{a_{i,j}\}$, dimana $a_{i,j}$ adalah elemen dalam baris ke-i kolom ke-j dengan $1 \leq i \leq n$ dan $1 \leq j \leq m$.

Definisi 1.5.2 Notasi $M_{n\times m}(R)$ adalah himpunan semua matriks ukuran $n\times m$ dengan elemen-elemen di R. Bila $n = m$, Notasi $M_{n\times n}(R)$ ditulis sebagai $M(n, R)$. Himpunan R bisa $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ atau sebarang Z_p dengan p bilanga prima.

Definisi 1.5.3 Misalkan $A = \{a_{i,j}\} \in M_{n\times m}(R)$ dan $B = \{b_{i,j}\} \in M_{n\times m}(R)$. **Jumlah** dari A dan B adalah $A+B = \{a_{i,j}+b_{i,j}\}$ dengan kata lain adalah matriks $\{c_{i,j}\} \in M_{n\times m}(R)$, dimana $c_{i,j} = a_{i,j}+b_{i,j}$ untuk semua i dan j, dimana $1 \leq i \leq n$ dan $1 \leq\leq m$. **Produk** dari suatu elemen $t \in R$ dengan suatu matriks $A = \{a_{i,j}\}$ didefinisikan oleh matriks $tA = \{ta_{i,j}\}$.

Perkalian dari dua matriks didifiniskan sebagai berikut.

Definisi 1.5.4 Misalkan $A = \{a_{i,j}\} \in M_{n\times m}(R)$ dan $B = \{b_{j,k}\} \in M_{m\times r}(R)$. **Perkalian** dari A dan B adalah matriks berukuran $n \times r$ yang diberikan oleh matriks $AB = \{c_{i,k}\} \in M_{n\times r}(R)$ dimana

$$c_{i,k} = a_{i,1}b_{1,k} + a_{i,2}b_{2,k} + \cdots + a_{i,m}b_{m,k},$$

untuk semua i dan k dengan $1 \leq n$ dan $1 \leq k \leq r$.

Contoh 1.5.2 Diberikan matriks-matriks

$$A=\begin{bmatrix}1 & 2 & 3\\ 5 & 3 & 4\end{bmatrix}, B=\begin{bmatrix}2 & 1\\ 3 & 7\\ 5 & 6\end{bmatrix}$$

Elemen baris ke-1 kolom ke-2 dan baris ke-2 kolom ke-1 matriks perkalian AB diberikan sebagai berikut

$$AB=\begin{bmatrix}\boxed{1} & \boxed{2} & \boxed{3}\\ \boxed{5} & \boxed{3} & \boxed{4}\end{bmatrix}\begin{bmatrix}\boxed{2} & \boxed{1}\\ \boxed{3} & \boxed{7}\\ \boxed{5} & \boxed{6}\end{bmatrix}=\begin{bmatrix}\square & \boxed{33}\\ \boxed{43} & \square\end{bmatrix}$$

$$(1\,.\,1)+(2\,.\,7)+(3\,.\,6)=33$$
$$(5\,.\,2)+(3\,.\,3)+(4\,.\,6)=43$$

Dengan melakukan hal yang serupa didapat

$$AB=\begin{bmatrix}1 & 2 & 3\\ 5 & 3 & 4\end{bmatrix}\begin{bmatrix}2 & 1\\ 3 & 7\\ 5 & 6\end{bmatrix}=\begin{bmatrix}23 & 33\\ 39 & 50\end{bmatrix}$$

dan perkalian matriks BA diberikan oleh

$$BA = \begin{bmatrix} 2 & 1 \\ 3 & 7 \\ 5 & 6 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 \\ 5 & 3 & 4 \end{bmatrix} = \begin{bmatrix} 7 & 7 & 10 \\ 38 & 27 & 37 \\ 35 & 28 & 39 \end{bmatrix}$$

terlihat bahwa $AB \neq BA$. ●

Contoh 1.5.3 Dalam $M(n, R)$ dimana R bisa sebarang dari $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ atau $\mathbb{Z}_p$, didapat suatu **matriks identitas** I_n dengan elemen diagonal $a_{i,i} = 1$ untuk semua i dimana $1 \leq i \leq n$ dan semua elemen yang lainnya sama dengan nol yaitu $a_{i,j} = 0$ bila $i \neq j$. Misalnya, matriks identitas

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Mudah diselidiki bahwa diberikan sebarang matriks berukuran 3×3 yaitu $A = \{a_{i,j}\}$, maka $AI_3 = A = I_3A$. ●

Contoh 1.5.4 Diberikan dua matriks

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \quad \text{dan} \quad B = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}.$$

Didapat

$$AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

dan

$$BA = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Terlihat bahwa $AB = I_2 = BA$. ●

Definisi 1.5.5 Suatu matriks $A \in M(n, R)$ **mempunyai invers** bila ada suatu matriks $A^{-1} \in M(n, R)$ yang memenuhi $AA^{-1} = I_n = A^{-1}A$. Matriks A^{-1} dinamakan **invers** dari A. ✓

Untuk menentukan matriks invers, perlu diberikan suatu pengertian dari apa yang dinamkan determinan dari suatu matriks. Pembahasan masalah ini hanya dibatasi untuk matriks yang berukuran 2×2.

Definisi 1.5.6 Diberikan matriks suatu matriks $A \in M(2, R)$ oleh

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix},$$

determinan dari matriks A didefinisikan sebagai $\det(A) = ad - bc \in R$. ✓

Contoh berikut menjelaskan sifat penting hubungan determinan dari dua matriks.

Contoh 1.5.5 Diberikan dua matriks

$$A = \begin{bmatrix} 3 & 1 \\ 4 & 2 \end{bmatrix} \quad \text{dan} \quad B = \begin{bmatrix} 4 & 5 \\ 1 & 2 \end{bmatrix}.$$

Maka $\det(A) = (3)(2) - (1)(4) = 2$ dan $\det(B) = (4)(2) - (5)(1) = 3$. Selanjutnya dihitung

$$AB = \begin{bmatrix} 3 & 1 \\ 4 & 2 \end{bmatrix}\begin{bmatrix} 4 & 5 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 13 & 17 \\ 18 & 24 \end{bmatrix}.$$

Didapat $\det(AB) = (13)(24) - (17)(18) = 312 - 306 = 6$. Terlihat bahwa $\det(AB) = 6 = (2)(3) = \det(A)\det(B)$. ●

Apa yang baru saja dibahas dalam contoh secara lebih general diberikan oleh proposisi berikut.

Proposisi 1.5.1 Untuk sebarang matriks $A, B \in M(2, R)$ didapat $\det(AB) = \det(A)\det(B)$.

Bukti Misalkan

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{dan} \quad B = \begin{bmatrix} a' & b' \\ c' & d' \end{bmatrix}.$$

Didapat

$$\det(A)\det(B) = (ad - bc)(a'd' - b'c') = (ada'd' + bcb'c') - (bca'd' + adb'c').$$

Selanjutnya dihitung perkalian

$$AB = \begin{bmatrix} aa' + bc' & ab' + bd' \\ a'c + dc' & cb' + dd' \end{bmatrix}.$$

Didapat

$$\begin{aligned} \det(AB) &= (aa' + bc')(cb' + dd') - (ab' + bd')(a'c + dc') \\ &= (aa'dd' + bc'cb') + (\cancel{aa'cb'} + \cancel{bc'dd'}) - (\cancel{ab'a'c} + \cancel{bd'dc'}) - (ab'dc' + bd'a'c) \\ &= (ada'd' + bcb'c') - (bca'd' + adb'c') \\ &= \det(A)\det(B). \quad \checkmark \end{aligned}$$

definisi determinan dan bukti sifat perkalian determinan dapat diperluas untuk matriks berukuran $n \times n$ yang mana dapat dijumpai pada buku aljabar linier. Selanjutnya kembali pada matriks berukuran 2×2 apa syaratnya suatu matriks ukuran 2×2 mempunyai invers? Pertanyaan ini dijawab oleh proposisi berikut.

Proposisi 1.5.2 Diberikan matriks

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

mempunyai invers bila dan hanya bila $\det(A) \neq 0$, dan bila $\det(A) \neq 0$, maka

$$A^{-1} = \frac{1}{\det(A)}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}.$$

Bukti Bila $\det(A) = 0$, maka dengan proposisi sebelumnya $\det(AB) = \det(A)\det(B) = 0 \cdot \det(B) = 0$, sedangkan $\det(I_2) = 1$. Jadi $AB \neq I_2$ untuk sebarang matriks B. Dengan demikian A tidak mempunyai invers. Bila $\det(A) \neq 0$, maka didapat

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \cdot \frac{1}{\det(A)} = \begin{bmatrix} ad-bc & 0 \\ 0 & ad-bc \end{bmatrix} \cdot \frac{1}{ad-bc} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I_2.$$

Terlihat A mempunyai invers sebagaimana diberikan oleh A^{-1}.

Latihan

Latihan 1.5.1 Hitung hasil operasi matriks berikut.

1. $\begin{bmatrix} 4 & 5 \\ 0 & -1 \\ 3 & 2 \end{bmatrix} + \begin{bmatrix} -2 & 1 \\ 3 & 5 \\ -3 & 3 \end{bmatrix}$ di $M_{3\times 2}(\mathbb{Z})$
2. $\begin{bmatrix} i & 2i \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 3 \\ i & 1 \end{bmatrix}$ di $M(2,\mathbb{C})$
3. $\begin{bmatrix} 1-i & 3+i \\ 0 & 4 \end{bmatrix} + \begin{bmatrix} 3i & 1-i \\ i & 2i \end{bmatrix}$ di $M(2,\mathbb{C})$
4. $\begin{bmatrix} i & 2i \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 & 3 \\ i & 1 \end{bmatrix}$ di $M(2,\mathbb{C})$
5. $i\begin{bmatrix} -1 & 1-i \\ 1+i & i \end{bmatrix}$ di $M(2,\mathbb{C})$
6. $2\begin{bmatrix} 3 & 2 \\ 4 & 1 \end{bmatrix}$ di $M(2,\mathbb{Z}_5)$
7. $\begin{bmatrix} 3 & 4 \\ 4 & 1 \end{bmatrix}\begin{bmatrix} 4 & 2 \\ 3 & 4 \end{bmatrix}$ di $M(2,\mathbb{Z}_5)$
8. $\begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}\begin{bmatrix} 2i & i \\ -i & 1 \end{bmatrix}$ di $M(2,\mathbb{C})$
9. $\begin{bmatrix} i & 0 \\ 0 & i \end{bmatrix}^5$ di $M(2,\mathbb{C})$
10. $\begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}^4$ di $M(2,\mathbb{C})$.

Latihan 1.5.2 Hitung determinan matriks berikut.

1. $\begin{bmatrix} i & 1+i \\ 2i & -i \end{bmatrix}$ di $\mathbb{C}$
2. $\begin{bmatrix} 4 & 2 \\ 5 & 3 \end{bmatrix}$ di $\mathbb{Z}_7$
3. $\begin{bmatrix} 5 & 1 \\ 2 & 2 \end{bmatrix}$ di $\mathbb{Z}_7$
4. $\begin{bmatrix} 10 & 9 \\ 7 & 8 \end{bmatrix}$ di $\mathbb{Z}_{11}$.

Latihan 1.5.3 Tentukan matriks berikut punya invers atau tidak.

1. $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ di $M(2,\mathbb{Q})$
2. $\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & 3\cos\theta \end{bmatrix}$ di $M(2,\mathbb{C})$
3. $\begin{bmatrix} i & i \\ i & -i \end{bmatrix}$ di $M(2,\mathbb{C})$
4. $\begin{bmatrix} 4 & 1 \\ -3 & 2 \end{bmatrix}$ di $M(2,\mathbb{Z}_5)$.

Latihan 1.5.4 Tunjukkan bahwa bila $A, B \in M(2,\mathbb{C})$ mempunyai invers, maka AB juga punya invers.

Latihan 1.5.5 Dapatkan semua matriks yang punya invers di $M(2,\mathbb{Z}_2)$.

Latihan 1.5.6 Dapatkan semua matriks A di $M(2,\mathbb{Z}_3)$ dimana $\det(A) = 1$.

Bagian I

Teori Grup

Bab 2

Grup

Sekarang siap untuk memulai kajian tentang aljabar abstrak. Kata "aljabar" berasal dari judul buku "Hisab al-jabr w'al-muqabala" ditulis oleh Abu Ja'far Muhammad bin Musa Al-Khawarizmi (790-840). Kata al-jabr sendiri berasal dari akar berbentuk unit dan mengacu pada salah satu metode penyelesaian persamaan kuadrat yang dijelaskan dalam buku tersebut. Buku ini dapat dianggap sebagai risalah pertama pada aljabar.

Pembahasan dalam bab ini dimulai dengan konsep grup. Beberapa sumber memberikan kontribusi terhadap munculnya konsep grup abstrak. Pertama, memahami sifat mendalam yang berbeda dari bilangan bulat adalah salah satu yang paling mengasyikan bagi matematikawan kuno. Selanjutnya, mencari solusi untuk persamaan polinomial selama berabad-abad adalah sumber penting lain dari masalah matematika. Akhirnya, kajian tentang transformasi objek geometris memunculkan ide-ide baru dalam pengembangan matematika di zaman modern. Ketiga disiplin matematika ***teori bilangan, teori persamaan aljabar***, dan ***teori transformasi geometris*** semuanya berkontribusi untuk pengembangan matematika dimasa kini, yaitu disebut konsep grup abstrak, atau sederhananya disebut grup.

Kata grup pertama kali diperkenalkan sebagai suatu istilah teknis dalam matematika untuk menyajikan suatu grup permutasi oleh matematikawan Prancis terkenal Galois yang mempunyai nama lengkap Évariste Galois. Galois berumur tidak panjang. Dia lahir di Bourg-la-Reine pada tanggal 25 Oktober 1811 dan meninggal 31 Mei 1832 kerena suatu perkelahian. Walaupun berumur tidak panjang, hasil kerjanya menempatkan pondasi yang mendasar yaitu teori Galois adalah suatu cabang utama dari aljabar abstrak dan subfield dari keterkaitan Galois.

Dalam bab ini akan terlihat bagaimana gagasan grup muncul dalam beberapa situasi yang benar-benar berbeda dan kemudian bagaimana mempelajarinya untuk bekerja dengan grup abstrak. Dalam bab pertama ini konstruksi grup dijadikan sebagai contoh dasar yang digunakan di seluruh bab-bab berikutnya.

2.1 Contoh-contoh dan Konsep Dasar

Pada awal bahasan ini diberikan beberapa contoh yang membantu untuk memahami konsep baru yang dikenalkan pada bab ini.

Contoh 2.1.1 Dapatkan semua akar dari persamaan $f(x) = x^3 - 1$ di $\mathbb{C}$. Perlu diperhatikan bahwa $f(x)$ dapat difaktorkan menjadi

$$f(x) = x^3 - 1 = (x-1)(x^2 + x + 1).$$

Bila digunakan formula untuk persamaan kuadrat didapat $\omega = (-1 + \sqrt{3}i)/2$ dan $\omega^2 = (-1 - \sqrt{3}i)/2$ adalah dua akar kompleks dari $x^2 + x + 1$. Jadi akar-akar dari $f(x)$ adalah $\{1, \omega, \omega^2\}$. Catatan bahwa, karena $f(\omega) = 0$, didapat $\omega^3 = 1$ dan $\omega^4 = \omega$. Bila digunakan perkalian bilangan kompleks sebagaimana biasanya, maka didapat tabel perkalian yang diberikan oleh Tabel 2.1.

Tabel 2.1: Perkalian dalam $\{1, \omega, \omega^2\}$

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

Contoh 2.1.2 Dapatkan semua akar dari $f(x) = x^4 - 1$ di $\mathbb{C}$. Catatan bahwa, $f(x)$ bisa difaktorkan sebagai

$$(x^2 - 1)(x^2 + 1) = (x-1)(x+1)(x-i)(x+i).$$

Jadi empat akar dari $f(x)$ adalah $\{1, -1, i, -i\}$. Bila digunakan perkalian bilangan kompleks sebagaimana biasa, didapat tabel perkalian yang disajikan oleh Tabel 2.2.

Tabel 2.2: Perkalian dalam $\{1, i, -1, -i\}$

$\times$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Contoh 2.1.3 Untuk $\mathbb{Z}_3 = \{[0]_3, [1]_3, [2]_3\}$, bila operasi penjumlahan diberlakukan di $\mathbb{Z}_3$, didapat Tabel 2.3.

Tabel 2.3: Penjumlahan dalam Z_3

$+$	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Contoh 2.1.4 Untuk $Z_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ bila dalam Z_4 diberlakukan operasi penjumlahan sebagaimana biasa didapat Tabel 2.4.

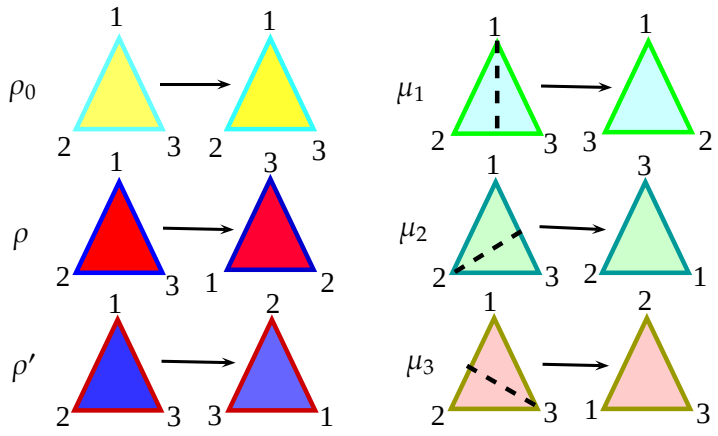
Tabel 2.4: Penjumlahan dalam $\mathbb{Z}_4$

+	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Bila dari contoh-contoh yang telah dibahas dan diperhatikan bahwa Tabel 2.1 dan Tabel 2.3 mempunyai kesamaan pola atau struktur, kecuali bahwa nama-nama elemennya yang berbeda. Hal yang sama juga terjadi pada Tabel 2.2 dan Tabel 2.4. Contoh-contoh yang dibahas ini adalah struktur dari apa yang dinamakan grup. Sebelum diberikan definisi secara formal dari konsep grup, diberikan beberapa contoh lagi yang berbeda.

Contoh 2.1.5 Diberikan segitiga sama sisi. Dibahas semua simetri dari segitiga sama sisi atau gerakan dari segitiga yang mempertahankan bentuk. Ada ada enam macam: identitas ρ_0 adalah menyatakan segitiga tetap pada posisi semula; ρ menyatakan rotasi 120° terhadap pusat segitiga berlawanan arah jarum jam; ρ' rotasi 240° terhadap pusat segitiga berlawanan arah jarum jam. Tiga pencerminan terhadap garis tengah: μ_1, μ_2 dan μ_3

Hal ini akan lebih memudahkan bila titik sudut segitiga dilabeli sebagaimana diberikan oleh Gambar 2.1. Misalkan S_3 adalah himpunan dari enam simetri yaitu



Gambar 2.1: Semua Simetri dari Δ

$$S_3 = \{\rho_0, \rho, \rho', \mu_1, \mu_2, \mu_3\}$$

Elemen-elemen S_3 adalah fungsi pada $\{1, 2, 3\}$, misalnya $\rho(1) = 2, \rho(2) = 3, \rho(3) = 1$ dan $\mu_1(1) = 1, \mu_1(2) = 3, \mu_1(3) = 2$.

Selanjutnya bila di S_3 diberlakukan operasi komposisi fungsi, misalnya ρ' adalah hasil melakukan 2 kali ρ yaitu $\rho' = \rho\rho = \rho^2$. Makna $\mu_1\mu_2$ adalah komposisi fungsi yaitu $\mu_1(\mu_2(x))$, $\forall x \in \{1,2,3\}$. Jadi

$$\mu_1(\mu_2(1)) = \mu_1(3) = 2, \mu_1(\mu_2(2)) = \mu_1(2) = 3, \mu_1(\mu_2(3)) = \mu_1(1) = 1,$$

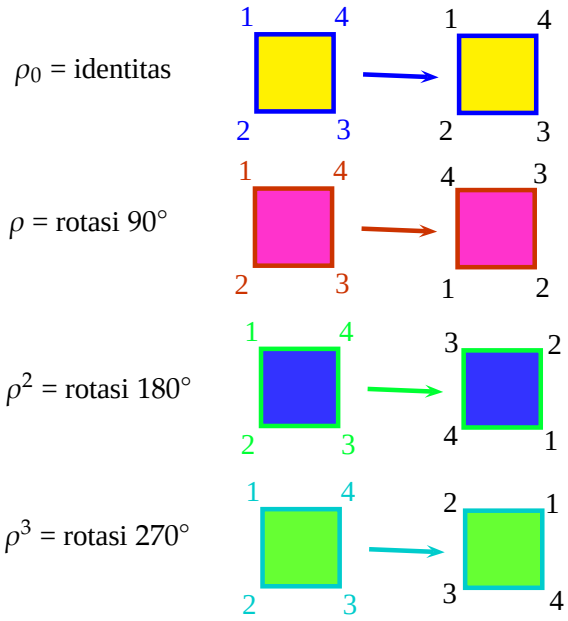
Terlihat bahwa $\mu_1\mu_2 = \rho$. Selain itu juga didapat

$$\mu_2(\mu_1(1)) = \mu_2(1) = 3, \mu_2(\mu_1(2)) = \mu_2(3) = 1, \mu_2(\mu_1(3)) = \mu_2(2) = 2,$$

Terlihat bahwa $\mu_2\mu_1 = \rho'$ dan $\mu_1\mu_2 \neq \mu_2\mu_1$. ●

Contoh 2.1.6 Diberikan masalah yang serupa sebelumnya simetri dari persegi. Ada sebanyak 4(2) = 8 simetri. Empat adalah rotasi yang diberikan oleh Gambar 2.2.

Empat rotasi dari persegi yang diberikan oleh Gambar 2.2 adalah rotasi persegi masing-

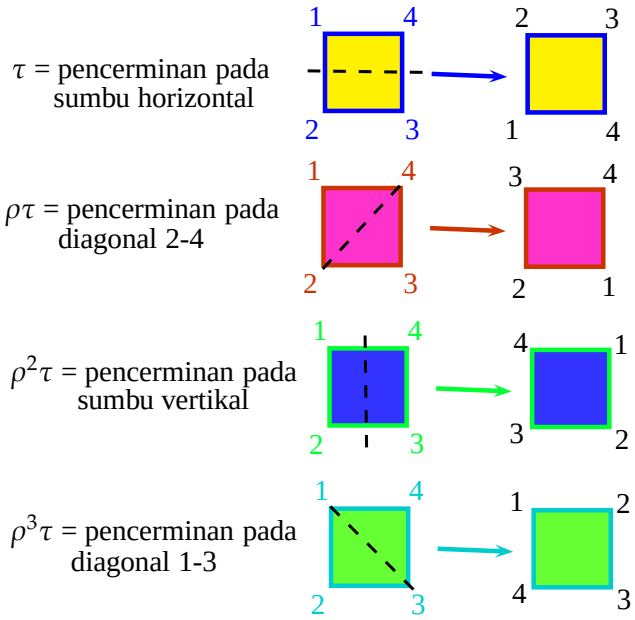


Gambar 2.2: Simetri Rotasi □

masing dirotasi $0°, 90°, 180°$ dan $270°$ terhadap pusat benda berlawanan arah dengan jarum jam. Perlu diperhatikan bahwa ρ adalah rotasi benda pada pusat berlawanan dengan arah jarum jam sebesar $90°$ dan ρ adalah fungsi pada $\{1,2,3,4\}$ dengan $\rho(1) = 2, \rho(2) = 3, \rho(3) = 4$ dan $\rho(4) = 1$. Dengan demikian rotasi sebesar dua kali $90°$ yaitu $180°$ adalah komposisi ρ^2. Dengan demikian didapat $\rho^2(1) = \rho(\rho(1)) = \rho(2) = 3, \rho^2(2) = \rho(\rho(2)) = \rho(3) = 4, \rho^2(3) = \rho(\rho(3)) = \rho(4) = 1$ dan $\rho^2(4) = \rho(\rho(4)) = \rho(1) = 2$. Semetri yang lain dari persegi adalah empat pencerminan yang diberikan oleh Gambar 2.3.

Sama halnya pada rotasi, pencerminan juga fungsi pada $\{1,2,3,4\}$. Jadi pencerminan pada sumbu horizontal τ diberikan oleh $\tau(1) = 2, \tau(2) = 1$ dan $\tau(3) = 4, \tau(4) = 3$. Sedangkan pencerminan pada diagonal 2-4 dalam hal ini diberikan oleh komposisi fungsi $\rho\tau$, dengan demikian didapat $\rho\tau(1) = \rho(\tau(1)) = \rho(2) = 3, \rho\tau(2) = \rho(\tau(2)) = \rho(1) = 2, \rho\tau(3) = \rho(\tau(3)) = \rho(4) = 1$ dan $\rho\tau(4) = \rho(\tau(4)) = \rho(3) = 4$. Himpunan fungsi-fungsi pada persegi yang dibahas tersebut dinotasikan oleh D_4. Jadi

$$D_4 = \{\rho_0, \rho, \rho_2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}.$$ ●



Gambar 2.3: Pencerminan dari □

Semua contoh-contoh yang telah dibahas adalah berkaitan dengan suatu himpunan dan operasi pada himpunan tersebut dengan sifat-sifat yang tertentu sebagaimana didefinisikan berikut.

Definisi 2.1.1 Suatu himpunan tak-kosong G bersama dengan suatu operasi $*$ pada G dinamakan **grup** terhadap operasi $*$ bila memenuhi **aksiomatik grup**:

(1) Teretutup Untuk setiap $a, b \in G$ berlaku $a * b \in G$.

(2) Assosiatif Untuk setiap $a, b, c \in G$ berlaku $a * (b * c) = (a * b) * c$.

(3) Identitas Ada suatu elemen $e \in G$ sedemikian hingga untuk semua $a \in G$ berlaku $a * e = a = e * a$. Elemen e dinamakan elemen **identitas** di G.

(4) Invers Untuk setiap $a \in G$ ada elemen $a^{-1} \in G$ yang memenuhi $a * a^{-1} = e = a^{-1} * a$. Elemen a^{-1} dinamakan **invers** dari elemen a. ✓

Catatan bahwa, operasi $*$ pada G yang memenuhi (1), juga dinyatakan sebagai fungsi yang diberikan oleh

$$* : G \times G \to G, \text{ dengan } *(a, b) \stackrel{\text{def}}{=} a * b, \ \forall (a, b) \in G \times G.$$

Penghapusan kurung, dikarenakan operasi biner $*$ adalah assosiatif, maka penulisan

$$(a * b) * (c * d) = ((a * b) * c) * d = (a * (b * c)) * d$$

ditulis $a * b * c * d$. Misalkan $n > 3$ dan $g, h \in G$ dengan

$$g = (g_1 \cdots g_i)(g_{i+1} \cdots g_n), \ \ h = (g_1 \cdots g_j)(g_{j+1} \cdots g_n)$$

Tanpa mengurangi generalitas, misalkan $i \leq j$ untuk $i = j$ jelas $g = h$. Jadi, misalkan $i < j$, maka kurung dapat disusun sebagai berikut

$$\begin{aligned} g &= (g_1 \cdots g_i)((g_{i+1} \cdots g_j)(g_{j+1} \cdots g_n)) \\ h &= ((g_1 \cdots g_i)(g_{i+1} \cdots g_j))(g_{j+1} \cdots g_n) \end{aligned}$$

Misalkan $A = (g_1 \cdots g_i), B = (g_{i+1} \cdots g_j)$ dan $C = (g_{j+1} \cdots g_n)$, didapat

$$g = A(BC) = (AB)C = h.$$

Kondisi aksiomatik grup dipenuhi oleh semua Contoh 2.1.1 sampai Contoh 2.1.6.

Definisi 2.1.2 Suatu grup G dengan operasi $*$ dinamakan grup **Abelian** atau **komutatif** bila untuk setiap $a, b \in G$ berlaku $a * b = b * a$.

Himpunan tak-kosong H dan suatu operasi $*$ pada H ditulis sebagai $\langle H, * \rangle$. Contoh 2.1.1 sampai Contoh 2.1.4 adalah contoh grup Abelian sedangkan Contoh 2.1.5 dan Contoh 2.1.6 bukan grup Abelian.

Contoh 2.1.7 Diberikan $\langle \mathbb{Z}, + \rangle$ adalah grup Abelian, dengan elemen identitas $0 \in \mathbb{Z}$ dan untuk setiap $a \in \mathbb{Z}$ elemen $-a$ adalah invers a.

Contoh 2.1.8 Diberikan $\langle 2\mathbb{Z}, + \rangle$ adalah grup Abelian, sebab sebarang dua bilangan bulat genap bila ditambahkan hasilnya juga genap. Lebih general $\langle n\mathbb{Z}, + \rangle$ adalah grup Abelian untuk setiap $n \in \mathbb{Z}$.

Contoh 2.1.9 Tiga contoh berikut ini $\langle \mathbb{Q}, + \rangle$, $\langle \mathbb{R}, + \rangle$ dan $\langle \mathbb{C}, + \rangle$ adalah grup komutatif.

Contoh 2.1.10 Himpunan bilangan rasional dengan operasi perkalian $\langle Q, \cdot \rangle$ bukan grup. Walaupun sebagian aksiomatik grup dipenuhi, termasuk semua elemen taknol $a \in Q$ punya iners $1/a$. Elemen 0 tidak punya invers terhadap perkalian.

Contoh 2.1.10 menunjukan bahwa $\langle \mathbb{Q}, . \rangle$ bukan grup tetapi pada Contoh 2.1.9, $\langle \mathbb{Q}, + \rangle$ adalah grup. Hal ini mengisyaratkan bahwa suatu grup ditentukan oleh operasi binernya.

Contoh 2.1.11 Misalkan himpunan $Q^* = Q - \{0\}$, maka $\langle Q^*, \cdot \rangle$ adalah grup komutatif. Dengan cara yang sama himpunan $\mathbb{R}^* = \mathbb{R} - \{0\}$, maka $\langle R^*, \cdot \rangle$ adalah grup komutatif.Himpunan $\mathbb{Z}$, walaupun tampa elemen nol terhadap operasi perkalian bukan grup. Untuk setiap bilangan bulat $a \neq \pm 1$ tidak mempunyai invers di $\mathbb{Z}$.

Contoh 2.1.12 Himpunan $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$ dengan operasi penjumlahan adalah grup komutatif. Setiap $a \in \mathbb{Z}_n$ mempunyai invers $n - a$.

Contoh 2.1.13 Diberikan himpunan $\mathbb{U}(n) = \{a \in \mathbb{Z}_n \,|\, \text{fpb}(a, n) = 1\}$ dengan operasi perkalian adalah grup komutatif. Lihat Akibat 1.3.4.

Contoh 2.1.14 Pada contoh himpunan semua akar dari polinomial $x^4 - 1$ terhadap perkalian adalah membentuk grup. Faktanya hal ini berlaku untuk himpunan semua akar dari $x^n - 1$, yaitu $\{1, \omega, \omega^2, \ldots \omega^{n-1}\}$ dimana $\omega = \cos(2\pi/n) + i \sin(2\pi/n)$.

Contoh 2.1.15 Himpunan $z \in \mathbb{C}$ merupakan lingkaran dengan jari-jari satu diberikan oleh

$$S^1 = \{z \in \mathbb{C} \,|\, |z| = 1\} = \{\cos\theta + i\sin\theta \,|\, \theta \in \mathbb{R}\},$$

adalah grup terhadap operasi perkalian bilangan kompleks sebab: Untuk setiap $z_1, z_2 \in S^1$, maka $z_1 = \cos\theta_1 + i\sin\theta_1$ dan $z_2 = \cos\theta_2 + i\sin\theta_2$, didapat

$$z_1 z_2 = (\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2) = \cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2) \in S^1.$$

Terlihat bahwa S^1 tertutup terhadap operasi perkalian. Sifat assosiatif sebagai berikut: Untuk $z_j = \cos\theta_j + i\sin\theta_j \in S^1$ dengan $j = 1, 2, 3$ didapat

$$\begin{aligned}
(z_1 z_2)z_3 &= ((\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2))(\cos\theta_3 + i\sin\theta_3) \\
&= (\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)(\cos\theta_3 + i\sin\theta_3) \\
&= \cos((\theta_1 + \theta_2) + \theta_3) + i\sin((\theta_1 + \theta_2) + \theta_3) \\
&= \cos(\theta_1 + (\theta_2 + \theta_3)) + i\sin(\theta_1 + (\theta_2 + \theta_3)) \\
&= (\cos\theta_1 + i\sin\theta_1)(\cos(\theta_2 + \theta_3) + i\sin(\theta_2 + \theta_3)) \\
&= (\cos\theta_1 + i\sin\theta_1)((\cos\theta_2 + i\sin\theta_2)(\cos\theta_3 + i\sin\theta_3)) \\
&= z_1(z_2 z_3).
\end{aligned}$$

Terlihat dalam S^1 berlaku sifat assosiatif. Sifat elemen netral: $e = 1 = 1 + i0 = \cos 0 + i\sin 0 \in S^1$ dan untuk sebarang $z = \cos\theta + i\sin\theta \in S^1$ didapat

$$ez = 1(\cos\theta + i\sin\theta) = (\cos 0 + i\sin 0)(\cos\theta + i\sin\theta) = \cos\theta + i\sin\theta = z$$

dan

$$ze = (\cos\theta + i\sin\theta)\,1 = (\cos\theta + i\sin\theta)(\cos 0 + i\sin 0) = \cos\theta + i\sin\theta = z.$$

Terlihat bahwa e memenuhi kondisi elemen netral dari S^1. Sifat invers, diberikan sebarang $z = \cos\theta + i\sin\theta \in S^1$ dapat dipilih $z^{-1} = \cos(-\theta) + i\sin(-\theta) \in S^1$ yang memenuhi

$$zz^{-1} = (\cos\theta + i\sin\theta)(\cos(-\theta) + i\sin(-\theta) = \cos 0 + i\sin 0 = 1 = e$$

dan

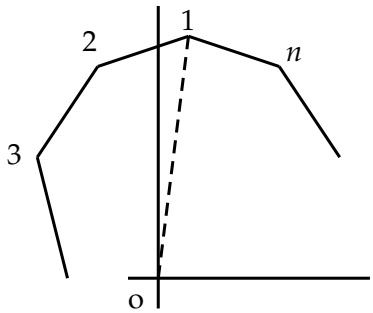
$$z^{-1}z = (\cos(-\theta) + i\sin(-\theta))(\cos\theta + i\sin\theta) = \cos 0 + i\sin 0 = 1 = e.$$

Terlihat bahwa setiap elemen $z = (\cos\theta + i\sin\theta) \in S^1$ mempunyai invers yang diberikan oleh $z^{-1} = (\cos(-\theta) + i\sin(-\theta)) \in S^1$. ●

Contoh 2.1.16 Pada Contoh 2.1.6 dibahas grup D_4 yaitu grup simetri dari persegi. Dengan cara yang sama dapat dikonstruksi grup simetri untuk segi-n beraturan yang dinamakan **grup dihedral** D_n. Misalkan untuk $n \geq 3$, segi-n beraturan pada bidang-x, y dengan pusat di O sebagaimana diberikan oleh Gambar 2.4. Maka bisa diperoleh $2n$ elemen dari D_n sebagai berikut: Misalkan ρ adalah rotasi pada pusat O berlawanan arah jarum jam sebesar $2\pi/n$ radian dan τ adalah pencerminan terhadap sumbu yang melalui pusat O dan titik sudut 1. Maka

$$D_n = \{\rho_0, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \rho\tau, \rho^2\tau, \ldots, \rho^{n-1}\tau\},$$

dimana ρ_0 adalah identitas dan $\rho\tau = \tau\rho^{-1}$. ●



Gambar 2.4: Segi-n beraturan

Pada tiga contoh berikut ini dibahas himpunan matriks berukuran 2×2 dengan elemen-elemen di R, dalam hal ini R dapat berupa $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ atau $\mathbb{Z}_n$.

Contoh 2.1.17 Misalkan $M(2, R)$ adalah himpunan semua matriks berukuran 2×2 dengan elemen-elemen di R. Maka $M(2, R)$ adalah grup terhadap operasi penjumlahan matriks. ●

Contoh 2.1.18 Sebagaimana telah dibahas pada Proposisi 1.5.2 suatu matriks A mempunyai invers bila dan hanya bila $\det(A) \neq 0$. Perlu diperhatikan bahwa, $\det(AB) = \det(A)\det(B)$. Jadi bila A dan B punya invers, maka AB juga punya invers. Misalkan, $GL(2, R)$ adalah himpunan semua matriks berukuran 2×2 dengan determinan taknol. Maka $GL(2, R)$ adalah suatu grup terhadap perkalian matriks. matriks identitas dan invers diberikan oleh

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \text{ dan } A^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & c \end{bmatrix}.$$

Secara umum perkalian matriks tidak komutatif. Jadi $GL(2, R)$ bukan grup komutatif dan dinamakan **grup linier umum**. ●

Contoh 2.1.19 Grup Linier Spesial, $SL(2, R)$ adalah himpunan semua matriks berukuran 2×2 dengan elemen-elemen di R dan $\det(A) = \pm 1$. Grup ini bukan grup komutatif. ●

Dua contoh berikut berkaitan dengan grup berhingga.

Contoh 2.1.20 Grup Empat Klein V yang dapat direpresentasikan oleh empat matriks di $SL(2, R)$, yaitu

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Bila digunakan tabel hasil perkalian matriks di grup V, maka akan diperoleh suatu pola yang tidak sama pada Contoh 2.1.2 dan 2.1.4. ●

Contoh 2.1.21 Grup Quaternion Q_8 dapat direpresentasikan oelh delapan matriks di $SL(2, \mathbb{C})$, $Q_8 = \{\pm I, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$, dimana

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{i} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \mathbf{j} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \mathbf{k} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}.$$

Karena $\mathbf{ij} = \mathbf{k}$ dan $\mathbf{ji} = -\mathbf{k}$, maka Q_8 bukan grup komutatif. ●

Terdapat tidak banyak sifat-sifat dasar grup yang sudah dapat dilihat dari beberapa contoh yang telah dibahas. Misalnya dalam beberapa kasus terlihat bahwa elemen identitas tunggal dan setiap elemen selalu mempunyai elemen invers tunggal. Hal ini bisa dilihat dalam tabel grup pada Contoh 2.1.1 sampai 2.1.4. Untuk pembahasan berikutnya bila dibahas grup abstrak G penulisan $a * b$ ditulis ab dan $\langle G, * \rangle$ cukup ditulis grup G.

Proposisi 2.1.1 Untuk sebarang grup G

(1) Elemen identitas dari G tunggal.

(2) Untuk setiap $a \in G$ invers a^{-1} adalah tunggal.

(3) Untuk sebarang $a \in G$, $(a^{-1})^{-1} = a$.

(4) Untuk sebarang $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

(5) Untuk sebarang $a, b \in G$ persamaan $ax = b$ dan $ya = b$ mempunyai penyelesaian tunggal.

(6) Untuk sebarang $a, bc \in G$ berlaku bila $ac = bc$, maka $a = b$ dan bila $ca = cb$, maka $a = b$. Atau dengan kata lain berlaku hukum kanselasi kanan dan kiri.

Bukti

(1) Misalkan e dan e' adalah elemen identitas di G. Didapat $ee' = e'$ (sebab e elemen identitas di G). Juga $ee' = e$ (sebab e' elemen identitas di G). Terlihat bahwa $e' = e$.

(2) Bila a' dan a'' adalah invers dari $a \in G$, maka

$$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''.$$

(3) Dari $aa^{-1} = e$ dan $(a^{-1})^{-1}a^{-1} = e$, terlihat bahwa inversnya a^{-1} adalah a dan juga $(a^{-1})^{-1}$. Berdasarkan (2) elemen invers adalah tunggal, jadi $a = (a^{-1})^{-1}$.

(4) Dari $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$ dengan cara yang sama didapat $(ab)(b^{-1}a^{-1}) = e$. Terlihat bahawa inversnya (ab) adalah $b^{-1}a^{-1}$, tetapi juga inversnya (ab) adalah $(ab)^{-1}$. Kerena invers adalah tunggal, maka $b^{-1}a^{-1} = (ab)^{-1}$.

(5) Untuk $a, b \in G$, persamaan $ax = b$ berakibat $a^{-1}(ax) = a^{-1}b$. Karena $a^{-1}(ax) = (a^{-1}a)x = ex = x$, didapat $x = a^{-1}b$. Juga, karena a^{-1} adalah tunggal, maka x tunggal. Dengan cara yang sama $ya = b$ berakibat $y = ba^{-1}$ dan y tunggal sebab a^{-1} tunggal.

(6) Dari $ac = bc$ berakibat bahwa $(ac)c^{-1} = (bc)c^{-1}$. Gunankan hukum assosiatif didapat $a = c$. Juga dengan cara yang sama $ca = cb$ berakibat $a = c$. ✓

Untuk bilangan bulat positip n, penulisan $\underbrace{a \cdot a \cdots a}_{\text{sebanyak } n}$ ditulis a^n dan $\underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{\text{sebanyak } n}$ ditulis a^{-n}, sedangkan $a^0 \stackrel{\text{def}}{=} e$. Bila operasi pada grup adalah penjumlahan a^n ditulis na untuk $n \in \mathbb{Z}$.

Contoh 2.1.22 Dalam grup $\mathbb{U} = \{1, 2, 4, 5, 7, 8\}$ terhadap perkalian mod 9, didapat

$$2 \cdot 5 = 1,\ 4 \cdot 7 = 1 \text{ dan } 8 \cdot 8 = 1.$$

Terlihat bahwa $5 = 2^{-1}, 7 = 4^{-1}$ dan $8 = 8^{-1}$. Juga, $8^{-1} = (2 \cdot 4)^{-1} = 4^{-1} \cdot 2^{-1} = 7 \cdot 5 = 8$. ●

Contoh 2.1.23 Dalam grupsimetri dari segitiga, S_3 Contoh 2.1.5, didapat $\rho\mu_1 = \mu_3, \mu_1^{-1} = \mu_1, \rho_{-1} = \rho^2, \mu_3^{-1} = \mu_3$ dan $(\rho\mu_1)^{-1} = \mu_3^{-1} = \mu_3 = \mu_1\rho^2 = \mu_1^{-1}\rho^{-1}$. ●

Contoh berikut membahas bagaimana mengkonstruksi grup abstrak dengan menggunakan suatu tabel grup.

Contoh 2.1.24 Diberikan grup abstrak G dengan tiga elemen. Ada berapa banyak tabel grup yang mungkin terjadi? Misalkan grup $G = \{e, a, b\}$ dengan $e \neq a \neq b$ dan e adalah elemen identitas dari G. Karena G adalah grup, maka berlaku aksiomatik tertutup, jadi $ab, ba, aa, bb \in G$. Bila $ab = a$, maka $b = e$. Jadi $ab \neq a$. Bila $ab = b$ maka $a = e$. Juga didapat $ab \neq b$. Jadi haruslah $ab = e$, dengan cara yang sama didapat $ba = e$. Selanjutnya, bila $aa = e$, maka $aa = ab$. Dengan hukum kanselasi didapat $a = b$ (tidak mungkin). Jadi $aa \neq e$. Bila $aa = a$, maka $a = e$ (tidak mungkin). Jadi haruslah $aa = b$. dengan cara yang sama didapat $bb = a$. Dengan demikian tabel grup yang mungkin diberikan oleh Tabel 2.5.

Tabel 2.5: Grup abstrak G, dengan $|G| = 3$

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Tabel grup dari sebarang grup dengan elemen sebanyak tiga harus mempunyai bentuk Tabel 2.5 walaupun elemen-elemenya berbeda. Hal ini bisa dibandingkan dengan tabel dalam Contoh 2.1.1 dan 2.1.3. ●

Definisi 2.1.3 Banyaknya elemen dari grup G dinamakan **order** G dan dinotasikan oleh $|G|$. Grup G **berhingga** bila $|G|$ berhingga. ✓

Jadi $\mathbb{Z}$ dan $n\mathbb{Z}$ adalah grup dengan order tak-berhingga, sedangkan $|\mathbb{U}(12)| = 4, |S_3| = 6, |D_4| = 8, |V| = 4, |Q_8| = 8$ dan $|\mathbb{Z}_n| = n$ adalah grup dengan order berhingga.

Contoh 2.1.25 Fungsi-ϕ Euler $\phi(n)$ untuk bilangan bulat $n \geq 2$ didefinisikan sebagai banyaknya semua bilangan positip s dengan $1 \leq s \leq n$ dan fpb$(s, n) = 1$. Jadi, untuk sebarang bilangan bulat $n \geq 2$ didapat $|\mathbb{U}(n)| = \phi(n)$ dan untuk bilangan prima p didapat $|\mathbb{U}(p)| = p - 1 = \phi(p)$. ●

Latihan

Latihan 2.1.1 Tunjukan himpunan G dengan operasi yang diberikan memenuhi aksiomatik dari definisi grup.

1. $G = 2\mathbb{Z}$ dengan operasi penjumlahan.
2. $G = \mathbb{Z}_5$ dengan operasi penjumlahan mod 5.
3. $G = \mathbb{U}(10)$ dengan operasi perkalian mod 10.

4. $G = \mathbb{C}^* = \mathbb{C} - \{0\}$ dengan operasi perkalian bilangan kompleks.
5. $G = GL(2, \mathbb{Q})$ dengan operasi perkalian matriks. ✓

Latihan 2.1.2 Buat tabel grup untuk grup yang diberikan berikut dan tentukan komutatif atau tidak.

1. $G = S_3$ (lihat Contoh 2.1.5).
2. $G = D_4$ (lihat Contoh 2.1.6).
3. $G = V$ (lihat Contoh 2.1.20).
4. $G = Q_8$ (lihat Contoh 2.1.21). ✓

Latihan 2.1.3 Tunjukkan bahwa $GL(2, Q)$ tidak komutatif. ✓

Latihan 2.1.4 Tunjukkan bahwa bila G adalah grup komutatif, maka untuk semua $a, b \in G$ dan untuk semua bilangan bulat n, $(ab)^n = a^n b^n$. ✓

Latihan 2.1.5 Dalam S_3 dapatkan elemen-elemen a, b sedemikian hingga $(ab)^2 \neq a^2 b^2$. ✓

Latihan 2.1.6 Dalam S_3 dapatkan semua elemen a sedemikian hingga $a^2 = \rho_0 =$ identitas dan semua elemen b sedemikian hingga $b^3 = \rho_0$. ✓

Latihan 2.1.7 Dapatkan invers masing-masing elemen dari $\mathbb{U}(10)$ dan $\mathbb{U}(15)$. ✓

Latihan 2.1.8 Misalkan G adalah grup perkalian dari akar-akar polinomial $x^n - 1$. Bila $a \in G$, maka tentukan a^{-1} (lihat Contoh 2.1.14). ✓

Latihan 2.1.9 Dalam D_4 dapatkan invers dari ρ, τ dan $\rho\tau$ (lihat Contoh 2.1.6). ✓

Latihan 2.1.10 Dalam grup Klein-4, tunjukkan bahwa setiap elemen mempunyai invers dirinya sendiri. ✓

Latihan 2.1.11 Tunjukkan bahwa bila setiap elemen dari suatu grup G mempunyai invers dirinya sendiri, maka G adalah komutatif. ✓

Latihan 2.1.12 Meniru Contoh 2.1.24, konstruksi semua tabel grup yang mungkin untuk suatu grup G dengan order 4. ✓

Latihan 2.1.13 Konstruksi semua tabel grup yang mungkin untuk suatu grup G berorder 5. (Petunjuk: pertama tunjukkan bahwa untuk sebarang $a \in G$, $a \neq e$, didapat $a^k \neq e$ untuk semua bilangan bulat $1 \leq k < 5$). ✓

Latihan 2.1.14 Berapakah order dari grup $GL(2, \mathbb{Z}_2)$? ✓

Latihan 2.1.15 Tunjukkan bahwa bila G adalah grup berhingga berorder genap, maka G mempunyai suatu elemen $a \neq e$ yang memenuhi $a^2 = e$. ✓

Latihan 2.1.16 Dalam dihedral grup D_n $n \geq 3$, tunjukkan bahwa $\rho\tau = \tau\rho^{-1}$ (lihat Contoh 2.1.16). ✓

Latihan 2.1.17 Tunjukkan bahwa, suatu grup berhingga adalah komutatif bila dan hanya bila mempunyai grup tabel adalah suatu **matriks simetri**, yaitu matriks $\{a_{i,j}\}$ dimana $a_{i,j} = a_{j,i}$ untuk semua i dan j.

Latihan 2.1.18 Misalkan G adalah suatu grup, $a \in G$ dan m, n bilangan bulat prima relatif. Tunjukkan bahwa bila $a^m = e$, maka ada suatu elemen $b \in G$ yang memenuhi $a = b^n$.

Latihan 2.1.19 Misalkan G adalah grup berhingga komutatif sedemikian hingga untuk semua $a \in G$, $a \neq e$ didapat $a^2 = e$. Bila $a_1, a_2, \ldots, a_n$ adalah semua elemen dari G yang berbeda, maka hitung $a_1 a_2 \cdots a_n$.

Latihan 2.1.20 Tunjukkan bahwa semua elemen taknol di $\mathbb{Z}_p$ dengan p bilangan prima membentuk suatu grup terhadap perkalian mod p.

Latihan 2.1.21 (**Teorema Wilson**) Buktikan bahwa bila p prima, maka $(p-1)! \equiv -1 \mod p$.

2.2 Subgrup

Dalam beberapa contoh yang dibahas pada bagian sebelumnya, himpunan elemen-elemen dari grup adalah suatu himpunan bagian dari suatu grup yang lain dengan operasi yang sama.

Contoh 2.2.1 Himpunan bilangan genap $2\mathbb{Z}$ adalah himpunan bagian dari $\mathbb{Z}$, dan keduanya adalah grup terhadap operasi penjumlahan.

Contoh 2.2.2 Himpunan akar-akar polinomial $x^4 - 1$, yaitu $\{\pm 1, \pm i\}$ adalah himpunan bagian dari himpunan bilangan kompleks taknol $\mathbb{C}^*$, keduanya adalah grup terhadap perkalian bilangan kompleks.

Contoh 2.2.3 Diberikan grup

$$\mathbb{Z}_8 = \{[0]_8, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}$$

dan himpunan bagian

$$H = \{[0]_8, [2]_8, [4]_8, [6]_8\} \subset \mathbb{Z}_8.$$

Maka H juga grup dengan operasi penjumlahan mod 8. Tabel grup sebagaimana diberikan oleh Tabel 2.6.

Tabel 2.6: Grup H

+	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$
$[0]_8$	$[0]_8$	$[2]_8$	$[4]_8$	$[6]_8$
$[2]_8$	$[2]_8$	$[4]_8$	$[6]_8$	$[0]_8$
$[4]_8$	$[4]_8$	$[6]_8$	$[0]_8$	$[2]_8$
$[6]_8$	$[6]_8$	$[0]_8$	$[2]_8$	$[4]_8$

Himpunan bagian dari suatu grup G yang merupakan grup terhadap oprasi yang sama seperti di G memainkan suatu peranan penting untuk identifikasi grup-grup yang berbeda.

Definisi 2.2.1 Suatu himpunan bagian tak-kosong H dari suatu grup G adalah suatu **subgrup** dari G bila H terhadap operasi yang sama di G adalah grup. Dalam hal ini ditulis $H \leq G$, bila $H \subseteq G$ dan ditulis $H < G$, bila $H \subset G$.

Contoh 2.2.4 $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ terhadap operasi penjumlahan.

Contoh 2.2.5 $\mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$ terhadap operasi perkalian.

Contoh 2.2.6 Untuk sebarang grup G dengan elemen identitas e, $\{e\}$ adalah subgrup dari G dinamakan **trivial subgrup** dan G sendiri adalah subgrup dari G dinamakan **subgrup tak-sejati**. Sebarang subgrup selain $\{e\}$ dan G sendiri dinamakan **subgrup sejati tak-trivial**.

Contoh 2.2.7 Himpunan $\{\pm 1\} < \{\pm 1, \pm i\}$ terhadap operasi perkalian.

Contoh 2.2.8 Himpunan $\{\rho_0, \rho, \rho^2\} < S$ terhadap operasi komposisi fungsi.

Untuk membuktikan bahwa suatu himpunan bagian H dari suatu grup G membentuk suatu grup, dibuktikan bahwa empat aksiomatik grup dipenuhi. Hal ini akan merumitkan dalam berbagai kasus, oleh karena itu untuk memudahkannya dibuktikan teorema berikut.

Teorema 2.2.1 (Test Subgrup) Suatu himpunan bagian tak-kosong H dari suatu grup G adalah subgrup dari G bila dan hanya bila kondisi berikut dipenuhi:

$$ab^{-1} \in H, \text{ untuk setiap } a, b \in H. \tag{2.1}$$

atau

$$a^{-1}b \in H, \text{ untuk setiap } a, b \in H. \tag{2.2}$$

Bukti ($\Rightarrow$) Asumsikan H adalah suatu subgrup dari G dan ambil sebarang $a, b \in H$. Karena H subgrup setiap elemen di H mempunyai invers, jadi $b^{-1} \in H$. Lagi, karena H subgrup, maka H tertutup terhadap operasi yang berlaku, jadi $ab^{-1} \in H$. ($\Leftarrow$) Misalkan kondisi (2.1) dipenuhi. Didapat, karena H tak-kosong, maka ada $a, b = a \in H$ dan gunakan kondisi (2.1) didapat $e = aa^{-1} = ab^{-1} \in H$ Jadi H memuat elemen identitas. Selanjutnya untuk setiap $b \in H$ dan karena $a = e \in H$, gunakan lagi kondisi (2.1) didapat $b^{-1} = eb^{-1} = ab^{-1} \in H$. Terlihat bahwa setiap elemen di H punya invers. Berikutnya, untuk setiap $a, b \in H$ dan karena $b^{-1} \in H$, maka untuk $a, b^{-1} \in H$ gunakan kondisi (2.1) didapat $ab = a(b^{-1})^{-1} \in H$. Jadi H memenuhi kondisi tertutup. Operasi pada H adalah assosiatif, sebab sifat ini diwarisi dari sifat grup G. Sejalan dengan yang telah dilakukan, ($\Rightarrow$) asumsikan H adalah suatu subgrup dari G dan ambil sebarang $a, b \in H$. Karena H subgrup setiap elemen di H mempunyai invers, jadi $a^{-1} \in H$. Lagi, karena H subgrup, maka H tertutup terhadap operasi yang berlaku, jadi $a^{-1}b \in H$. ($\Leftarrow$) Misalkan kondisi (2.2) dipenuhi. Didapat, karena H tak-kosong, maka ada $b = a, b \in H$ dan gunakan kondisi (2.2) didapat $e = b^{-1}b = a^{-1}b \in H$. Jadi H memmuat elemen identitas. Selanjutnya untuk setiap $a \in H$ dan karena $b = e \in H$, gunakan lagi kondisi (2.2) didapat $a^{-1} = a^{-1}e = a^{-1}b \in H$. Terlihat bahwa setiap elemen di H punya invers. Berikutnya, untuk setiap $a, b \in H$ dan karena $a^{-1} \in H$, maka untuk $a^{-1}, b \in H$ gunakan kondisi (2.2) didapat $ab = (a^{-1})^{-1}b \in H$. Jadi H memenuhi kondisi tertutup. Juga, operasi pada H adalah assosiatif, sebab sifat ini diwarisi dari sifat grup G.

Catatan bahwa, bila operasi pada grup adalah penjumlahan, maka kondisi (2.1) ditulis sebagai

$$a - b \in H, \text{ untuk setiap } a, b \in H.$$

Contoh 2.2.9 Untuk sebarang bilangan bulat $n \geq 0$, $n\mathbb{Z}$ adalah subgrup dari $\mathbb{Z}$ terhadap operasi penjumlahan. Sebab, bila $a, b \in \mathbb{Z}$, maka $a = nr$ untuk beberapa bilangan bulat r dan $b = ns$ untuk beberapa bilangan bulat s. Didapat, $a - b = nr - ns = n\underbrace{(r-s)}_{\in\mathbb{Z}} \in n\mathbb{Z}$.

Contoh 2.2.10 Himpunan bilangan bulat ganjil H bukan suatu subgrup dari grup $\mathbb{Z}$ terhadap perkalian. Sebab, $1, 5 \in H$, tetapi $-4 = 1 - 5 \notin H$.

Alternatif lain untuk test subgrup teorema berikut dapat digunakan.

Teorema 2.2.2 Suatu himpunan bagian tak-kosong H dari suatu grup G adalah subgrup bila dan hanya bila pernyataan berikut dipenuhi:

(1) (Tertutup) $ab \in H$, untuk setiap $a, b \in H$.

(2) (Invers) Untuk setiap $b \in H$, $b^{-1} \in H$.

Bukti ($\Rightarrow$) Bila H subgrup, maka kondisi tertutup dan invers dipenuhi sebab semua aksiomatik grup dipenuhi oleh H. ($\Leftarrow$) Asumsikan kondisi tertutup dan invers dipenuhi di H. Misalkan $a, b \in H$, didapat $b^{-1} \in H$. Jadi $ab^{-1} \in H$ (menggunakan kondisi tertutup). Selanjutnya digunakan Teorema TeoriSubgrup, didapat bahwa H adalah subgrup dari grup G.

Contoh 2.2.11 Himpunan $SL(2, \mathbb{Q})$ adalah subgrup dari grup $GL(2, \mathbb{Q})$. Bila $A \in SL(2, \mathbb{Q})$, maka $\det(A) = 1$, jadi $\det(A^{-1}) = \pm 1/\det(A) = 1/\pm 1 = \pm 1$. Jadi $A^{-1} \in Sl(2, \mathbb{Q})$. Selanjutnya bila $A, B \in SL(2, \mathbb{Q})$, maka $\det(AB) = \det(A) \cdot \det(B) = \pm 1 \cdot \pm 1 = \pm 1$, jadi $AB \in SL(2, \mathbb{Q})$. Dengan menggunakan Teorema 2.2.2 didapat $SL(2, \mathbb{Q})$ adalah subgrup dari $GL(2, \mathbb{Q})$.

Teorema 2.2.3 Misalkan G adalah suatu grup dan $H \subset G$ dengan H berhingga. Maka H adalah subgrup dari G bila dan hanya bila memenuhi (Tertutup) $ab \in H$ untuk sebarang $a, b \in H$.

Bukti Menggunakan Teorema 2.2.2 hanya butuh menunjukkan sifat tertutup berakibat kondisi invers dipenuhi. Jadi asumsikan kondisi tertutup dipenuhi dan misalkan sebarang $a \in H$. Bila $a = e$, maka $a^{-1} = e^{-1} = e = a \in H$. Bila $e \neq e$, perhatikan pangkat berikut $a = a^1, a^2, a^3, a^4, \ldots$. Kondisi tertutup berakibat $a^i \in H$ untuk semua i. Karena H berhingga, ada beberapa pangkat-pangkat tersebut yang sama. Oleh karena itu ada beberapa i dan j dengan $i < j$ dan $a^i = a^j$ atau $a^{(i-j)} = a^i(a^j)^{-1} = a^i a^{-j} = e$. Jadi $aa^{(i-j-1)} = e$. Terlihat $a^{-1} = a^{(i-j-1)} \in H$. Dengan demikian kondisi invers dipenuhi.

Definisi 2.2.2 Misalkan G adalah suatu grup dan $a \in G$. Didefinisikan himpunan

$$\langle a \rangle \stackrel{\text{def}}{=} \{a^n \mid n \in \mathbb{Z}\}.$$

Bila operasi dalam grup adalah penjumlahan, maka

$$\langle a \rangle \stackrel{\text{def}}{=} \{na \mid n \in Z\}.$$

Proposisi 2.2.1 Misalkan G adalah suatu grup dan $a \in G$. Maka $\langle a \rangle$ adalah suatu subgrup dari G, yang dinamakan **subgrup siklik dibangun oleh** a.

Bukti Misalkan $x, y \in \langle a \rangle$, maka $x = a^m, y = a^n$ untuk beberapa $m, n \in \mathbb{Z}$. Didapat $xy^{-1} = x^m(a^n)^{-1} = a^{m-n}$. Karena $m - n \in \mathbb{Z}$, maka $xy^{-1} \in \langle a \rangle$. Dengan demikian $\langle a \rangle$ adalah subgrup dari grup G.

Contoh 2.2.12 Dalam $\mathbb{Z}$ subgrup yang dibangun oleh 3 adalah $\langle 3 \rangle = 3\mathbb{Z}$.

Contoh 2.2.13 Dalam grup $\mathbb{C}^*$ subgrup yang dibangun oleh i adalah $\langle i \rangle = \{i, i^2, i^3, i^4\} = \{i, -1, -i, 1\}$.

Contoh 2.2.14 Dalam S_3 subgrup yang dibangun oleh ρ adalah $\langle rho \rangle = \{\rho_0, \rho, \rho^2\}$.

Contoh 2.2.15 Dalam D_4, $\langle \rho \rangle = \{\rho_0, \rho, \rho^2, \rho^3\}$ dan $\langle \tau \rangle = \{\rho_0, \tau\}$.

Contoh 2.2.16 Semua subgrup dari $\mathbb{Z}_6$ adalah:
$\{0\}$, subgrup trivial.
$\{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\} = \mathbb{Z}_6$, subgrup taksejati.
$\{[0]_6, [2]_6, [4]_6\} = \langle [2]_6 \rangle = \langle [4]_6 \rangle$
$\{[0]_3, [3]_6\} = \langle [3]_6 \rangle$.
Catatan bahwa, bila H adalah suatu subgrup dan $5 \in H$, maka $-5 = 1 \in H$ dan bila $2, 3 \in H$, maka $3 - 2 = 1 \in H$. Dalam hal yang demikian $H = \mathbb{Z}_6$. Jadi semua subgrup dari $\mathbb{Z}_6$ telah dibuat.

Pengertian berikut yang dikenalkan adalah penting sekali untuk kajian grup.

Definisi 2.2.3 Misalkan G adalah suatu grup dan $a \in G$. **order** elemen a ditulis $|a|$ adalah bilangan bulat positip terkecil n yang memenuhi $a^n = e$ atau takberhingga bila n tidak ada. Bila operasi pada grup adalah penjumlahan $a^n = e$ ditulis $na = e$.

Contoh 2.2.17 Dalam S_3, $|\mu_1| = 2, |\rho| = 3$.

Contoh 2.2.18 Dalam $\mathbb{Z}_6$, $|[0]_6| = 1, |[1]_6| = |[5]_6| = 6, |[2]_6| = |[4]_6| = 3, |[3]_6| = 2$.

Contoh 2.2.19 Dalam $\mathbb{Z}$, $|0| = 1$ dan $|n|$ takhingga untuk semua $n \neq 0$.

Contoh 2.2.20 Dalam $\mathbb{C}^*$, $|i| = 4$.

Sebelum mengakhiri bagian ini, dikenalkan subgrup yang sangat penting dari suatu grup G.

Definisi 2.2.4 Misalkan G sebarang grup. Maka **senter** dari G ditulis $Z(G)$, ada himpunan bagian dari G yang elemen-elemennya komutatif dengan semua elemen G, dengan kata lain

$$Z(G) \stackrel{\text{def}}{=} \{x \in G \mid xy = yx, \text{ untuk semua } y \in G\}.$$

Catatan bahwa, $ey = y = ye$ untuk semua $y \in G$. Jadi $e \in Z(G)$ dengan demikian $Z(G) \neq \emptyset$.

Teorema 2.2.4 Senter $Z(G)$ dari suatu grup G adalah subgrup dari G.

Bukti Cukup dibuktikan memenuhi tertutup dan invers. Misalkan $a, b \in Z(G)$, maka $ax = xa$ untuk semua $x \in G$ dan $bx = xb$ untuk semua $x \in G$. Didapat

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab).$$

Terlihat bahwa $ab \in Z(G)$. Selanjutnya diberikan sebarang $a \in Z(G)$, maka $ay = ya$ untuk semua $y \in G$. Didapat $a^{-1}y = a^{-1}(y^{-1})^{-1} = (y^{-1}a)^{-1} = (ay^{-1})^{-1} = (y^{-1})^{-1}a^{-1} = ya^{-1}$. Terlihat bahwa $a^{-1} \in Z(G)$.

Catatan bahwa, bila G grup komutatif, maka $Z(G) = G$.

Contoh 2.2.21 Misalkan dicari senter dari grup takkomutatif D_4 (Contoh 2.1.6),

$$D_4 = \{\rho_0, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}.$$

Didapat $\tau\rho = \rho^3\tau$, jadi $\rho \notin Z(D_4)$ dan $\rho^3 \notin Z(D_4)$. Dilain pihak, didapat

$$\tau\rho^2 = (\tau\rho)\rho = (\rho^3\tau)\rho = \rho^3(\tau\rho) = \rho^3(\rho^3\tau) = (\rho^3\rho^3)\tau = \rho^2\tau.$$

Maka, mudah ditunjukkan bahwa ρ^2 komutatif dengan semua elemen dari D_4. Jadi $\rho^2 \in Z(D_4)$. Selanjutnya, didapat

$$\begin{aligned} (\rho\tau)\rho = \rho(\rho^3\tau) = \tau &\neq \rho^2\tau = \rho(\rho\tau) \\ (\rho^2\tau)\rho = \rho^2(\rho^3\tau) = \rho\tau &\neq \rho^3\tau = \rho(\rho^2\tau) \\ (\rho^3\tau)\rho = \rho^3(\rho^3\tau) = \rho^2\tau &\neq \tau = \rho(\rho^3\tau). \end{aligned}$$

Jadi $Z(D_4) = \{\rho_0, \rho^2\}$.

Subgrup penting lainnya diberikan oleh definisi berikut.

Definisi 2.2.5 Misalkan G adalah suatu grup dan $a \in G$. Maka **sentralisir** dari $a \in G$ dinotasikan oleh $C_G(a)$ didefinisikan sebagai berikut:

$$C_G(a) = \{x \in G \,|\, ax = xa\}.$$

Catatan bahwa, untuk sebarang $a \in G$ didapat $Z(G) \subseteq C_G(a)$. Hal ini berarti bahwa senter dari G termuat dalam sentralisir sebarang elemen.

Untuk grup yang sudah jelas, penulisan $C_G(a)$ cukup ditulis $C(a)$.

Contoh 2.2.22 Misalkan dicari sentralisir dari ρ dalam S_3. Jelas $\rho_0, \rho, \rho^2 \in C(\rho)$. Juga $\rho\mu_1 \neq \mu_1\rho$. Dapat dihitung pula $\rho\mu_2 = \mu_1$ sedangkan $\mu_2\rho = \mu_3$. jadi $\rho\mu_2 \neq \mu_2\rho$. Juga, $\rho\mu_3 = \mu_2$ dan $\mu_3\rho = \mu_1$. Jadi $\mu_3\rho \neq \rho\mu^3$. Dengan demikian $C(\rho) = \{\rho_0, \rho, \rho^2\}$.

Latihan

Latihan 2.2.1 Dapatkan order elemen dari grup yang berikut ini.

1. $2 \in \mathbb{Z}_3$
2. $4 \in \mathbb{Z}_{10}$
3. $\mu_2 \in S_3$
4. $\rho \in D_4$
5. $\rho^2\tau \in D_4$
6. $(-1 + \sqrt{3}i)/2 \in \mathbb{C}^*$
7. $\mathbf{j} \in Q_8$
8. $-i \in \mathbb{C}^*$
9. $(-1 - \sqrt{3}i)/2 \in \mathbb{C}^*$
10. $\cos(2\pi/7) + i\sin(2\pi/7) \in \mathbb{C}^*$.

Latihan 2.2.2 Dapatkan setidaknya dua subgrup sejati taktrivial dari grup berikut.

1. $\mathbb{Z}$
2. $\mathbb{Q}$
3. $\mathbb{C}^*$
4. $\mathbb{Z}_8$
5. S_3
6. D_4
7. $8\mathbb{Z}$
8. $GL(2, \mathbb{Q})$
9. Q_8.

Latihan 2.2.3 Misalkan G adalah suatu grup. Tunjukkan bahwa $\langle a \rangle = \left\langle a^{-1} \right\rangle$ dan $|a| = |a^{-1}|$.

Latihan 2.2.4 Misalkan $G = \{a + b\sqrt{2}i \mid a, b \in \mathbb{Q}\}$. Tunjukkan bahwa G adalah subgrup dari $\mathbb{R}$ terhadap operasi penjumlahan.

Latihan 2.2.5 Misalkan $G = \{n + mi \mid m, n \in \mathbb{Z}, i^2 = -1\}$. Tunjukkan bahwa G adalah subgrup dari $\mathbb{C}$ terhadap operasi penjumlahan.

Latihan 2.2.6 Misalkan $G = \{\cos(2k\pi/7) + i\sin(2k\pi/7), \mid k \in \mathbb{Z}\}$. Tunjukkan bahwa G adalah subgrup dari $\mathbb{C}^*$ terhadap operasi perkalian. Berapakah $|G|$?

Latihan 2.2.7 Misalkan $G = \{a + bi \mid a, b \in \mathbb{R}, a^2 + b^2 = 1\}$. Tentukan apakah G subgrup dari $\mathbb{C}^*$ atau bukan subgrup terhadap operasi perkalian.

Latihan 2.2.8 Untuk $\theta \in \mathbb{R}$, misalkan $A(\theta) \in SL(2, \mathbb{R})$ adalah matriks representasi dari suatu rotasi θ radian:

$$A(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

(a) Tunjukkan bahwa $H = \{A(\theta) \mid \theta \in \mathbb{R}\}$ adalah suatu subgrup dari $SL(2, \mathbb{R})$.

(b) Dapatkan invers dari $A(2\pi/3)$.

(c) Dapatkan order dari $A(2\pi/3)$.

Latihan 2.2.9 Dalam $SL(2, \mathbb{Z}_{10})$, misalkan

$$A = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}.$$

(a) Hitung A^3 dan A^{11}.

(b) Dapatkan order dari A.

Latihan 2.2.10 Dalam $Sl(3,\mathbb{R})$, untuk sebarang $a, b \in \mathbb{R}$, misalkan

$$D(a,b,c) = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}.$$

Tunjukkan bahwa $H = \{D(a,b,c) \,|\, ab, c \in \mathbb{R}\}$ adalah subgrup dari $SL(3,\mathbb{R})$.

Latihan 2.2.11 Tunjukkan bahwa dalam suatu grup komutatif G, himpunan yang semua elemen-elemennya mempunyai order berhingga di G adalah subgrup dari G.

Latihan 2.2.12 Tunjukkan bahwa bila H dan K adalah subgrup dari G, maka $H \cap K$ adalah subgrup dari G.

Latihan 2.2.13 Tunjukkan bahwa bila G adalah suatu grup dan sebarang elemen-elemen $a, b \in G$, maka $|aba^{-1}| = |b|$.

Latihan 2.2.14 Tunjukkan bahwa bila G adalah suatu grup dan sebarang elemen-elemen $a, b \in G$, maka $|ab| = |ba|$.

Latihan 2.2.15 Misalkan G adalah suatu grup dan $a \in G$. Tunjukkan bahwa sentralisir dari a, $C_G(a)$ adalah subgrup dari G.

Latihan 2.2.16 Dapatkan sentralisir $C(\mu_1)$ di S_3.

Latihan 2.2.17 Dapatkan sentralisir $C(\rho^2)$ di D_4.

Latihan 2.2.18 *Misalkan bahwa G adalah suatu grup dan $a \in G$. Tunjukkan bahwa $C(a) = G$ bila dan hanya bila $a \in Z(G)$.*

Latihan 2.2.19 Dapatkan senter $Z(S_3)$ dari grup S_3.

Latihan 2.2.20 Diberikan grup G dan $H \subset G$ dengan $H \neq \emptyset$. Tunjukkan bahwa H adalah subgrup dari G bila dan hanya bila berlaku

$$a^{-1}b \in H, \text{ untuk setiap } a, b \in H.$$

2.3 Grup Siklik

Pada bagian ini dibahas kajian dari grup khusus yang dinamakan *grup siklik*. Dalam pembahasan sebelumnya sudah dikenalkan pengertian subgrup siklik $\langle a \rangle$ dari suatu grup G yang dibangun oleh suatu elemen a.

Contoh 2.3.1 Sudah diperlihatkan bahwa dalam $\mathbb{Z}_6$ subgrup yang dibangun oleh $[1]_6$ adalah $\mathbb{Z}_6$ sendiri, juga dibangun oleh $[5]_6$. Jadi $\mathbb{Z}_6 = \langle [1]_6 \rangle = \langle [5]_6 \rangle$.

Contoh 2.3.2 Dalam $\mathbb{Z}$, subgrup yang dibangun oleh 1 dan -1 adalah $\mathbb{Z}$ sendiri, jadi $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

Contoh 2.3.3 Dalam $G = \{1, i, -1, -i\}$, subgrup yang dibangun oleh i dan $-i$ adalah G sendiri. Jadi $G = \langle i \rangle = \langle -i \rangle$.

Contoh-contoh yang baru saja dibahas adalah grup siklik. Berikut ini secara formal diberikan pengertian grup siklik.

Definisi 2.3.1 Suatu grup G dinamakan grup **siklik** bila ada suatu elemen $a \in G$ sedemikian rupa sehingga $G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$. Dalam hal ini elemen a dinamakan suatu **generator** dari G.

Bila operasi pada grup adalah penjumlahan kondisi $G = \{a^n \mid n \in \mathbb{Z}\}$ ditulis $G = \{na \mid n \in \mathbb{Z}\}$. Ketika menghitung $\langle a \rangle$ untuk suatu elemen a di G, dihitung berturut-turut pangkat dari a. Sedangkan bila operasi pada grup adalah penjumlahan, maka dihitung berturut-turut kelipatan dari a. Bila semua hasil hitungan memberikan semua elemen-elemen dari G, maka G dibangun oleh a.

Contoh 2.3.4 Untuk sebarng bilangan bulat $n > 1$, maka $\mathbb{Z}_n = \langle [1]_n \rangle = \langle [n-1]_n \rangle$ adalah grup siklik berorder n.

Contoh 2.3.5 Diberikan $\mathbb{Z}_{[1]_{10}} = \langle [1]_{10} \rangle = \langle [3]_{10} \rangle = \langle [1]_7 \rangle = \langle [9]_{10} \rangle$, terlihat bahwa semua generator dari $\mathbb{Z}_{10}$ adalah $[1]_{10}, [3]_{10}, [7]_{10}$ dan $[9]_{10}$. Akan diperlihat menghitung kelipatan dari $[3]_{10}$ secara berturutan sebagai berikut. Dimulai dari $1 \cdot [3]_{10} = [3]_{10}$ dan berikutnya $2 \cdot [3]_{10} = [6]_{10}$, $3 \cdot [3]_{10} = [9]_{10}$, $4 \cdot [3]_{10} = [12]_{10} = [2]_{10}$, $5 \cdot [3]_{10} = [15]_{10} = [5]_{10}$, $6 \cdot [3]_{10} = [18]_{10} = [8]_{10}$, $7 \cdot [3]_{10} = [21]_{10} = [1]_{10}$, $8 \cdot [3]_{10} = [24]_{10} = [4]_{10}$, $9 \cdot [3]_{10} = [27]_{10} = [7]_{10}$, $10 \cdot [3]_{10} = [30]_{10} = [0]_{10}$. Terlihat penghitungan kelipatan dari $[3]_{10}$ secara berturut-turut menghasilkan semua elemen-elemen di $\mathbb{Z}_{10}$, jadi $[3]_{10}$ adalah generator dari $\mathbb{Z}_{10}$. Perlakuan yang serupa akan memberikan hasil yang sama bila dilakukan pada elemen $[1]_{10}, [7]_{10}$ dan $[9]_{10}$.

Contoh 2.3.6 Juga, $\mathbb{U}(10) = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\} = \{[3]^0_{10}, [3]^1_{10}, [3]^2_{10}, [3]^3_{10}\} = \langle [3]_{10} \rangle$.

Berikut ini diberikan grup yang tidak siklik.

Contoh 2.3.7 Dalam S_3, $\langle \rho \rangle = \left\langle \rho^2 \right\rangle = \{\rho_0, \rho, \rho^2\}$ dan $\langle \mu_i \rangle = \{\rho_0, \mu_i\}$, $i = 1, 2, 3$. Jadi tak ada elemen dari S_3 yang membangun S_3 sebagai grup. Dengan demikian S_3 bukan grup siklik.

Contoh 2.3.8 Grup $2\mathbb{Z} = \langle 2 \rangle$, secara umum, untuk setiap $n \geq 1$ didapat $n\mathbb{Z} = \langle n \rangle$. Semua grup ini adalah grup siklik takberhingga.

Contoh 2.3.9 Grup $\mathbb{Z}_{10} \neq \langle [2]_{10} \rangle = \{[0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10}\}$. Penghitungan kelipatan dari $[2]_{10}$ secara berturutan sampai 5 kali menghasilkan semua elemen di $\langle [2]_{10} \rangle$. Bila hal ini dilanjutkan didapat

$$6[2]_{10} = [2]_{10},\ 7[2]_{10} = [4]_{10},\ 8[2]_{10} = [6]_{10},\ 9[10]_{10} = [8]_{10},\ 10[2]_{10} = [0]_{10}.$$

Terlihat menghasilkan pola yang berulang lagi.

Teorema berikut menjelaskan bahwa pengulangan bentuk dalam contoh yang baru saja dibahas terjadi secara umum.

Teorema 2.3.1 Misalkan G adalah suatu grup dan $a \in G$. Maka untuk semua $i, j \in \mathbb{Z}$ didapat

(1) Bila a mempunyai order takhingga, maka $a^i = a^j$ bila dan hanya bila $i = j$.

(2) Bila a mempunyai order berhingga, maka $a^i = a^j$ bila dan hanya bila n membagi $i - j$.

Bukti

(1) Misalkan a mempunyai order takhingga. Bila $i = j$, maka jelas $a^i = a^j$. Sebaliknya, bila $a^i = a^j$, maka $a^{i-j} = a^i a^{-j} = e$. Tetapi karena a mempunyai order takhingga, maka $a^n = e$ bila dan hanya bila $n = 0$. Sehingga didapat $i - j = 0$ atau $i = j$.

(2) Misalkan $|a| = n$. Bila n membagi $i-j$, maka $i-j = nk$ untuk beberapa $k \in \mathbb{Z}$ atau $i = nk+j$ untuk beberapa $k \in \mathbb{Z}$. Didapat

$$a^i = a^{nk+j} = a^{nk}a^j = (a^n)^k a^j = e^k a^j = ea^j = a^j.$$

Sebaliknya, bila $a^i = a^j$ atau ekivalen $a^{i-j} = e$. Dengan menggunakan algoritma pembagian bilangan bulat didapat $i - j = qn + r$, dimana $0 \leq r < n$. Jadi

$$e = a^{i-j} = a^{qn+r} = a^{qn}a^r = (a^n)^q a^r = e^q a^r = ea^r = a^r.$$

Karena $0 \leq r < n$ dan n adalah order dari a, maka n adalah bilangan positip terkecil yang memenuhi $a^n = e$. Jadi haruslah $r = 0$. Dengan demikian didapat $i - j = qn$ atau n membagi $i - j$. ✓

Akibat 2.3.1 Misal G adalah suatu grup dan $a \in G$ dengan $|a| = n$. Maka untuk sebarang $k \in \mathbb{Z}$, $a^k = e$ bila dan hanya bila n membagi k.

Bukti Gunakan Teorema 2.3.1 bagian (2) didapat n membagi k. ✓

Akibat 2.3.2 Misalkan G adalah suatu grup dan $a \in G$ dengan $|a| = n$. Maka $\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$.

Bukti Misalkan $|a| = n$ dan

$$\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}.$$

Dengan menggunakan algoritma pembagian bilangan bulat $m = qn + r$ untuk beberapa $q \in \mathbb{Z}$ dan $0 \leq r < n$. Sehingga didapat

$$\begin{aligned}
\langle a \rangle &= \{a^m \mid m \in \mathbb{Z}\} \\
&= \{a^{qn+r} \mid 0 \leq r < n\} \\
&= \{(a^{qn})a^r \mid 0 \leq r < n\} \\
&= \{(a^n)^q a^r \mid 0 \leq r < n\} \\
&= \{e^q a^r = ea^r \mid 0 \leq r < n\} \\
&= \{a^r \mid 0 \leq r < n\} \\
&= \{e, a, a^2, \ldots, a^{n-1}\}.
\end{aligned}$$

✓

Akibat 2.3.3 Misalkan G adalah suatu grup dan $a \in G$ mempunyai order berhingga. Maka $|\langle a \rangle| = |a|$.

Bukti Misalkan $|a| = n$. Dengan menggunakan Akibat 2.3.2 didapat

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}$$

Jelas bahwa $|\langle a \rangle| = n$. Jadi $|\langle a \rangle| = |a|$. ✓

Contoh 2.3.10 Diberikan G grup siklik dengan $|G| =$. Jadi

$$G = \langle a \rangle = \{e, a, a^2, a^3, a^4, a^5\}.$$

Didapat

$$(a^4)^2 = a^8 = a^{6+2} = a^6a^2 = ea^2 = a^2 \neq e,$$

sedangkan

$$(a^4)^3 = a^{12} = a^{6+6} = a^6a^6 = e \cdot e = e.$$

Jadi $|a^4| = 3$. ●

Teorema berikut sangat penting menjadikan mudah untuk mendapatkan order elemen dari suatu grup siklik.

Teorema 2.3.2 Misalkan $G = \langle a \rangle$ dan $|G| = |a| = n$. Maka untuk sebarang elemen $a^k \in G$ didapat $|a^k| = n/\text{fpb}(n, k)$.

Bukti Dari Akibat 2.3.1 didapat $(a^k)^m = a^{km} = e$ bila dan hanya bila n membagi km atau km kelipatan dari n juga kelipatan dari k. Jadi bila order $|a^k|$ adalah bilangan bulat positip terkecil m sedemikian hingga km kelipatan dari n dan k atau ekivalen km adalah bilangan bulat positip terkecil yang merupakan kelipatan dari n dan k, yaitu $km = \text{kpk}(n, k)$. Dengan menggunakan Proposisi 1.3.3 bagian (3) didapat $\not{k}m = \not{k}n/\text{fpb}(n, k)$ atau $m = n/\text{fpb}(n, k)$. Jadi $|a^k| = n/\text{fpb}(n, k)$. ✓

Contoh 2.3.11 Dalam suatu grup siklik $G = \langle a \rangle$ dengan $|G| = 210$, maka

$$|a^{80}| = 210/\text{fpb}(210, 80) = 210/10 = 21.$$ ●

Contoh 2.3.12 Dalam $\mathbb{Z}_{105}$, maka $|[84]_{105}| = 105/\text{fpb}(105, 84) = 105/21 = 5$. ●

Teori yang baru dibahas tidak hanya untuk menyederhanakan penghitungan order sebarang elemen dari suatu grup siklik sebagaimana pembahasan contoh sebelumnya, tetapi juga untuk mendapatkan generator dari grup sebagaimana diberikan dalam contoh berikut.

Contoh 2.3.13 Diberikan grup $\mathbb{Z}_{12}$. Untuk mendapatkan order semua elemen dari $\mathbb{Z}_{12}$, atau mendapatkan semua $[s]_{12} \in \mathbb{Z}_{12}$ yang memenuhi $|[s]_{12}| = 12$. Gunakan Teorema 2.3.2, didapat

$$|[s]_{12}| = 12/\text{fpb}(12, s).$$

Jadi $|[s]_{12}| = 12$ bila dan hanya bila $12/\text{fpb}(12, s) = 12$ atau $\text{fpb}(12, s) = 12/12 = 1$. Dengan demikian elemen-elemen $[s]_{12} \in \mathbb{Z}_{12}$ adalah generator dari $\mathbb{Z}_{12}$ bila $\text{fpb}(12, s) = 1$. Jadi elemen-elemen tersebut adalah: $[1]_{12}, [5]_{12}, [7]_{12}$ dan $[11]_{12}$. ●

Akibat 2.3.4 Diberikan grup siklik G dengan generator a, $G = \langle a \rangle$ dengan $|G| = |a| = n$. Maka a^s adalah generator dari G bila dan hanya bila $\text{fpb}(n, s) = 1$.

Bukti Elemen a^s adalah generator dari G bila dan hanya bila $G = \langle a^s \rangle$. Gunakan Akibat 2.3.3, didapat $|\langle a^s \rangle| = |a^s|$, dan dari Teorema 2.3.2 didapat $|a^s| = n/\text{fpb}(n, s)$. Tetapi $|a^s| = |G| = n$. Jadi a^s adalah generator dari grup G bila dan hanya bila $n/\text{fpb}(n, s) = n$ atau ekivalen dengan $\text{fpb}(n, s) = 1$. ✓

Akibat 2.3.5 Misalkan G adalah suatu grup siklik dengan order n. Maka banyaknya elemen generator dari G adalah $\phi(n)$ dimana ϕ adalah fungsi Euler.

Bukti Dari kesimpulan yang baru saja dibahas, banyaknya elemen generator dari G adalah bilangan s dengan $1 \leq s < n$ yang memenuhi $\text{fpb}(n, s) = 1$. Hal ini sesuai dengan definisi $\phi(n)$. ✓

Contoh berikut mengilustrasikan bahwa suatu sifat yang dipunyai oleh grup siklik, membuat sifat ini secara khusus mudah dipahami.

Contoh 2.3.14 Misalkan akan dicari semua subgrup dari grup $\mathbb{Z}_{15}$. Untuk memulainya, jelas subgrup trivial $\langle 0 \rangle$ adalah subgrup dari $\mathbb{Z}_{15}$. Misalkan H adalah sebarang subgrup tak-trivial dari $\mathbb{Z}_{15}$. Dari Akibat 2.3.4 didapat semua generator dari $\mathbb{Z}_{15}$ adalah

$$[1]_{15}, [2]_{15}, [4]_{15}, [7]_{15}, [11]_{15}, [13]_{15}, [14]_{15}.$$

Didapat subgrup tak-sejati:

$$\mathbb{Z}_{15} = \langle [1]_{15} \rangle = \langle [2]_{15} \rangle = \langle [4]_{15} \rangle = \langle [7]_{15} \rangle = \langle [8]_{15} \rangle = \langle [11]_{15} \rangle = \langle [13]_{15} \rangle = \langle [14]_{15} \rangle .$$

Selanjutnya, misalkan H adalah subgrup sejati tak-trivial dari G. Misalkan $[3]_{15} \in H$, maka untuk sebarang $[y]_{15} \in H$ dengan menggunakan algoritma pembagian bilangan bulat didapat $y = 3q + r$ untuk beberapa r dengan $0 \leq r < 3$. Tetapi $[3]_{15}, [y]_{15} \in \mathbb{Z}_{15}$, maka $[r]_{15} = [y]_{15} - q[3]_{15} \in H$. Tetapi H adalah himpunan bagian sejati dari $\mathbb{Z}_{15}$, maka $[1]_{15}, [2]_{15} \notin H$. Jadi haruslah $r = 0$. Dengan demikian semua elemen dari H adalah kelipatan dari $[3]_{15}$. Jadi $H = \langle [3]_{15} \rangle = \{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\} = 3\mathbb{Z}_{15}$. Karena $3[6]_{15} = 2[9]_{15} = 4[12]_{15} = [3]_{15}$, maka sebarang subgrup sejati tak-trivial dari $\mathbb{Z}_{15}$ yang memuat $[6]_{15}, [9]_{15}$ dan $[12]_{15}$ juga pasti memuat $[3]_{15}$ dan sama dengan

$$3\mathbb{Z}_{15} = \langle [3]_{15} \rangle = \langle [6]_{15} \rangle = \langle [9]_{15} \rangle = \langle [12]_{15} \rangle .$$

Berikutnya, misalkan H subgrup sejati tak-trivial dan $[5]_{15} \in H$. Dengan argumentasi yang sama didapat $H = \langle [5]_{15} \rangle = \{[0]_{15}, [5]_{15}, [10]_{15}\} = 5\mathbb{Z}_{15}$, dan sebarang subgrup sejati yang memuat $[10]_{10}$ juga sama dengan $5\mathbb{Z}_{15} = \langle [5]_{15} \rangle = \langle [10]_{15} \rangle$. Dengan demikian semua subgrup yang mungkin dari $\mathbb{Z}_{15}$ adalah

$$0\mathbb{Z}_{15} = \{[0]_{15}\}, \quad 1\mathbb{Z}_{15} = \mathbb{Z}_{15}, \quad 3\mathbb{Z}_{15}, \quad \text{dan} \quad 5\mathbb{Z}_{15}. \qquad ●$$

Teorema 2.3.3 Setiap subgrup dari suatu grup siklik adalah siklik.

Bukti Misalkan $G = \langle a \rangle$ dan H adalah sebarang subgrup dari G. Bila H adalah subgrup

trivial, yaitu H={e}, maka $H = \langle e \rangle$ adalah siklik. Asumsikan H subgrup tak-trivial. Jadi, dapat dipilih $b \in H$ dengan $b \neq e$. Karena juga $b \in G = \langle a \rangle$, maka $b = a^s$ untuk beberapa $s \in \mathbb{Z}$ dan karena $b \neq e$, maka $s \neq 0$. Juga karena $b \in H$, maka $b^{-1} = (a^s)^{-1} = a^{-s} \in H$. Karena satu diantara s atau $-s$ adalah positip, maka H memuat beberapa pangkat positip dari a. Dengan menggunakan prinsip keterurutan secara baik bilangan bulat positip, maka dapat diplih bilangan bulat positip terkecil m yang memenuhi $a^m \in H$. Selanjutnya, diberikan sebarang $x \in H$, maka $y = a^n$ untuk beberap bilangan bulat n (sebab juga $y \in G$). Gunakan algoritma pembagian bilangan bulat pada m dan n didapat $n = qm + r$ untuk beberapa bilangan bulat q dan $0 \leq r < m$. Didapat

$$y = a^n = a^{qm+r} = (a^m)^q a^r.$$

Hal ini berakibat

$$a^r = y(a^m)^{-q} \in H \text{ (sebab } H < G, y \in H \text{ dan } a^m \in H).$$

Tetapi m adalah bilangan bulat positip terkecil yang memenuhi $a^m \in H$, dengan dan juga $a^r \in H$ dengan $0 \leq r < m$. Jadi haruslah $r = 0$. Dengan demikian didapat

$$y = a^n = a^{qm+r} = a^{qm} = (a^m)^q, \text{ dengan } q \in \mathbb{Z}.$$

Terlihat bahwa sebarang $y \in H$ merupakan suatu pangkat dari a^m, dengan demikian $H = \{(a^m)^k \mid k \in \mathbb{Z}\} = \langle a^m \rangle$. Jadi H adalah subgrup siklik. ✓

Akibat 2.3.6 Semua subgrup dari $\mathbb{Z}$ adalah $n\mathbb{Z} = \langle n \rangle$ untuk semua $n \geq 0$.

Bukti $\mathbb{Z} = \langle 1 \rangle$ adalah siklik. Jadi menurut Teorema 2.3.3 sebarang subgrup $H \leq \mathbb{Z}$ juga siklik. Oleh karena itu, $H = \langle m \rangle$ untuk beberapa bilangan bulat m. Karena $\langle -m \rangle = \langle m \rangle$ dan salah satu dari m atau $-m$ adalah taknegatip, maka $H = \langle n \rangle$ untuk $n \geq 0$. ✓

Contoh 2.3.15 Karena $\mathbb{Z}_{12}$ adalah grup siklik, maka semua subgrup dari $\mathbb{Z}_{12}$ adalah siklik. Jadi bila subgrup $H = \langle [s]_{12} \rangle$, maka $|H| = |[s]_{12}| = 12/\text{fpb}(12, s)$ adalah pembagi dari 12. Semua pembagi 12 adalah $1, 2, 3, 4, 6$ dan 12 sendiri. Subgrup H dengan $|H| = 1$ adalah $\{[0]_{12}\} = \langle [0]_{12} \rangle$. Berikutnya bila $2 = |H| = |[s]_{12}| = 12/\text{fpb}(12, s)$, maka $s = 6$. Didapat $H = \langle [6]_{12} \rangle = \{[0]_{12}, [6]_{12}\}$. Sedangkan subgrup yang lain adalah

$$\langle [4]_{12} \rangle = \{[0]_{12}, [4]_{12}, [8]_{12}\}, \text{ order } |\langle [4]_{12} \rangle| = 3,$$

$$\langle [3]_{12} \rangle = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}, \text{ order } |\langle [3]_{12} \rangle| = 4,$$

$$\langle [2]_{12} \rangle = \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}, \text{ order } |\langle [2]_{12} \rangle| = 6$$

dan $\langle [1]_{12} \rangle = \mathbb{Z}_{12}$ dengan order $|\langle [1]_{12} \rangle| = |\mathbb{Z}_{12}| = 12$. ●

Teorema 2.3.4 Misalkan $G = \langle a \rangle$ berorder n. Maka

(1) order $|H|$ sebarang subgrup H dari grup G adalah pembagi dari $n = |G|$.

(2) Untuk semua bilangan bulat positip d yang membagi n ada tunggal subgrup yang berorder d yaitu $H = \left\langle a^{n/d} \right\rangle$.

Bukti

(1) Misalkan H adalah suatu subgrup dari $G = \langle a \rangle$. Dengan menggunakan Teorema 2.3.3, didapat $H = \langle a^m \rangle$ untuk beberapa $m \geq 0$, dengan menggunakan Teorema 2.3.2 didapat $|H| = |a^m| = n/\text{fpb}(n, m)$. Terlihat bahwa order $|H|$ membagi n.

(2) Karena $e \in H$ untuk sebarang subgrup H dari grup G, maka subgrup dari G yang berorder 1 hanya $\{e\} = \langle e \rangle$. Misalkan d pembagi dari n dan $d > 1$. Gunakan Teorema 2.3.2 didapat $|a^{n/d}| = n/\text{fpb}(n, n/d) = n/(n/d) = d$. Jadi $\left\langle a^{n/d} \right\rangle$ adalah subgrup berorder d. Tinggal menunjukkan ketunggalan, misalkan H adalah subgrup dari G yang berorder d dan karena G siklik yaitu $G = \langle a \rangle$, maka menurut Teorema 2.3.3 didapat H adalah subgrup siklik. Jadi $H = \langle a^m \rangle$, dimana m adalah bilangan bulat positip terkecil yang memenuhi $a^m \in H$. Selanjutnya dari Teorema 1.3.6 bagian (2) ada bilangan bulat u dan v yang memenuhi $\text{fpb}(n, m) = un + vm$. Sehingga didapat

$$a^{\text{fpb}(n,m)} = a^{un+vm} = a^{un}a^{vm} = (a^n)^u(a^m)^v = e^u(a^m)^v = e(a^m)^v = (a^m)^v \in H.$$

Karena $1 \leq \text{fpb}(n, m) \leq m$ dan m adalah bilangan bulat positip terkecil yang memenuhi $a^m \in H$, maka haruslah $\text{fpb}(n, m) = m$. Maka dengan menggunakan Teorema 2.3.2 didapat

$$d = |H| = |a^m| = n/\text{fpb}(n, m) = n/m.$$

Jadi $d = n/m$ atau $m = n/d$. dengan demikian didapat $H = \langle a^m \rangle = \left\langle a^{n/d} \right\rangle$ sebagaimana diharapkan. ✓

Contoh 2.3.16 Dibahas lagi menentukan semua subgrup dari grup $\mathbb{Z}_{12}$ sebagaimana telah dibahas dalam Contoh 2.3.15. Tetapi sekarang menggunakan Teorema 2.3.4. Grup siklik $\mathbb{Z}_{12} = \langle [1]_{12} \rangle$, dengan demikian $a = [1]_{12}, n = 12$ dan semua pembagi dari $n = 12$ adalah $d = 1, 2, 3, 4, 6, 12$. Untuk $d = 1$ didapat

$$H = \langle (12/1)[1]_{12} \rangle = \langle 12[1]_{12} \rangle = \langle [12]_{12} \rangle = \{[0]_{12}\}.$$

Untuk $d = 2$, didapat subgrup

$$H = \langle (12/2)[1]_{12} \rangle = \langle 6[1]_{12} \rangle = \langle [6]_{12} \rangle = \{[0]_{12}, [6]_{12}\}.$$

Untuk $d = 3$, didapat subgrup

$$H = \langle (12/3)[1]_{12} \rangle = \langle 4[1]_{12} \rangle = \langle [4]_{12} \rangle = \{[0]_{12}, [4]_{12}, [8]_{12}\}.$$

Untuk $d = 4$, didapat subgrup

$$H = \langle (12/4)[1]_{12} \rangle = \langle 3[1]_{12} \rangle = \langle [3]_{12} \rangle = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}.$$

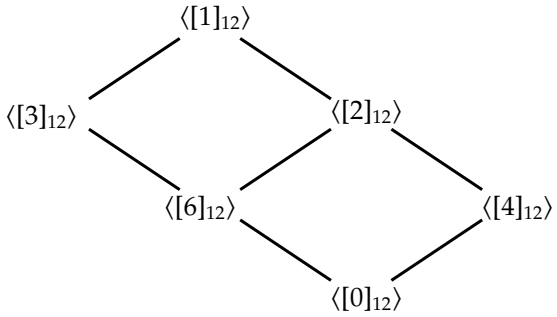
Untuk $d = 6$, didapat subgrup

$$H = \langle (12/6)[1]_{12} \rangle = \langle 2[1]_{12} \rangle = \langle [2]_{12} \rangle = \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}.$$

Untuk $d = 12$, didapat subgrup

$$H = \langle (12/12)[1]_{12} \rangle = \langle 1[1]_{12} \rangle = \langle [1]_{12} \rangle = \mathbb{Z}_{12}.$$

Gambar 2.5 adalah penampilan dari semua subgrup dari $\mathbb{Z}_{12}$ dalam bentuk diagram yang dinamakan **lattice subgrup**. Gambar tersebut menunjukkan bagaimana subgrup-subgrup mempunyai keterkaitan satu dengan yang lainnya. Garis dalam diagram menyatakan inklusi. Jadi, dalam diagram menunjukkan bahwa $\langle [3]_{12} \rangle$ memuat $\langle [6]_{12} \rangle$ dan $\langle [6]_{12} \rangle$ memuat $\langle [0]_{12} \rangle$. Diagram menunjukkan bahwa irisan dari $\langle [3]_{12} \rangle$ dan $\langle [2]_{12} \rangle$ adalah $\langle [6]_{12} \rangle$ dan irisan dari $\langle [6]_{12} \rangle$ dan $\langle [4]_{12} \rangle$ adalah $\langle [0]_{12} \rangle$. ●



Gambar 2.5: Lattice Subgrup

Latihan

Latihan 2.3.1 Dapatkan order elemen dari grup berikut:

(1) $[6]_{10} \in \mathbb{Z}_{10}$ (2) $[6]_{15} \in \mathbb{Z}_{15}$ (3) $[10]_{42} \in \mathbb{Z}_{42}$
(4) $[77]_{210} \in \mathbb{Z}_{210}$ (5) $[40]_{210} \in \mathbb{Z}_{210}$ (6) $[70]_{210} \in \mathbb{Z}_{210}$.

Latihan 2.3.2 Misalkan $G = \langle a \rangle$ dan $|G| = 21$. Hitung order dari elemen-elemen:

$$a^2, a^6, a^8, a^9, a^{14}, a^{15} \quad \text{dan} \quad a^{18}.$$

Latihan 2.3.3 Misalkan G adalah suatu grup dan $a \in G$ dengan $|a| = 6$.
(a) Tulis semua elemen dari $\langle a \rangle$.
(b) Dapatkan dalam $\langle a \rangle$ elemen-elemen a^{32}, a^{47}, a^{70}.

Latihan 2.3.4 Dapatkan semua generator dari $\mathbb{Z}_{10}, \mathbb{Z}_{12}$ dan $\mathbb{Z}_{15}$.

Latihan 2.3.5 Diberikan grup $G = \langle a \rangle$ dan $|G| = 30$. Dapatkan semua generator dari G.

Latihan 2.3.6 Gambar diagram lattice subgrup untuk $\mathbb{Z}_{18}$.

Latihan 2.3.7 Dapatkan semua elemen $a \in \mathbb{Z}_{15}$ dimana $|a| = 5$.

Latihan 2.3.8 Diberikan $G = \langle a \rangle$ dengan $|G| = 20$. Dapatkan semua elemen $b \in G$ dimana $|b| = 10$.

Latihan 2.3.9 Dapatkan semua subgrup siklik dari S_3. Apakah S_3 mempunyai suatu subgrup sejati tak-siklik? Jelaskan jawaban saudara.

Latihan 2.3.10 Dapatkan semua subgrup siklik dari D_4. Apakah D_3 mempunyai suatu subgrup sejati tak-siklik? Jelaskan jawaban saudara.

Latihan 2.3.11 Apakah benar bahwa bila setiap subgrup sejati dari suatu grup G adalah siklik, maka G harus juga siklik? Jawab dengan suatu bukti bila benar atau berikan contoh penyangkal bila salah.

Latihan 2.3.12 Berikan contoh-contoh subgrup siklik berhingga dari $\mathbb{C}^*$.

Latihan 2.3.13 Tunjukkan bahwa setiap grup siklik adalah komutatif.

Latihan 2.3.14 Berikan suatu contoh grup yang memenuhi sifat berikut:

(a) suatu grup siklik takberhingga.

(b) suatu grup komutatif takberhingga yang tak-siklik.

(c) suatu grup siklik berhingga dengan tepat mempunyai enam generator.

(d) suatu grup komutatif berhingga yang tak-siklik.

Latihan 2.3.15 Misalkan H dan K adalah subgrup siklik dari suatu grup komutatif G dengan $|H| = 10$ dan $|K| = 14$. Tunjukkan bahwa grup G memuat suatu subgrup siklik yang berorder 70.

Latihan 2.3.16 Diberikan grup G yang tak mempunyai subgrup sejati tak-trivial.
(a) Tunjukkan bahwa G harus siklik.
(b) Apa yang bisa dikatakan mengenai order dari G?

Latihan 2.3.17 Diberikan bilangan bulat m dan n; dan himpunan

$$m\mathbb{Z} + n\mathbb{Z} \stackrel{\text{def}}{=} \{a + b \,|\, a \in m\mathbb{Z},\ b \in n\mathbb{Z}\}.$$

(a) Tunjukkan bahwa $m\mathbb{Z} + n\mathbb{Z}$ adalah suatu subgrup dari $\mathbb{Z}$.

(b) Dapatkan suatu generator untuk subgrup $12\mathbb{Z} + 21\mathbb{Z}$.

(c) Dapatkan suatu generator untuk subgrup $m\mathbb{Z} + n\mathbb{Z}$.

Latihan 2.3.18 Dapatkan suatu generator subgrup $6\mathbb{Z} \cap 15\mathbb{Z}$ dari grup $\mathbb{Z}$.

Latihan 2.3.19 Diberikan bilangan bulat m dan n. Dapatkan suatu generator subgrup $m\mathbb{Z} \cap n\mathbb{Z}$ dari grup $\mathbb{Z}$.

Latihan 2.3.20 Tentukan grup yang berikut siklik atau tidak:
(a) $\mathbb{U}(10)$ (b) $\mathbb{U}(12)$ (c) $\mathbb{U}(20)$ (d) $\mathbb{U}(24)$.

Latihan 2.3.21 Diberikan grup G dan $a, b \in G$ dengan $|a| = 14$ dan $|b| = 15$. Uraikan subgrup $\langle a \rangle \cap \langle b \rangle$. Jelaskan jawaban saudara.

Latihan 2.3.22 Diberikan grup $G = \langle a \rangle$ dan $|G| = 20$. Himpunan H dan K adalah dua subgrup sejati tak-trivial yang berbeda dari grup G sedemikian hingga $H < K$ dan $a^4 \notin K$. Uraikan H dan K.

Latihan 2.3.23 Diberikan grup $G = \langle a \rangle$ dan $|G| = n$, d suatu pembagi dari n. Tunjukkan bahwa banyaknya elemen-elemen di G yang berorder d adalah $\phi(d)$ dimana ϕ adalah suatu fungsi-ϕ Euler.

2.4 Permutasi

Pembahasan berikut ini tentang contoh yang paling penting dari grup berhingga, yaitu grup permutasi. Alasan grup permutasi menjadi pokok penting adalah bahwa, seperti yang akan terlihat pada bab mendatang , setiap grup berhingga dapat dilihat sebagai subgrup dari grup permutasi. Ini berarti bahwa kajian grup berhingga dapat dibahas pada sebagian kajian grup permuatsi. Ketika dikonstruksi suatu grup berhingga dengan sifat tertentu, dapat ditemukan grup permutasi yang menghasilkan subgrup dengan sifat-sifat yang sama. Bahasan dimulai dengan memberikan beberapa contoh permutasi dan fungsi yang bukan permutasi.

Contoh 2.4.1 Diberikan fungsi $f : \mathbb{Z} \to \mathbb{Z}$ didefinisikan oleh $f(n) = n + 1$, $\forall n \in \mathbb{Z}$ adalah satu-satu, sebab bila $f(n_1) = f(n_2)$, maka $n_1 + 1 = n_2 + 1$ dan $n_1 = n_2$. Fungsi f juga pada, sebab untuk sebarang $m \in \mathbb{Z}$ (kodomain), maka dapat diplih $m - 1 \in \mathbb{Z}$ (domain) sehingga $f(m - 1) = (m - 1) + 1 = m$. 🔴

Contoh 2.4.2 Diberikan fungsi $g : \mathbb{Z} \to \mathbb{Z}$ didefinisikan oleh $g(n) = 2n$, $\forall n \in \mathbb{Z}$ adalah satu-satu, sebab bila $g(n_1) = g(n_2)$, maka $2n_1 = 2n_2$ dan $n_1 = n - 2$. Fungsi g tidak pada, sebab $g(\mathbb{Z}) = 2\mathbb{Z} \neq \mathbb{Z}$. 🔴

Contoh 2.4.3 Fungsi $j : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ didefinisikan oleh

$$j(1) = 3, \quad j(2) = 4, \quad j(3) = 1, \quad j(4) = 2.$$

Jelas fungsi j satu-satu dan pada. 🔴

Contoh 2.4.4 Fungsi $k : \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ didefinisikan oleh

$$k(1) = 2, \quad k(2) = 2, \quad k(3) = 4, \quad j(4) = 3.$$

Jelas fungsi k tidak satu-satu dan tidak pada. 🔴

Definisi 2.4.1 Suatu fungsi $\phi : A \to A$ dinamakan **permutasi dari himpunan** A bila ϕ fungsi satu-satu dan pada atau bijektif. ✓

Dari contoh-contoh yang dibahas, maka Contoh 2.4.1 dan 2.4.3 adalah permutasi. Sedangkan Contoh 2.4.2 dan 2.4.4 bukan permutasi.

Contoh 2.4.5 Diberikan himpunan $A = \{1, 2, 3, 4, 5, 6\}$ dan dua permutasi ϕ dan τ yang disajikan oleh

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 1 & 2 & 3 & 5 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 5 & 4 & 6 & 1 \end{pmatrix}.$$

Penyajian ϕ dan τ mempunyai arti :

$$\phi(1) = 4,\ \phi(2) = 6,\ \phi(3) = 1,\ \phi(4) = 2,\ \phi(5) = 3,\ \phi(6) = 5$$

dan

$$\tau(1) = 2,\ \tau(2) = 3,\ \tau(3) = 5,\ \tau(4) = 4,\ \tau(5) = 6,\ \tau(6) = 1.$$

Karena ϕ dan τ adalah fungsi, maka dapat dikonstruksi komposisi fungsi $\phi \circ \tau : A \to A$ sebagai berikut

$$\phi \circ \tau(1) = \phi(\tau(1)) = \phi(2) = 6,\ \phi \circ \tau(2) = \phi(\tau(2)) = \phi(3) = 1,\ \phi \circ \tau(3) = \phi(\tau(3)) = \phi(5) = 3,$$

didapat

$$\phi \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 3 & 2 & 5 & 4 \end{pmatrix}.$$

Dengan cara yang sama didapat

$$\tau \circ \phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 5 & 6 \end{pmatrix}.$$

Catatan bahwa hasil komposisi fungsi juga fungsi bijektif oleh karenanya juga permutasi. Pada umumnya komposisi dari permutasi tidak komutatif, dalam contoh terlihat bahwa $\phi \circ \tau \neq \tau \circ \phi$.

Definisi 2.4.2 Diberikan dua permutasi ϕ dan τ pada suatu himpunan A komposisi $\phi \circ \tau$ dinamakan **produk permutasi** dari ϕ dan τ dan operasi komposisi disebut **perkalian permutasi**.

Perkalian permutasi adalah operasi yang akan digunakan untuk membuat himpunan semua permutasi pada suatu himpunan A membentuk grup. Perlu diingatkan lagi, dimana grup permutasi ini telah dikenal.

Contoh 2.4.6 Misalkan dicari semua permutasi pada himpunan $A = \{1, 2, 3\}$. Pertama, perlu dicatat akan ada tepat enam permutasi. Bila dimulai dari 1 ada tiga kemungkinan pengaitan $1 \to 1, 1 \to 2$ atau $1 \to 3$, selanjutnya untuk 2 tinggal 2 pilihan pengaitan sebab fungsinya pada dan untuk 3 tinggal satu pilihan pengaitan. Dengan demikian ada sebanyak $3 \cdot 2 \cdot 1 = 6$ permutasi. Enam permutasi pada A adalah:

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \qquad \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad \rho^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \rho\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \qquad \rho^2\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Permutasi yang terbentuk sudah dikenal sebagai grup simetri dari segitiga sama sisi S_3 yang sudah dibahas dalam Contoh 2.1.5.

Teorema 2.4.1 Diberikan $A = \{1, 2, 3, \ldots, n\}$ dan S_n adalah himpunan semua permutasi pada A. Maka S_n adalah suatu grup terhadap perkalian permutasi.

Bukti (Tertutup) Dari Teorema 1.1.2 menyatakan bahwa komposisi fungsi satu-satu dan pada menghasilkan fungsi satu-satu dan pada. Karena permutasi adalah fungsi satu-satu dan pada serta perkalian permutasi bermakna komposisi fungsi, maka berdasarkan teorema yang telah disebutkan sifat tertutup dipenuhi. (Assosiatif) Sifat ini juga dipenuhi berdasarkan Teorema 1.1.2. (Identitas) Permutasi yang didefinisikan oleh $\rho_0(i) = i$ untuk semua $i \in A$ adalah elemen identitas terhadap perkalian permutasi. (Invers) Untuk sebarang $\phi \in S_n$, ϕ adalah satu-satu dan pada, maka berdasarkan Teorema 1.1.4 fungsi diberikan oleh $\phi^{-1}(i) = j$ dimana $\phi(j) = i$ adalah terdefinisi dengan baik dan merupakan invers dari ϕ terhadap operasi perkalian permutasi.

Karena elemen-elemen dari sebarang himpunan dengan n elemen dapat dilabel oleh $1, 2, 3, \ldots, n$,berlaku juga Teorema 2.4.1 berlaku juga untuk seberang himpunan berhingga A.

Definisi 2.4.3 Grup dari himpunan S_n terhadap operasi perkalian permutasi dinamakan **grup simetri** berderajad n.

Proposisi 2.4.1 Grup simetri S_n mempunyai order $|S_n| = n!$.

Bukti Misalkan $\phi \in S_n$, ϕ dapat ditulis sebagai

$$\phi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ \phi(1) & \phi(2) & \phi(3) & \ldots & \phi(n-1) & \phi(n) \end{pmatrix}.$$

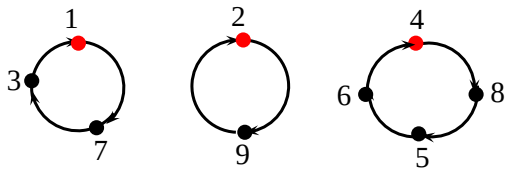
Ada sebanyak n pilihan untuk menetapkan niali $\phi(1)$. Sekali telah dipilih suatu nilai untuk $\phi(1)$, ada sebanyak $n-1$ pilihan untuk menetapkan nilai $\phi(2)$. Sekali nilai $\phi(1)$ dan $\phi(2)$ dipilih, ada sebanyak $n-2$ pilihan untuk menetapkan nilai $\phi(3)$, dan seterusnya. Dengan demikian ada sebanyak

$$n \cdot (n-1) \cdot (n-2) \cdots 2 \cdot 1 = n!.$$

Contoh 2.4.7 Diberikan himpunan $A = \{1, 2, 3, \ldots, 9\}$ dan permutasi

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 9 & 1 & 8 & 6 & 4 & 3 & 5 & 2 \end{pmatrix} \in S_9.$$

Selanjutnya dibahas aplikasi dari ϕ secara berulang dikenakan pada berbagai elemen dari himpunan A:
$1 \to \phi(1) = 7 \to \phi^2(1) = \phi(7) = 3 \to \phi^3(1) = \phi(3) = 1$. Permutasi ϕ dikenakan pada 1 sebanyak 3 kali, hasilnya kembali lagi ke 1.
$2 \to \phi(2) = 9 \to \phi^2(2) = \phi(9) = 2$. Permutasi ϕ dikenakan pada 2 sebanyak 2 kali, hasilnya kembali lagi ke 2.
$4 \to \phi(4) = 8 \to \phi^2(4) = \phi(8) = 5 \to \phi^3(4) = \phi(5) = 6 \to \phi^4(4) = \phi(6) = 4$. Permutasi ϕ dikenakan pada 4 sebanyak 4 kali, hasilnya kembali lagi ke 4.



Gambar 2.6: Pengulangan ϕ dikenakan pada $i \in A$

Pertama pemutasi ϕ berturut-turut memetakan : 1 ke 7, 7 ke 3, 3 ke 1 dan tinggalkan elemen yang lain tetap didapat (1 7 3). Selanjutnya dengan cara yang sama didapat (2 9) dan (4 8 5 6). Tiga permutasi yang didapat diberikan oleh Gambar 2.6. Permutasi asal ϕ adalah produk $\phi = (1\ 7\ 3)(2\ 9)(4\ 8\ 5\ 6)$. Akibatnya, permutasi ϕ mempartisi himpunan $A = \{1, 2, 3, 4, \ldots, 9\}$ menjadi tiga himpunan bagian yang saling asing, dengan demikian menentukan suatu relasi ekivalen pada himpunan A. Dua elemen $i, j \in A$ ekivalen , ditulis $i \sim j$ bila $\phi^n(i) = j$ untuk

beberapa $n \in \mathbb{Z}$. Jadi $1 \sim 3$ sebab $\phi^2(1) = 3$ dan $4 \sim 6$ sebab $\phi^3(4) = 6$. Klas ekivalennya adalah

$$\{1,7,3\},\ \{2,9\} \text{ dan } \{4,8,5,6\}.$$

Teorema 2.4.2 Diberikan permutasi $\phi \in S_n$, maka ϕ menentukan suatu relasi klas ekivalen pada himpunan $A = \{1,2,3,\ldots,n\}$ yang didefinisikan oleh kondisi untuk $r,s \in A$, $r \sim s$ bila dan hanya bila $s = \phi^i(r)$ untuk beberapa $i \in \mathbb{Z}$.

Bukti
(Refkesif) $r \sim r$ sebab $r = \phi^0(r)$.
(Simetri) Bila $r \sim s$, didapat $s = \phi^i(r)$ untuk beberapa $i \in \mathbb{Z}$. Dengan demikian $r = \phi^{-i}(s)$, dimana $-i \in \mathbb{Z}$. Jadi $s \sim r$.
(Transitif) Bila $r \sim s$ dan $s \sim t$, maka $s = \phi^i(r)$ dan $t = \phi^j(s)$ untuk beberapa $i, j \in \mathbb{Z}$. Dengan demikian, $t = \phi^j(s) = \phi^j(\phi^i(r)) = \phi^{j+i}(r)$ dimana $j + i \in \mathbb{Z}$. Jadi $r \sim t$.

Definisi 2.4.4 Diberikan $\phi \in S_n$, klas ekivalen dalam $A = \{1,2,3,\ldots\}$ yang ditentukan oleh ϕ dinamakan **orbit** dari ϕ.

Definisi 2.4.5 Suatu permutasi $\sigma \in S_n$ dinamakan **sikel** bila permutasi ini setidaknya adalah satu orbit yang memuat lebih dari satu elemen. **Panjang** dari sikel adalah banyaknya elemen yang paling besar pada orbit-orbitnya. Suatu sikel dengan panjang k juga dinamakan **sikel-k** dan dapat ditulis $(a_1\ a_2 \ldots a_k)$, dimana untuk semua i, a_i adalah elemen dari orbit terbesar dan

$$a_2 = \sigma(a_1),\ a_3 = \sigma^2(a_1) = \sigma(a_2), \ldots, a_k = \sigma^{k-1}(a_1) = \sigma(a_{k-1}), a_1 = \sigma^k(a_1) = \sigma(a_k).$$

Dua sikel **saling asing** bila himpunan orbitnya saling asing.

Contoh 2.4.8 Semua sikel-3 dalam S_4 adalah

(1 2 3)	(1 3 2)	(1 2 4)	(1 4 2)
(1 3 4)	(1 4 3)	(2 3 4)	(2 4 3).

Catatan, sikel yang sama dapat ditulis lebih dari satu cara, misalnya (1 2 3) = (2 3 1) = (3 1 2).

Teorema 2.4.3 Setiap permutasi $\phi \in S_n$ dapat ditulis sebagai produk dari sikel-sikel yang saling asing.

Bukti Misalkan orbit dari ϕ adalah $O_1, O_2, \ldots, O_s$. Untuk masing-masing orbit O_i didefinisikan sikel yang sesuai σ_i sebagai berikut:

$$\sigma_i(a) = \begin{cases} \phi(a), & \text{bila } a \in O_i \\ a, & \text{bila } a \notin O_i. \end{cases}$$

Sikel-sikel adalah saling asing sebab orbit O_i adalah klas ekivalen dengan demikian σ_i adalah sikel yang saling asing. Selanjutnya ditunjukan bahwa $\phi = \sigma_1\sigma_2 \ldots \sigma_s$. Misalkan sebarang $a \in A$, bila $a \in O_i$, maka

$$\sigma_1\sigma_2 \ldots \sigma_s(a) = \sigma_i(a) = \phi(a),$$

dan bila $a \notin O_i$, maka $a \in O_{j_0}$ untuk suatu $j_0 \neq i$ dengan $1 \leq j_0 \leq s$, sehingga didapat

$$\sigma_1\sigma_2 \ldots \sigma_s(a) = \sigma_{j_0}(a) = \phi(a).$$

Jadi $\phi(a) = \sigma_1\sigma_2 \ldots \sigma_s(a)$ untuk semua $a \in A$. Dengan demikian $\phi = \sigma_1\sigma_2 \ldots \sigma_s$.

Contoh 2.4.9 Dalam S_6, diberikan sikel $\sigma = (1\ 3\ 5\ 4)$ dan $\tau = (1\ 5\ 6)$. Didapat

$$\tau\sigma = (1\ 5\ 6)(1\ 3\ 5\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 4 & 1 \end{pmatrix}$$

dan

$$\sigma\tau = (1\ 3\ 5\ 4)(1\ 5\ 6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 5 & 1 & 6 & 3 \end{pmatrix}.$$

Terlihat bahwa $\tau\sigma \neq \sigma\tau$.

Dalam Contoh 2.4.9 menunujukkan bahwa produk dari dua sikel tidak komutatif. Sifat berikut ini memberikan suatu kondisi bahwa produk dua sikel adalah komutatif.

Proposisi 2.4.2 Misalkan σ_1 dan σ_2 adalah dua sikel yang saling asing di S_n. Maka $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Bukti Misalkan O_1 dan O_2 masing-masing adalah orbit dari sikel σ_1 dan σ_2 yang saling asing. Catatan, untuk $i = 1$ atau $i = 2$, didapat $\sigma_i(a) \in O_i$ bila $a \in O_i$ dan $\sigma_i(a) = a$ bila $a \notin O_i$. Oleh karena itu, bila $b \in O_1$, maka $\sigma_1\sigma_2(b) = \sigma_1(\sigma_2(b)) = \sigma_1(b)$ dan $\sigma_2\sigma_1(b) = \sigma_2(\sigma_1(b)) = \sigma_1(b)$. Selanjutnya bila $b \notin O_1$ ini berarti $b \in O_2$, didapat $\sigma_1\sigma_2(b) = \sigma_1(\sigma_2(b)) = \sigma_2(b)$ dan $\sigma_2\sigma_1(b) = \sigma_2(\sigma_1(b)) = \sigma_2(b)$. Dengan demikian

$$\sigma_1\sigma_2(b) = \sigma_2\sigma_1(b),\ \forall b \in O_1 \cup O_2.$$

Jadi $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Proposisi yang baru saja dibahas dapat digunakan untuk menghitung order permutasi.

Contoh 2.4.10 Dalam S_{10}, diberikan permutasi

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 6 & 10 & 7 & 2 & 9 & 5 & 3 & 4 & 1 \end{pmatrix}.$$

Dalam notasi sikel didapat

$$\phi = (1\ 8\ 3\ 10)\ (2\ 6\ 9\ 4\ 7\ 5).$$

Order dari $(1\ 8\ 3\ 10)$ adalah 4 dan order dari $(2\ 6\ 9\ 4\ 7\ 5)$ adalah 6. Karena dua permutasi tersebut saling asing, maka komutatif, jadi $|\phi| = \text{kpk}(4, 6) = 12$.

Contoh 2.4.11 Elemen dari D_4 grup simetri dari segi empat beraturan dapat direpresentasikan sebagai permutasidalam S_4 dengan melabel empat titik sudut pada persegi: $1, 2, 3, 4$ sebagaimana dalam Contoh 2.1.6. Didapat

$\rho_0 = \text{identitas}$	$\tau = (1\ 2)(3\ 4)$
$\rho = (1\ 2\ 3\ 4)$	$\rho\tau = (1\ 2\ 3\ 4)(1\ 2)(3\ 4) = (1\ 3)$
$\rho^2 = (1\ 3)(2\ 4)$	$\rho^2\tau = (1\ 3)(2\ 4)(1\ 2)(3\ 4) = (1\ 4)(2\ 3)$
$\rho^3 = (1\ 4\ 3\ 2)$	$\rho^3\tau = (1\ 4\ 3\ 2)(1\ 2)(3\ 4) = (2\ 4)$.

Contoh 2.4.12 Untuk menghitung produk $\phi = (1\ 4)(1\ 3)(1\ 2)$, dilakukan sebagai berikut: Dimulai dari permutasi (1 2) yang mengubah 1 menjadi 2, sedangkan (1 3) dan (1 4) tidak mengubah 2, jadi $\phi(1) = 2$. Kemudian, $(1, 2)$ mengubah 2 menjadi 1 sedangkan $(1, 3)$ mengubah 1 menjadi 3 dan (1 4) tidak mengubah 3, jadi $\phi(2) = 3$. Berikutnya, (1 2) tidak mengubah 3, (1 3) mengubah 3 menjadi 1 dan (1 4) mengubah 1 menjadi 4, jadi $\phi(3) = 1$. Terakhir, (1 2) tidak mengubah 4, (1 3) juga tidak mengubah 4, sedangkan (1 4) mengubah 4 menjadi 1, jadi $\phi(4) = 1$. Dengan demikian didapat

$$\phi = (1\ 4)\ (1\ 3)\ (1\ 2) = (1\ 2\ 3\ 4).$$ ●

Teorema 2.4.4 Setiap sikel dapat ditulis sebagai produk dari sikel-2 (transposisi).

Bukti Suatu cara yang sama sebagaimana telah dikerjakan dalam Contoh 2.4.12, secara umum didapat

$$(a_1\ a_2\ a_3 \cdots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1}) \cdots\ (a_1\ a_3)(a_1\ a_2).$$ ✓●

Proposisi 2.4.3 Setiap permutasi dapat ditulis sebagai produk dari sikel-2.

Bukti Pertama, tulis sebarang permutasi sebagai produk dari sikel yang saling asing (berdasarkan Teorema 2.4.3). Selanjutnya pada sikel-sikel yang terbentuk gunakan Teorema 2.4.4 didapat semua sikel yang terbentuk dapat ditulis sebagai produk dari sikel-2. Dengan demikian sebarang permutasi dapat ditulis sebagai produk dari sikel-2. ✓●

Contoh 2.4.13 Umumnya, suatu permutasi dapat ditulis sebagai prduk dari sikel-2 dalam beberapa cara. Misalnya, dalam S_6 permutasi identitas dapat ditulis sebagai (1 2)(1 2) dan juga sebagai (1 2)(3 4)(1 2)(3 4) dan sebagainya. Permutasi (1 2 3) dapat ditulis sebagai (1 3)(1 2) tetapi dapat juga sebagai (3 4)(1 2) atau sebagai (4 5)(1 3)(4 5)(1 2). Permutasi (1 2 3 4) dapat ditulis sebagai (1 4)(1 3)(1 2) juga dapat ditulis sebagai (5 6)(1 4)(1 3)(5 6)(1 2). Catatan, apapun penyajian penulisan pada semua penulisan produk dari sikel-2 dengan cara yang berbeda tersebut semuanya berkaitan dengan banyaknya sikel-2 yang terbentuk genap atau ganjil. ●

Contoh 2.4.14 Misalkan n bilangan bulat positip. Untuk sebarang barisan berhingga dari bilangan bulat

$$s = (a_1, a_2, \ldots, a_n)$$

didefinisikan

$$p(s) \overset{\text{def}}{=} \prod_{1 \le i < j \le n} (a_i - a_j)$$

dan untuk sebarang $\tau \in S_n$, misalkan $\tau s = (a_{\tau(1)}, a_{\tau(2)}, \cdots, a_{\tau(n)})$. Misalnya untuk $n = 6$ dan $s = (1, 2, 3, 4, 5, 6)$, didapat

$$\begin{aligned} p(s) \quad = \quad & (1-2)(1-3)(1-4)(1-5)(1-6)(2-3)(2-4)(2-5)(2-6) \\ & (3-4)(3-5)(3-6)(4-5)(4-6)(5-6), \end{aligned}$$

bila $\tau = (2\ 5)$, maka $\tau s = (1, 5, 3, 4, 2, 6)$. Dengan demikian

$$\begin{aligned} p(\tau s) \quad = \quad & (1-5)(1-3)(1-4)(1-2)(1-6)(\underline{5-3})(\underline{5-4})(\underline{5-2})(5-6) \\ & (3-4)(\underline{3-2})(3-6)(\underline{4-2})(4-6)(2-6), \end{aligned}$$

dimana suku-suku yang digaris bawahi mempunyai tanda yang berubah. Suku-suku ini adalah $(2-5)$, suku-suku $(2-j)$ untuk $2<j<5$ dan suku-suku $(i-5)$ untuk $2<i<5$. Catatan ada lima suku-suku tersebut Jadi tampa melakukan proses perkalian yang panjang terlihat bahwa $p(\tau s)=(-1)^5 p(s)=-p(s)$.

Teorema 2.4.5 Dengan notasi sebagaimana baru saja dibahas, untuk sebarang bilangan bulat positip n, sebarang barisan bilangan bulat $s=(a_1,a_2,\ldots,a_n)$ dan sebarang sikel-2 $\tau\in S_n$, maka $p(\tau s)=-p(s)$.

Bukti Misalkan $\tau=(k\ l)$, dimana $k<l$ dan misalkan dibandingkan produk dari $p(s)$ dan $p(\tau s)$. Dibedakan lima kasus:

(1) Bila $i<k$, maka untuk sebarang j dengan $i<j$, didapat $i=\tau(i)$ dan $i<\tau(j)$, juga suku $(a_i-a_{\tau(j)})$ adalah suatu faktor dari $p(\tau s)$ dan $p(s)$.

(2) Bila $l<j$, maka untuk sebarang i dengan $i<j$, dengan argumen yang sama suku $(a_{\tau(i)}-a_j)$ adalah suatu faktor dari $p(\tau s)$ dan $p(s)$.

(3) Bila $i=k$, maka untuk sebarang j dengan $k<j<l$ didapat $j=\tau(j)$ dan $(a_{\tau(k)}-a_{\tau(j)})=(a_l-a_j)=-(a_j-a_l)$. Jadi suku (a_j-a_l) di $p(s)$ berubah tanda di $p(\tau s)$. Dalam kasus ini, ada sebanyak $(l-k-1)$ suku yang berubah.

(4) Bila $j=l$, maka untuk sebarang i dengan $k<i<l$, dengan argumen yang sama seperti yang dilakukan di (3), suku (a_l-a_k) di $p(s)$ berubah tanda di $p(\tau s)$. Ada sebanyak $(l-k-1)$ perubahan tanda.

(5) Terakhir, $(a_{\tau(k)}-a_{\tau(l)})=(a_l-a_k)=-(a_k-a_l)$, terlihat bahwa suku (a_k-a_l) di $p(s)$ mengalami perubahan tanda di $p(\tau s)$.

Dari lima kasus yang telah dibahas total perubahan tanda yang terjadi dari $p(s)$ menjadi $p(\tau s)$ adalah $2(l-k-1)+1$ yang merupakan bilangan bulat ganjil, dengan demikian didapat $p(\tau s)=-p(s)$.

Teorema 2.4.6 Tidak ada permutasi di S_n dapat ditulis sebagai produk dari sikel-2 sebanyak bilangan bulat genap dan sekaligus produk dari sikel-2 sebanyak bilangan bulat ganjil.

Bukti Menggunakan notasi yang sama sebagaimana dalam pembahasan Teorema 2.4.5, misalkan τ dan ρ dua sikel-2 di S_n. Maka untuk sebarang barisan $s=(a_1,a_2,\ldots,a_n)$ didapat

$$\begin{aligned}(\rho\tau)s &= (a_{\rho\tau(1)},a_{\rho\tau(2)},\ldots,a_{\rho\tau(n)})\\ &= (a_{\rho(\tau(1))},a_{\rho(\tau(2))},\ldots,a_{\rho(\tau(n))})\\ &= \rho(a_{\tau(1)},a_{\tau(2)},\ldots,a_{\tau(n)})\\ &= \rho(\tau s),\end{aligned}$$

dengan demikian didapat

$$p((\rho\tau)s)=p(\rho(\tau s))=-1\ p(\tau s)=(-1)^2 p(s).$$

Dengan cara yang sama, diberikan sebarang permutasi $\phi\in S_n$, bila ϕ adalah produk dari sikel-2 sebanyak k, maka $p(\phi s)=(-1)^k p(s)$. Dengan demikian diberikan sebarang $\phi\in S_n$,

maka k salah satu dari dari hal yang berikut: k selalu genap atau k selalu ganjil dan tidak mungkin terjadi kedua-duanya untuk segala cara penulisan ϕ sebagai suatu produk dari sikel-2.

Definisi 2.4.6 Suatu permutasi $\phi \in S_n$ dinamakan permutasi **genap** bila ϕ dapat dituliskan sebagai produk dari sikel-2 sebanyak bilangan bulat genap dan dinamakan permutasi **ganjil** bila ϕ dapat dituliskan sebagai produk dari sikel-2 sebanyak bilangan bulat ganjil.

Proposisi 2.4.3 menjamin bahwa sebarang permutasi dapat dikelompokkan sebagai permutasi genap atau ganjil. Sedangkan Teorema 2.4.6 menyatakan bahwa sebarang permutasi adalah genap atau ganjil tidak bisa terjadi dua-duanya.

Contoh 2.4.15 Dalam S_9, diberikan permutasi

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 5 & 1 & 7 & 8 & 2 & 6 & 4 & 3 \end{pmatrix}.$$

Permutasi ϕ dapat ditulis sebagai

$$\begin{aligned} \phi &= (1\ 9\ 3)(2\ 5\ 8\ 4\ 7\ 6) \\ &= (1\ 3)(1\ 9)(2\ 6)(2\ 7)(2\ 4)(2\ 8)(2\ 5). \end{aligned}$$

Terlihat bahwa ϕ bisa disajikan oleh produk sikel-2 sebanyak 7, dengan demikian ϕ adalah permutasi ganjil. Menggunakan fakta dalam sebarang grup, maka $(ab)^{-1} = b^{-1}a^{-1}$, didapat

$$\begin{aligned} \phi^{-1} &= (2\ 5)(2\ 8)(2\ 7)(2\ 6)(1\ 9)(1\ 3) \\ &= (2\ 6\ 7\ 4\ 8\ 5)(1\ 3\ 9) \\ &= (1\ 3\ 9)(2\ 6\ 7\ 4\ 8\ 5). \end{aligned}$$

Catatan bahwa, ϕ^{-1} juga permutasi ganjil.

Teorema 2.4.7 Misalkan A_n adalah himpunan semua permutasi genap di S_n. Maka A_n adalah subgrup dari S_n dalam hal ini A_n dinamakan **grup alternating** derajad n.

Bukti Menggunakan Teorema 2.2.2 cukup dibuktikan tertutup dan eksistensi invers. (**Tertutup**) Bila $\phi, \rho \in A_n$, maka ϕ dan ρ masing-masing dapat dituliskan sebagai produk dari sikel-2 sebanyak bilangan genap $2r$ dan $2s$. Dengan demikian $\phi\rho$ dapat dituliskan sebagai produk dari sikel-2 sebanyak $2r + 2s = \underbrace{2(r+s)}_{\text{genap}}$. Jadi $\phi\rho \in A_n$. (**Invers**) Bila $\phi \in A_n$, maka ϕ dapat dituliskan sebagai produk sikel-2:

$$\phi = \sigma_1\sigma_2 \cdots \sigma_{2r},\ 2r \text{ adalah genap},$$

didapat

$$\begin{aligned} \phi^{-1} &= (\sigma_1\sigma_2 \cdots \sigma_{2r})^{-1} \\ &= (\sigma_{2r})^{-1} \cdots (\sigma_2)^{-1}(\sigma_1)^{-1} \\ &= \sigma_{2r} \cdots \sigma_2\sigma_1. \end{aligned}$$

Terlihat bahwa $\phi^{-1} \in A_n$.

Contoh 2.4.16 Dalam S_3, dimana $|S_3| = 3! = 6$, himpunan permutasi genap adalah

$$A_3 = \{\rho_0 = \text{elemen identitas}, \rho = (1\ 2\ 3), \rho^2 = (1\ 3\ 2)\}.$$

Terlihat ada tepat sebanyak 3 pemutasi genap, jadi banyaknya permutasi ganjil dalam S_3 adalah $6 - 3 = 3$. Selanjutnya dalam S_4 dimana $|S_4| = 4! = 24$. Bila elemen di A_4 ditulis sebagai produk sikel-sikel yang saling asing, didapat tiga permutasi yang yang mengubah semua elemen, yaitu

$$\sigma_1 = (1\ 2)(3\ 4) \qquad \sigma_2 = (1\ 3)(2\ 4) \qquad \sigma_3 = (1\ 4)(2\ 3).$$

Untuk i dengan $1 \leq i \leq 4$ ada dua permutasi di A_4 yang membuat i tetap. Sehingga ada delapan permutasi di A_4 yang membuat tepat satu elemen tidak berubah (tetap) yaitu

$\rho_1 = (2\ 3\ 4)$	$\rho_1^2 = (2\ 4\ 3)$	1 tetap
$\rho_2 = (1\ 3\ 4)$	$\rho_2^2 = (1\ 4\ 3)$	2 tetap
$\rho_3 = (1\ 2\ 4)$	$\rho_3^2 = (1\ 4\ 2)$	3 tetap
$\rho_4 = (1\ 2\ 3)$	$\rho_4^2 = (1\ 3\ 2)$	4 tetap.

Dalam A_4 tidak ada permutasi yang membuat tetap dua elemen, elemen-elemen ini adalah sikel-2 yang tidak di A_4. Satu lagi elemen di A_4 adalah elemen identitas. Jadi ada dua belas elemen di A_4:

$$A_4 = \{\rho_0 = \text{elemen identiats}, \rho_1, \rho_1^2, \rho_2, \rho_2^2, \rho_3, \rho_3^2, \rho_4, \rho_4^2, \sigma_1, \sigma_2, \sigma_3\}.$$

Pada pembahasan A_3 dalam S_3 dan A_4 dalam S_4 tepat separuh dari permutasinya adalah permutasi genap. Hal ini berlaku secara umum untuk S_n dengan $n \geq 3$.

Teorema 2.4.8 Order dari grup alternating derajad n dengan $n \geq 3$ adalah

$$|A_n| = |S_n|/2 = n!/2.$$

Bukti Misalkan O_n adalah himpunan semua permutasi ganjil di S_n. Karena setiap permuatasi di S_n adalah salah satu diantara berikut yaitu berada di A_n atau berada di O_n tetapi tidak di keduanya. Dengan demikian

$$n! = |S_n| = |A_n| + |O_n|.$$

Jadi untuk membuktikan teorema cukup dibuktikan $|A_n| = |O_n|$. Untuk hal ini dibuat suatu pementaan $\gamma : A_n \to O_n$, dengan aturan $\gamma(\phi) = \phi(1\ 2)$, $\forall \phi \in A_n$. Selanjutnya dibuktikan γ adalah satu-satu dan pada. Pemetaan γ adalah satu-satu, sebab bila $\gamma(\phi) = \gamma(\psi)$ didapat $\phi(1\ 2) = \psi(1\ 2)$ hal ini berakibat bahwa

$$\phi = \phi(1\ 2)(1\ 2) = \psi(1\ 2)(1\ 2) = \psi.$$

Terlihat bahwa γ adalah satu-satu. Tinggal menunjukkan γ adalah pada sebagai berikut. Karena sebarang $\tau \in O_n$ adalah permutasi ganjil, maka $\tau(1\ 2) \in A_n$ adalah permuatsi genap yang memenuhi $\gamma(\tau(1\ 2)) = \tau(1\ 2)(1\ 2) = \tau$.

Contoh 2.4.17 Sebagaimana telah dibahas dalam Contoh 2.1.6 D_4 adalah subgrup dari S_4. Dengan cara yang sama, D_5 adalah subgrup dari S_5, elemen-elemen dari D_5 adalah:

$$\begin{array}{ll} \rho_0 = \text{identitas} & \tau = (1\ 3)(4\ 5) \\ \rho = (1\ 2\ 3\ 4\ 5) & \rho\tau = (1\ 2\ 3\ 4\ 5)(1\ 3)(4\ 5) = (1\ 4)(2\ 3) \\ \rho^2 = (1\ 3\ 5\ 2\ 4) & \rho^2\tau = (1\ 3\ 5\ 2\ 4)(1\ 3)(4\ 5) = (1\ 5)(2\ 4) \\ \rho^3 = (1\ 4\ 2\ 5\ 3) & \rho^3\tau = (1\ 4\ 2\ 5\ 3)(1\ 3)(4\ 5) = (2\ 5)(3\ 4) \\ \rho^4 = (1\ 5\ 4\ 3\ 2) & \rho^4\tau = (1\ 5\ 4\ 3\ 2)(1\ 3)(4\ 5) = (1\ 2)(3\ 5). \end{array}$$

Terlihat semua elemen di D_5 adalah permutasi genap dalam S_5. Jadi D_5 adalah subgrup dari A_5. ●

Latihan

Latihan 2.4.1 Tentukan mana fungsi berikut yang merupakan permutasi atau tidak. Jelaskan jawaban saudara.

1. $f : \mathbb{R} \to \mathbb{R}$, dimana $f(x) = 3x + \sqrt{2}$
2. $f : \mathbb{R} \to \mathbb{R}$, dimana $f(x) = 3x^2 + 2$
3. $f : \mathbb{Z} \to \mathbb{Z}$, dimana $f(x) = |x|$
4. $f : \mathbb{U}(5) \to \mathbb{U}(5)$, dimana $f(x) = x^{-1}$
5. $f : \mathbb{Z}_6 \to \mathbb{Z}_6$, dimana $f(x) = x + 3$.

Latihan 2.4.2 Dapatkan semua orbit dari permutasi berikut.

1. $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 3 & 2 & 1 & 4 & 5 \end{pmatrix}$
2. $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 5 & 9 & 4 & 1 & 8 & 7 & 2 & 3 \end{pmatrix}$
3. $\tau : \mathbb{Z} \to \mathbb{Z}$, dimana $\tau(x) = x + 5$
4. $\tau : \mathbb{Z} \to \mathbb{Z}$, dimana $\tau(x) = x - 3$.

Latihan 2.4.3 Misalkan

$$\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 4 & 1 & 6 & 7 & 2 & 5 \end{pmatrix}, \qquad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 1 & 2 & 7 & 8 & 5 & 3 \end{pmatrix}.$$

Hitung:
(a) $\phi\tau$ dan $\tau\phi$
(b) $\phi^2\tau$ dan $\phi\tau^2$
(c) ϕ^{-1} dan τ^{-1}
(d) $|\phi|$ dan $|\tau|$.

Latihan 2.4.4 Ungkapkan permutasi berikut sebagai suatu produk dari sikel yang saling asing dan hitung ordernya.

1. $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 8 & 2 & 9 & 7 & 5 & 4 & 3 & 10 & 6 \end{pmatrix}$
2. $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 6 & 2 & 4 & 3 & 7 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 4 & 5 & 1 & 3 & 2 \end{pmatrix}$
3. $\phi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 5 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 3 & 1 & 2 \end{pmatrix}$.

Latihan 2.4.5 Tunjukkan bahwa permutasi sikel-n mempunyai order n.

Latihan 2.4.6 Tunjukkan bahwa bila ρ dan σ di S_n adalah sikel-sikel yang saling asing dan $\phi = \rho\sigma$, maka $|\phi| = \text{kpk}(|\rho|, |\sigma|)$.

Latihan 2.4.7 Tunjukkan bahwa permutasi sikel-m adalah suatu permutasi genap bila dan hanya bila m adalah ganjil.

Latihan 2.4.8 Tunjukkan bahwa himpunan semua permuatsi ganjil dalam S_n bukan suatu subgrup dari S_n.

Latihan 2.4.9 Dapatkan order terbesar dari elemen-elemen dalam grup:
1. S_4, 2. S_5 3. S_6 4. S_7 5. A_5 6. A_6 7. A_7.

Latihan 2.4.10 Tunjukkan bahwa sebarang subgrup H dari grup permutasi S_n adalah salah satu dari hal yang berikut: setiap elemen dari H adalah suatu permutasi genap atau bila tidak $H = A_n$.

Latihan 2.4.11 Buat tabel hasil operasi dalam grup A_4.

Latihan 2.4.12 Misalkan $H = \{\sigma \in S_4 \,|\, \sigma(2) = 2\}$.
(a) Tunjukkan bahwa H adalah subgrup dari S_4.
(b) Berapakah $|H|$?
(c) Dapatkan semua permutasi genap dalam H.

Latihan 2.4.13 Misalkan $n \geq 3$, $i \leq 3$ dan $H = \{\sigma \in S_n \,|\, \sigma(i) = i\}$.
(a) Tunjukkan bahwa H adalah subgrup dari S_n.
(b) Berapakah $|H|$?
(c) Dapatkan semua permutasi genap dalam H.

Latihan 2.4.14 Tunjukkan bahwa untuk sebarang bilangan bulat $n \geq 3$ grup S_n adalah takkomutatif.

Latihan 2.4.15 Dapatkan semua elemen yang berorder 2 dalam S_4.

Latihan 2.4.16 Tunjukkan bahwa bila $\sigma \in S_n$ dan $|\sigma| = 2$, maka σ adalah suatu produk dari sikel-2 yang saling asing.

Latihan 2.4.17 Tunjukkan bahwa bila $\sigma \in S_n$, maka σ dapat dituliskan sebagai suatu produk dari sikel-3.

Latihan 2.4.18 Tunjukkan bahwa bila $\sigma \in S_n$, maka σ dapat dituliskan sebagai suatu produk dari sikel-3 $(1\ 2\ s)$ dimana $s = 3, 4, \ldots, n$.

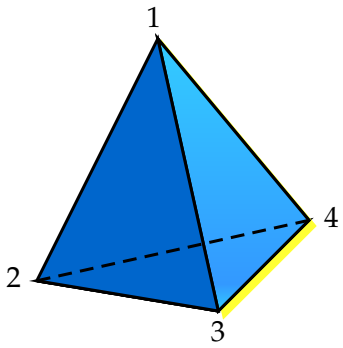
Latihan 2.4.19 Tunjukkan bahwa setiap permutasi $\rho \in S_n$ dapat dituliskan sebagai suatu produk sikel-2 berbentuk $(i\ i+1)$ dimana $1 \leq i \leq n$.

Latihan 2.4.20 Tunjukkan bahwa setiap permutasi $\phi \in S_n$ dapat dituliskan sebagai suatu produk dari pangkat $\rho = (1\ 2\ 3\ \cdots\ n)$ dan $\phi = (1\ 2)$.

Latihan 2.4.21 Tunjukkan bahwa bila $m \leq n$, maka banyaknya sikel-m $(a_1\ a_2\ a_3\ \cdots a_m)$ dalam S_n adalah

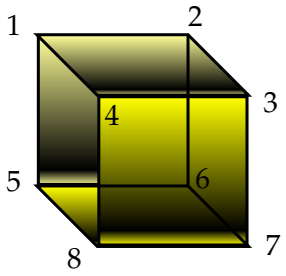
$$n(n-1)(n-2)\cdots(n-m+1)/m.$$

Latihan 2.4.22 Diberikan gambar tetrahedon teratur berikut.
(a) Dapatkan semua rotasi yang mugkin dari tetrahedron teratur.
(b) Dapatkan semua rotasi dari tetrahedron teratur yang membentuk grup.



Gambar 2.7: Tetrahedron

Latihan 2.4.23 Diberikan gambar kubus berikut.



Gambar 2.8: Kubus

Dapatkan suatu grup yang elemen-elemennya berkaitan dengan rotasi dari kubus.

Bab 3

Homomorpisma Grup

Pada pembahasan sebelumnya telah diberikan pengertian dari grup dan sifat-sifatnya dan dibahas berbagai macam grup yang berbeda dan subgrupnya. Pada bab ini dikenalkan empat pengertian dasar baru kesemuanya mempunyai keterkaitan yang erat. Pertama ditunjukkan bagaimana suatu subgrup menentukan suatu relasi ekivalen pada elemen-elemen grup. Oleh karena itu mempartisi grup kedalam klas ekivalen yang dinamakan *koset* dari subgrup. Partisi ini digunakan untuk memberikan suatu bukti yang sederhana dan elok pada teorema Lagrange merupakan hasil yang sangat dasar dalam teori grup. Kedua dikenalkan suatu pemetaan tertentu dikenakan pada grup yang dinamakan *homomorpisma*. Ketiga, ditunjukkan bagaimana pengertian suatu homomorpisma menimbulkan suatu gagasan subgrup khusus yang dinamakan *subgrup normal*. Keempat, image dari suatu grup oleh homomorpisma adalah suatu grup dengan struktur khusus. Selanjutnya ditunjukkan bahwa hal itu dapat dianggap sebagai suatu grup yang elemen-elemennya merupakan koset dari subgrup normal dari grup yang diberikan. Grup yang demikian dinamakan *grup kuasi/grup faktor*. Empat konsep baru: koset, homomorpisma, subgrup normal dan grup kuasi akan tampak alami setelah disadari betapa saling keterkaitannya.

3.1 Koset dan Teorema Lagrange

Sudah ditunjukkan bahwa dalam Teorema 2.3.4 bila G adalah suatu grup siklik berhingga dan H adalah suatu subgrup dari G, maka order H membagi order G. Pada bagian ini dibuktikan teorema Lagrange, yang menyatakan pernyataan dalam Teorema 2.3.4 berlaku untuk sebarang grup berhingga G. Untuk membuktikan hal ini, pertama ditunjukkan bagaimana suatu subgrup H menentukan suatu relasi ekivalen pada G. Kemudian ditunjukkan bahwa masing-masing klas ekivalen ini banyaknya elemen adalah sama dan sama dengan banyaknya elemen H. Dari sini terlihat bahwa banyaknya elemen-elemen di G adalah kelipatan dari banyaknya elemen-elemen di H. Dimulai dari contoh-contoh untuk memberikan gambaran bagaimana sebarang subgrup H dari sebarang grup G menentukan suatu relasi ekivalen pada G, bahkan hal ini tidak hanya pada grup berorder hingga.

Contoh 3.1.1 Dalam grup $\mathbb{Z}$, misalkan subgrup $3\mathbb{Z} = \langle 3 \rangle$. Untuk bilangan bulat $a, b \in \mathbb{Z}$, relasi ekivalen $a \sim b$ berlaku bila $b - a \in 3\mathbb{Z}$ atau dengan kata lain, bila $a \equiv b \mod 3$. Maka tiga klas ekivalen adalah:

$3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$, $1 + 3\mathbb{Z} = \{\ldots, -5, -2, 1, 4, 7, \ldots\}$,
dan $2 + 3\mathbb{Z} = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$.

Contoh 3.1.2 Dalam grup $\mathbb{Z}_{15}$, misalkan subgrup $H = \langle [3]_{15} \rangle$. Maka H mempartisi $\mathbb{Z}_{15}$ sebagai berikut:
$H = \{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\}$, $[1]_{15} + H = \{[1]_{15}, [4]_{15}, [7]_{15}, [10]_{15}, [13]_{15}\}$,
dan $[2]_{15} + H = \{[2]_{15}, [5]_{15}, [8]_{15}, [11]_{15}, [14]_{15}\}$.
Lagi, dari apa yang dibahas ini secara langsung relasi ekivalen dapat diungkapkan sebagai $a \sim b$ bila $b - a \in H$.

Berikut ini dinyatakan bahwa suatu relasi ekivalen ditentukan oleh suatu subgrup H dari sebarang grup G.

Teorema 3.1.1 Misalkan G sebarang grup dan H adalah subgrup dari G. Maka

(1) Untuk $a, b \in G$, relasi yang didefinisikan oleh $a \sim b$ bila $a^{-1}b \in H$ adalah suatu relasi ekivalen pada G.

(2) Untuk sebarang $a \in G$, klas ekivalen dari a adalah $aH = \{ah \mid h \in H\}$.

Bukti

(1) (Refleksif) Untuk sebarang $a \in G$, karena H subgrup dari G didapat $e = a^{-1}a \in H$. Jadi $a \sim a$.
(Simetri) Untuk sebarang $a, b \in G$. Bila $a \sim b$, maka $a^{-1}b \in H$. Karena H subgrup dari G, maka $b^{-1}a = (a^{-1}b)^{-1} \in H$. Jadi $b \sim a$.
(Transitif) Untuk sebarang $a, b, c \in G$. Bila $a \sim b$ dan $b \sim c$, maka $a^{-1}b \in H$ dan $b^{-1}c \in H$. Karena H subgrup dari G, didapat $a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$. Jadi $a \sim c$.

(2) Untuk sebarang $a \in G$ klas ekivalen dari a memuat semua $x \in G$ yang memenuhi $a^{-1}x \in H$. Bila $x \sim a$, maka $x = a(a^{-1}x) = ah$ dimana $h = a^{-1}x \in H$. Sebaliknya, bila $x = ah$ untuk beberapa $h \in H$, maka $a^{-1}x = (a^{-1}a)h = h \in H$ hal ini menunjukkan bahwa $x \sim a$.

Definisi 3.1.1 Misalkan G adalah suatu grup, H adalah suatu subgrup dari G dan sebarang $a \in G$ tetapi tetap. Maka himpunan $aH = \{ah \mid h \in H\}$ dinamakan **koset kiri** dari H dalam grup G dan himpunan $Ha = \{ha \mid h \in H\}$ dinamakan **koset kanan** dari H dalam grup G.

Contoh 3.1.3 Dalam $S_3 = \{\rho_0, \rho, \rho^2, \mu_1, \mu_2, \mu_3\}$ dan $H = \langle \mu_1 \rangle$, maka koset kiri dari H adalah:

$$H = \{\rho_0, \mu_1\}, \quad \rho H = \{\rho, \rho\mu_1 = \mu_3\} \quad \text{dan} \quad \rho^2 H = \{\rho^2, \rho^2\mu_1 = \mu_2\}.$$

Sedangkan koset kanan dari H adalah:

$$H = \{\rho_0, \mu_1\}, \quad H\rho = \{\rho, \mu_1\rho = \mu_2\} \quad \text{dan} \quad H\rho^2 = \{\rho^2, \mu_1\rho^2 = \mu_3\}.$$

Perlu diperhatikan bahwa dua relasi ekivalen yang ditentukan oleh $H = \langle \mu_1 \rangle$ memberikan dua partisi yang berbeda.

Dalam suatu grup komutatif G, karena semua elemen di G komutatif, maka koset kiri dan kanan dari suatu subgrup adalah sama.

Contoh 3.1.4 Dalam $\mathbb{Z}$ perhatikan bahwa subgrup $3\mathbb{Z} \supseteq 6\mathbb{Z}$. Koset dari $6\mathbb{Z}$ dalam $\mathbb{Z}$ adalah

$$6\mathbb{Z},\ 1+6\mathbb{Z},\ 3+6\mathbb{Z},\ 4+6\mathbb{Z},\ 5+6\mathbb{Z}.$$

Sedangkan koset dari $6\mathbb{Z}$ dalam $3\mathbb{Z}$ adalah $6\mathbb{Z}$ dan $3+6\mathbb{Z}$. ●

Teorema berikut memperlihatkan bahwa koset kiri dari suatu subgrup H dalam grup G mempartisi G menjadi klas-klas yang saling asing.

Teorema 3.1.2 Untuk setiap dua elemen a dan b di grup G dan $H < G$, maka

1. Bila $a \sim b$, maka $aH = bH$ ($Ha = Hb$).
2. Bila $a \nsim b$, maka $aH \cap bH = \varnothing$ ($Ha \cap Hb = \varnothing$).
3. $aH = bH$ bila dan hanya bila $a^{-1}b \in H$ ($ab^{-1} \in H$).

Bukti

1. Misalkan $a \sim b$, maka $a^{-1}b = h_0$ untuk suatu $h_0 \in H$, didapat $b = ah_0$ atau $a = bh_0^{-1}$. Misalkan sebarang $ah \in aH$, didapat $ah = h(bh_0^{-1})h = b(hh_0) \in bH$. Jadi $aH \subset bH$. Misalkan sebarang $bh \in bH$, maka $bh = (ah_0)h = a(hh_0) \in aH$. Jadi $bH_{\subset}aH$. Maka dari itu, didapat $aH = bH$.

2. Misalkan $a \nsim b$ dan andaikan $g \in aH \cap bH$, maka $g = ah_1$ untuk suatu $h_1 \in H$ dan $g = bh_2$ untuk suatu $h_2 \in H$. Jadi $a^{-1} = h_1 g^{-1}$ dan $b = gh_2^{-1}$. Didapat

$$a^{-1}b = (h_1 g^{-1})(gh_2^{-1}) = h_1(g^{-1}g)h_2^{-1} = h_1 e h_2^{-1} = h_1 h_2^{-1} \in H \quad \text{(sebab } H < G\text{)}.$$

   Terlihat bahwa $a \sim b$, kontradiksi dengan kenyataan bahwa $a \nsim b$. Dengan demikian haruslah $aH \cap bH = \varnothing$.

3. Misalkan $a^{-1}b \in H$, hal ini berarti bahwa $a \sim b$. Akibatnya menurut hasil 1. didapat $aH = bH$. Sebaliknya misalkan $aH = bH$. Karena $b \in bH$, maka $b \in aH$. Jadi $b = ah$ untuk beberapa $h \in h$ atau $a^{-1}b = h \in H$. ✓

Teorema berikut menjelaskan bahwa banyaknya elemen sebarang koset dalam satu koset dengan koset yang lainnya adalah sama.

Teorema 3.1.3 Misalkan G adalah grup dan $H < G$. Maka untuk sebarang $a \in G$, $|H| = |aH| = |Ha|$.

Bukti Didefinisikan pemetaan $f : H \to aH$ oleh $f(h) \stackrel{\text{def}}{=} ah$, $\forall h \in H$. Pemetaan f adalah satu-satu, sebab bila $f(h) = f(h_1)$ atau $ah = ah_1$, maka $h = h_1$. Pemetaan f adalah pada, sebab bila diberikan sebarang $ah \in aH$, maka dapat dipilih $h \in H$ sehingga $f(h) = ah$. Jadi pemetaan f adalah satu-satu pada, maka dari itu $|H| = |aH|$. Dengan cara yang sama bila didifisikan pemetaan $g : H \to Ha$ oleh $g(h) \stackrel{\text{def}}{=} ha$, $\forall h \in H$. Maka pemetaan g adalah satu-satu, sebab bila $g(h) = g(h_1)$ atau $ha = h_1 a$, maka $h = h_1$. Pemetaan g adalah pada, sebab bila diberikan sebarang $ha \in Ha$, maka dapat dipilih $h \in H$ sehingga $g(h) = ha$. Jadi pemetaan g adalah satu-satu pada, maka dari itu $|H| = |Ha|$. ✓

Teori-teori yang telah dibahas digunakan untuk membuktikan teorema Lagrange, sebagaimana berikut.

Teorema 3.1.4 (**Teorema Lagrange**) Misalkan G grup berhingga dan $H < G$. Maka

(1) $|H|$ membagi $|G|$.

(2) Banyak nya koset yang berbeda dari H sama dengan $|G|/|H|$.

Bukti Menggunakan Teorema 3.1.2 didapat koset kiri kiri dari H mempartisi G menjadi klas-klas yang saling asing. Misalkan

$$a_1H, a_2H, \ldots, a_sH$$

adalah semua koset kiri dari H yang saling asing dalam G, maka didapat

$$|G| = \overbrace{|a_1H| + |a_2H| + \cdots + |a_sH|}^{s},$$

dan dari Teorema 3.1.3 didapat $|a_iH| = |H|$ untuk semua $a_i \in G$. Jadi $|G| = s \cdot |H|$ dan $s = |G|/|H$ adalah banyaknya koset kiri dari H yang berbeda dalam G. ✓

Catatan bahwa, jugah sudah dibuktikan bahwa $|aH| = |Ha| = |H|$. Dengan demikian, $|G|/|H|$ juga adalah banyaknya koset kanan yang berbeda dari H dalam G. Berikut ini diberikan nama untuk banyaknya koset yang berbeda dari H dalam G.

Definisi 3.1.2 Misalkan G adalah suatu grup dan suatu subgrup $H < G$. Maka banyaknya koset kiri dari H dalam G dinamakan **Indeks** dari H dalam G dan dinotasikan oleh $\text{Indeks}_G(H)$ atau $[G : H]$. ✓

Mengingat Definisi 3.1.2, maka dua pernyataan dalam Teorema 3.1.4 dapat dikombinasikan dalam formulasi $|G| = |H| \cdot [G : H]$.

Contoh 3.1.5 Misalkan H adalah subgrup dari grup G dengan $|G| = 10$, maka menurut teorema Lagrange didapat $|H| = 1, 2, 5$ atau 10. Misalnya, bila

$$G = D_5 = \{\rho_0, \rho, \rho^2, \rho^3, \rho^4, \tau, \rho\tau, \rho^2\tau, \rho^3\tau, \rho^4\tau\}$$

sebagaimana dalam Contoh 2.4.17, maka

$$\left|\langle\rho_0\rangle\right| = 1, \ \left|\left\langle\rho^i\right\rangle\right| = 5, \ |\langle\tau\rangle| = \left|\left\langle\rho^i\tau\right\rangle\right| = 2, \text{ untuk } 1 \le i \le 4$$

dan $|D_5| = 10$. ●

Contoh 3.1.6 Grup simetri S_3 dapat dilihat sebagai suatu subgrup dari grup simetri S_4 dimana $S_3 = \{\phi \in S_4 \,|\, \phi(4) = 4\}$. Karena $|S_4| = 4! = 24$ dan $|S_3| = 3! = 6$, indeks $[S_4 : S_3] = 24/6 = 4$. Dengan demikian S_3 mempunyai empat koset dalam S_4. Untuk mendapatkan empat koset yang berbeda dari S_3, pertama dapatkan elemen $\phi \in S_4$ tetapi $\phi \notin S_3$, dengan kata lain $\phi(4) \neq 4$. Salah satu elemen ini adalah $\phi = (1\ 2\ 3\ 4) \in S_4$. Karena $\phi \notin S_3$ dengan menggunakan Teorema 3.1.2 bagian (3) didapat $\phi S_3 \neq S_3$. Juga $\phi^2 = (1\ 3)(2\ 4) \notin S_3$ dan $\phi^{-1}\phi^2 \notin S_3$, gunakan lagi Teorema 3.1.2 bagian (3) didapat $\phi^2 S_3 \neq S_3$ dan $\phi^2 S_3 \neq \phi S_3$. Terakhir, $\phi^3 = (1\ 4\ 3\ 2) \notin S_3$, $\phi^{-1}\phi^3 \notin S_3$ dan $\phi^2\phi^3 \notin S_3$. Dengan demikian sekali lagi digunakan Teorema 3.1.2 bagian (3) didapat

$$S_3, \ \phi S_3, \ \phi^2 S_3 \ \text{ dan } \ \phi^3 S_3$$

adalah empat koset yang berbeda dari S_3 dalam S_4. ●

Akibat berikut adalah akibat langsung dari teorema Lagrange.

Akibat 3.1.1 Dalam suatu grup berhingga G, order $|a|$ dari sebarang elemen a membagi order $|G|$ dari grup G.

Bukti Untuk sebarang elemen $a \in G$ dengan $|G|$ berhingga, misalkan $H = \langle a \rangle$. Maka H adalah suatu subgrup dari G dan menurut Akibat 2.3.3 maka $|H| = |\langle a \rangle| = |a|$. Selanjutnya gunakan teorema Lagrange bagian (1) didapat $|H|$ membagi $|G|$. Dengan demikian oreder $|a|$ membagi $|G|$. ✓

Akibat berikut memberikan suatu hasil yang **sangat penting**.

Akibat 3.1.2 Misalkan G adalah suatu grup berhingga dan sebarang elemen $a \in G$. Maka $a^{|G|} = e$, dimana e adalah elemen netral dari G.

Bukti Dari kesimpulan 3.1.1 didapat

$$a^{|G|} = a^{m|a|}, \text{ untuk beberapa } m \in \mathbb{Z}.$$

Gunakan Akibat 2.3.1, didapat

$$a^{m|a|} = \left(a^{|a|}\right)^m = e^m = e. \quad ✓$$

Contoh 3.1.7 Misalkan G adalah grup berorder 7. Maka dengan menggunakan Teorema Lagrange G tidak mempunyai subgrup sejati tak-trivial. Sebab misalkan sebarang $a \in G$ dan $a \neq e$, maka $|a| \neq 1$. Jadi $|a| = 7$ dan $G = \langle a \rangle$ adalah siklik. ●

Teorema 3.1.5 Suatu grup yang berorder p dengan p adalah prima adalah grup siklik.

Bukti Misalkan grup G dengan $|G| = p$ dimana p adalah prima dan sebarang $a \in G$ dengan $a \neq e$. Maka $|a| \neq 1$, jadi $|a| = p = |G|$. Dengan demikian $G = \langle a \rangle$. ✓

Contoh 3.1.8 Grup G taksiklik yang berorder $|G| < 7$ yang sudah dijumpai adalah dua macam:

(1) Grup yang berorder 4, misalnya adalah $\mathbb{U}(8), \mathbb{U}(12)$ dan grup-4 Klein V sebagaimana diberikan dalam Contoh 2.1.20.

(2) Grup berorder 6, misalnya adalah S_3. ●

Pada bahasan akhir ini ditunjukkan suatu hasil terkenal dalam teori bilangan, yaitu Teorema Euler yang dapat diturukan dari Teorema Lagrange.

Teorema 3.1.6 Diberikan bilangan bulat $n \geq 2$ dan a dengan $\text{fpb}(a, n) = 1$. Maka $a^{\phi(n)} \equiv 1 \mod n$.

Bukti Gunakan algoritma pembagian bilangan bulat didapat, $a = qn + r$, dimana $0 \leq r < n$. Karena $\text{fpb}(a, n) = 1$, maka $\text{fpb}(r, n) = \text{fpb}(a - qn, n) = 1$. Jadi $r \in \mathbb{U}(n)$. Karena $|\mathbb{U}(n)| = \phi(n)$ dan gunakan Akibat 3.1.2 didapat $r^{\phi(n)} = 1$ di $\mathbb{U}(n)$. Dengan demikian $a^{\phi(n)} \equiv r^{\phi(n)} \equiv 1 \mod n$. ✓

Teorema 3.1.7 (**Teori Fermat Kecil**) Bila p adalah prima, maka untuk sebarang bilangan bulat a didapat $a^p \equiv a \mod p$.

Bukti Bila p membagi a, maka $a \equiv 0 \mod p$ dan jelas bahwa $a^p \equiv 0 \mod p$. Bila p tidak membagi a, maka fpb$(a,p) = 1$ dan gunakan Teorema 3.1.6 didapat $a^{\phi(p)} \equiv 1 \mod p$. Tetapi $\phi(p) = p-1$. Dengan demikian didapat $a^{p-1} = a^{\phi(p)} \equiv 1 \mod p$. Jadi $a^p \equiv a \mod p$.

Contoh 3.1.9 Misalkan dihitung sisa pembagian dari 5^{148} oleh 7. Karena $5^6 \equiv 1 \mod 7$ dan $148 = 24 \cdot 6 + 4$ didapat

$$5^{148} = (5^6)^{24} \cdot 5^4 \equiv 1 \cdot 5^4 \mod 7 \equiv (-2)^4 \mod 7 \equiv 2 \mod 7.$$

Jadi sisa pembagian dari 5^{148} oleh 7 adalah 2.

Contoh 3.1.10 Misalkan akan ditunjukkan bahwa untuk sebarang bilngan bulat n maka $n^{13} - n$ habis dibagi oleh 15. Untuk menunjukkan bahwa $15 = 3 \cdot 5$ membagi $n^{13} - n = n(n^{12} - 1)$ cukup ditunjukkan bahwa 3 dan 5 keduanya membagi $n(n^{12} - 1)$. Jelas bahwa bila 3 membagi n, maka 3 membagi $n(n^{12} - 1)$. Bila 3 tidak membagi n, maka $n^2 \equiv 1 \mod 3$, jadi $n^{12} - 1 = (n^2)^6 - 1 \equiv 0 \mod 3$. Terlihat bahwa 3 membagi $(n^{12} - 1)$. Dengan demikan 3 membagi $n(n^{12} - 1)$. Dengan cara yang sama didapat, bila 5 membagi n, maka 5 membagi $n(n^{12} - 1)$ dan bila 5 tidak membagi n, maka $n^4 \equiv 1 \mod 5$. Jadi, $n^{12} - 1 = (n^2)^6 - 1 \equiv 0 \mod 5$. Terlihat bahwa 5 membagi $n^{12} - 1$. Dengan demikian 5 membagi $n(n^{12} - 1)$.

Latihan

Latihan 3.1.1 Dapatkan semua koset dari subgrup $5\mathbb{Z}$ dalam $\mathbb{Z}$.

Latihan 3.1.2 Dapatkan semua koset dari $9\mathbb{Z}$ dalam $\mathbb{Z}$ dan dalam $3\mathbb{Z}$.

Latihan 3.1.3 Dapatkan semua koset dari $\langle 6 \rangle$ dalam $\mathbb{Z}_{12}$ dan semua koset dari $\langle 6 \rangle$ dalam subgrup $\langle 2 \rangle$ dari grup $\mathbb{Z}_{12}$.

Latihan 3.1.4 Dalam D_4 dapatkan semua koset kiri dan kanan dari $\langle \tau \rangle$.

Latihan 3.1.5 Dapatkan indeks dari $\langle 10 \rangle$ dalam $\mathbb{Z}_{12}$.

Latihan 3.1.6 Dapatkan indeks dari $\langle \mu_2 \rangle$ dalam S_3.

Latihan 3.1.7 Dapatkan indeks dari $\langle \rho^2\tau \rangle$ dalam D_4.

Latihan 3.1.8 Misalkan $H = \{\phi \in S_n \mid \phi(n) = n\}$. Dapatkan indeks dari H dalam S_n.

Latihan 3.1.9 Misalkan H adalah subgrup dari grup G. Tunjukkan untuk sebarang $a \in G$ bahwa $aH = H$ bila dan hanya bila $a \in H$.

Latihan 3.1.10 Misalkan $H = 5\mathbb{Z}$ dalam $\mathbb{Z}$. Tentukan apakah koset dari H berikut adalah sama:

(a) $12 + H$ dan $27 + H$

(b) $13 + H$ dan $-2 + H$

(c) $126 + H$ dan $-1 + H$.

Latihan 3.1.11 Diberikan grup G berorder 42. Dapatkan semua order yang mungkin untuk subgrup H dari G. Untuk hal yang demikian tentukan banyaknya koset kiri dari H.

Latihan 3.1.12 Misalkan $G = \langle a \rangle$ adalah suatu grup siklik berorder 60 dan $H = \left\langle a^{35} \right\rangle$. Daftarkan semua koset kiri dari H dalam GG.

Latihan 3.1.13 Misalkan G adalah grup berorder 36. Bila G mempunyai suatu elemen $a \in G$ dimana $a^{12} \neq e$ dan $a^{18} \neq e$. Tunjukkan bahwa G adalah siklik.

Latihan 3.1.14 Misalkan grup G dengan $|G| < 300$. Bila G mempunyai suatu subgrup H berorder 24 dan suatu subgrup K berorder 54, berapakah order G?

Latihan 3.1.15 Misalkan H dan K adalah subgrup dari grup G dimana $|H| = 9$, $|K| = 12$ dan indeks $[G : H \cap K] \neq |G|$. Dapatkan $|H \cap K|$.

Latihan 3.1.16 Misalkan G grup dengan $|G| = p^2$, dimana p adalah prima. Tunjukkan bahwa sebarang subgrup sejati dari G adalah siklik.

Latihan 3.1.17 Diberikan grup G dengan $|G| = pq$ dimana p dan q adalah prima. Tunjukkan bahwa setiap subgrup sejati dari G adalah siklik.

Latihan 3.1.18 Misalkan H dan K adalah subgrup dari grup G dengan $|H| = n$, $|K| = m$ dan $\text{fpb}(m, n) = 1$. Tunjukkan bahwa $H \cap K = \{e\}$.

Latihan 3.1.19 Misalkan G adalah grup dan $a, b \in G$ dengan $|a| = n$, $|b| = m$ dan $\text{fpb}(m, n) = 1$. Bila untuk beberapa bilangan bulat k didapat $a^k = b^k$, tunjukkan bahwa mn membagi k. (Petunjuk gunakan Latihan 3.1.18).

Latihan 3.1.20 Tunjukkan bahwa untuk setiap bilangan bulat n, bilangan $n^{19} - n$ habis dibagi oleh 21.

Latihan 3.1.21 Dapatkan sisa pembagian 9^{1573} oleh 11.

Latihan 3.1.22 Hitung $\phi(p^2)$, dimana p adalah prima.

Latihan 3.1.23 Hitung $\phi(pq)$, dimana p dan q adalah prima berbeda.

Latihan 3.1.24 Dapatkan sisa pembagian 5^{1258} oleh 12.

Latihan 3.1.25 Misalkan G adalah grup takkomutatif dimana $|G| = 2p$ dan p adalah prima. Tunjukkan bahwa ada suatu elemen $g \in G$ yang memenuhi $|g| = p$.

Latihan 3.1.26 Misalkan G adalah grup takkomutatif dimana $|G| = 2p$ dan p adalah prima. Tunjukkan bahwa G mempunyai sebanyak p elemen yang berorder 2.

Latihan 3.1.27 Misalkan G adalah suatu grup berorder $|G| > 1$ yang mana G tidak mempunyai subgrup sejati tak-trivial. Tunjukkan bahwa G adalah suatu grup siklik berhingga berorder prima.

Latihan 3.1.28 Misalkan G adalah grup berorder 15. Tunjukkan bahwa G memuat suatu elemen berorder 3.

Latihan 3.1.29 Misalkan H adalah suatu subgrup dari grup berhingga G dan K adalah suatu subgrup dari H. Misalkan indeks $[G : H] = n$ dan indeks $[H : K] = m$. Tunjukkan bahwa indeks $[G : K] = mn$. (Petunjuk: Misalkan x_iH adalah koset-koset kiri yang berbeda dari H dalam G dan y_jK adalah koset-koset kiri yang berbeda dari K dalam H. Tunjukkan bahwa x_iy_jK adalah koset-koset kiriyang berbeda dari K dalam G).

Latihan 3.1.30 Misalkan H dan K adalah subgrup dari grup G dan untuk semua $a, b \in G$, $a \sim b$ bila dan hanya bila $a = hbk$ untuk beberapa $h \in H$ dan beberapa $k \in K$. Tunjukkan bahwa relasi $\sim$ adalah relasi ekivalen. Uraikan klas ekivalennya (klas ekivalen ini dinamakan **koset ganda**).

Latihan 3.1.31 Misalkan H dan K adalah subgrup dari suatu grup berhingga G dengan indeks $[G : H] = n$ dan indeks $[G : K] = m$. Tunjukkan bahwa

$$\text{kpk}(m, n) \leq [G : H \cap K] \leq mn.$$

Latihan 3.1.32 Diberikan H dan K adalah subgrup berhingga dari suatu grup G. Misalkan himpunan

$$HK = \{hk \,|\, h \in H, k \in K\}.$$

Tunjukkan bahwa $|HK| = |H|\,|K|/|H \cap K|$. (Petunjuk: $HK = \bigcup_{h \in H} hK$).

Latihan 3.1.33 Untuk sebarang bilangan positip n tunjukkan bahwa $n = \sum_{d|n} \phi(d)$, dimana ϕ adalah fungsi-ϕ Euler.

Latihan 3.1.34 Tunjukkan bahwa kebalikan dari Teorema Lagrange tidak benar. (Petunjuk: Tunjukkan bahwa A_4 tidak mempunyai subgrup yang berorder 6).

3.2 Homomorpisma

Sudah dibahas mengenai apa grup dan subgrup dan beberapa macam grup: siklik dan taksiklik, komutatif dan takkomutatif, berhingga dan takberhingga. Apapun itu, belum dibahas pemetaan diantara grup. Karena grup bukan sekedar suatu himpunan, tatapi bersamaan himpunan ini melekat suatu operasi biner yang memenuhi beberapa aksiomatik tertentu. Pemetaan diantara grup yang akan dibahas dikaitkan dengan operasi biner yang berlaku pada masing-masing grup.

Contoh 3.2.1 Dibahas tiga fungsi berbeda dari $\mathbb{Z}$ to $\mathbb{Z}$ dan diidentifikasi beberapa sifat dari fungsi tersebut Misalkan tiga fungsi $f, g, h : \mathbb{Z} \to \mathbb{Z}$ yang diberikan oleh

(1) $f(x) = x^2$

(2) $g(x) = x + 1$

(3) $h(x) = 2x$.

Dalam kasus (1), image dari f bukan suatu subgrup dari $\mathbb{Z}$. Juga bila diambil dua elemen $x, y \in \mathbb{Z}$ didapat

$$f(x + y) = (x + y)^2 = x^2 + 2xy + y^2 \neq x^2 + y^2 = f(x) + f(y).$$

Dalam kasus (2), image dari g adalah subgrup dari $\mathbb{Z}$, sebab $\text{im}(f) = \mathbb{Z}$ dan

$$g(x + y) = x + y + 1 \neq (x + 1) + (y + 1) = g(x) + g(y).$$

Dalam kasus (3), image dari h adalah subgrup $2\mathbb{Z}$ dari grup $\mathbb{Z}$ dan

$$h(x + y) = 2(x + y) = 2x + 2y = h(x) + h(y).$$ ●

Definisi 3.2.1 Diberikan suatu pemetaan $\phi : G \to G'$ dimana G dan G' adalah grup. Pemetaan ϕ dinamakan **homomorpisma** grup bila memenuhi

$$\phi(ab) = \phi(a)\phi(b), \text{ untuk semua } a, b \in G.$$

Perlu diperhatikan bahwa, dalam $\phi(ab)$ operasi biner yang digunakan adalah dalam G, sedangkan dalam $\phi(a)\phi(b)$ operasi biner yang digunakan dalam G'. ✓

Contoh 3.2.2 Dalam Contoh 3.2.1, pemetaan h adalah homomorpisma. Sedangkan f dan g bukan. Juga perlu diperhatikan bahwa selain $h(x + y) = h(x) + h(y)$ didapat $h(0) = 0$ dan $h(-x) = -h(x)$. ●

Contoh 3.2.3 Pemetaan $\phi : \mathbb{Z} \to \mathbb{Z}$ yang diberikan oleh $\phi(x) = 5x$, $\forall x \in \mathbb{Z}$ adalah suatu homomorpisma, sebab

$$\phi(x + y) = 5(x + y) = 5x + 5y = \phi(x) + \phi(y), \text{ untuk semua } x, y \in \mathbb{Z}.$$ ●

Contoh 3.2.4 Pemetaan $\phi : \mathbb{R}^* \to \mathbb{Z}_2$ diberikan oleh

$$\phi(x) = \begin{cases} [0]_2, & \text{bila } x > 0 \\ [1]_2, & \text{bila } x < 0, \end{cases}$$

adalah suatu homomorpisma. Sebab, bila x dan y keduanya positip, maka xy adalah positip, didapat $\phi(xy) = [0]_2 = [0]_2 + [0]_2 = \phi(x) + \phi(y)$. Juga bila x dan y keduanya negatif, maka xy positip, didapat $\phi(xy) = [0]_2 = [1]_2 + [1]_2 = f(x) + f(y)$. Juga, bila x positip dan y negatif, maka xy negatip, didapat $\phi(xy) = [1]_2 = [0]_2 + [1]_2 = \phi(x) + \phi(y)$. Dengan cara yang sama bila x negatip dan y positip, maka hasil xy negatip, sehingga didapat $\phi(xy) = [1]_2 = [1]_2 + [0]_2 = \phi(x) + \phi(y)$. ●

Contoh 3.2.5 Untuksebarang grup G, pemetaan identitas adalah suatu homomorpisma. Sebab bila $\phi : G \to G$ adalah pemetaan identitas maka $\phi(x) = x, \forall x \in G$ dan $\phi(xy) = xy = \phi(x)\phi(y)$. ●

Contoh 3.2.6 Untuk sebarang grup G dan G',pemetaan $\phi : G \to G'$ diberikan oleh $\phi(x) = e',\ \forall x \in G$ dimana e' adalah elemen netral di G'. Maka ϕ adalah suatu homomorpisma yang dinamakan **trivial** homomorpisma diantara G dan G'. Untuk $x, y \in G$ didapat $\phi(xy) = e' = e'e' = \phi(x)\phi(y)$.

Contoh 3.2.7 Untuk sebarang grup G dan sebarang $a \in G$ diberikan pemetaan $\phi : \mathbb{Z} \to \langle a \rangle$ yang dinamakan **pemetaan eksponensial** oleh $\phi(n) = a^n,\ \forall n \in \mathbb{Z}$. Maka ϕ adalah homomorpisma, sebab $\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\phi(n)$.

Contoh 3.2.8 Misalkan $\phi : \mathbb{Z} \to \mathbb{Z}_5$ didefinisikan oleh $\phi(n) = [n]_5,\ \forall n \in \mathbb{Z}$. Jadi $\phi(7) = [2]_5, \phi(8) = [3]_5$ dan $\phi(7+8) = \phi(15) = [0]_5$ juga $\phi(7)+\phi(8) = [2]_5+[3]_5 = [5]_5 = [0]_5$. Misalkan sebarang $m, n \in \mathbb{Z}$, maka gunakan algoritma pembagian didapat $n = 5q_1 + r_1,\ 0 \le r_1 < 5$ dan $m = 5q_2 + r_2,\ 0 \le r_2 < 5$ untuk beberapa $q_1, q_2 \in \mathbb{Z}$. Sehingga didapat

$$\begin{aligned} \phi(m+n) &= \phi(5q_1 + r_1 + 5q_2 + r_2) \\ &= \phi(5(q_1+q_2) + (r_1+r_2)) \\ &= [r_1 + r_2]_5 \\ &= [r_1]_5 + [r_2]_5 \\ &= \phi(m) + \phi(n). \end{aligned}$$

Jadi ϕ adalah suatu homomorpisma.

Proposisi 3.2.1 Untuk sebarang grup G, G' dan G'', diberikan pemetaan $\phi : G \to G'$ dan $\psi : G' \to G''$ keduanya adalah homomorpisma. Maka komposisi $\psi \circ \phi(x) = \psi(\phi(x))$ adalah suatu homomorpisma grup dari G ke G''.

Bukti Misalkan sebarang $x, y \in G$ didapat

$$\begin{aligned} \psi \circ \phi(xy) &= \psi(\phi(xy)) \\ &= \psi(\phi(x)\phi(y)) \\ &= \psi(\phi(x))\psi(\phi(y)) \\ &= \psi \circ \phi(x)\, \psi \circ \phi(y). \end{aligned}$$

Suatu homomorpisma $\phi : G \to G'$ menentukan suatu subgrup khusus dari grup G yang sangat berperan penting untuk pemahaman homomorpisma.

Definisi 3.2.2 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma dan e' adalah elemen netral di G', maka **kernel** dari ϕ dinotasikan oleh $\ker(\phi)$ adalah himpunan

$$\ker(\phi) = \{x \in G \mid \phi(x) = e'\}.$$

Contoh 3.2.9 Kernel dari $\phi : \mathbb{Z} \to \mathbb{Z}_5$ dalam Contoh 3.2.8 adalah $\ker(\phi) = 5\mathbb{Z}$.

Contoh 3.2.10 Kernel $\phi : \mathbb{Z} \to \langle a \rangle$ dalam Contoh 3.2.7 adalah

$$\ker(\phi) = \{n \in \mathbb{Z} \mid |a| \text{ membagi } n\}.$$

Contoh 3.2.11 Kernel dari $\phi : \mathbb{R}^* \to \mathbb{Z}_2$ dalam Contoh 3.2.4 adalah

$$\ker(\phi) = \{x \in \mathbb{R}^* \mid x > 0\}.$$

Sifat dasar homomorpisma berikut bukanlah suatu hal yang mengejutkan sebab dari beberapa contoh yang telah dibahas menjelaskan hal ini.

Proposisi 3.2.2 (**Sifat-sifat Dasar Homomorpisma Grup**) Misalkan $\phi : G \to G'$ adalah suatu homomorpisma grup. Maka

(1) $\phi(e) = e'$, dimana e elemen netral di G dan e' elemen netral di G'.

(2) $\phi(a^{-1}) = (\phi(a))^{-1}$ untuk sebarang $a \in G$.

(3) $\phi(a^n) = \phi(a)^n$ untuk sebarang $n \in \mathbb{Z}$.

(4) Bila $|a|$ berhingga, maka $|\phi(a)|$ membagi $|a|$.

(5) Bila H adalah suatu subgrup dari G, maka $\phi(H) = \{\phi(x) \,|\, x \in H\}$ adalah suatu subgrup dari G'.

(6) Bila K adalah suatu subgrup dari G', maka $\phi^{-1}(K) = \{x \in G \,|\, \phi(x) \in K\}$ adalah subgrup dari G.

Bukti

(1) Karena $\phi(e)\cancel{\phi(e)} = \phi(e\,e) = \phi(e) = e'\cancel{\phi(e)}$, gunakan hukum kanselasi didapat $\phi(e) = e'$.

(2) Karena $\cancel{\phi(a)}\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e' = \cancel{\phi(a)}(\phi(a))^{-1}$, gunakan hukum kanselasi didapat $\phi(a^{-1}) = (\phi(a))^{-1}$.

(3) $\phi(a^n) = \phi(a)^n$ untuk $n = 0$ mengikuti hasil (1). Untuk $n > 0$ digunakan induksi: untuk $n = 1$ didapat $\phi(a) = \phi(a)$. Misalkan benar untuk bilangan bulat positip k, maka

$$\phi(a^{k+1}) = \phi(a^k a) = \phi(a^k)\phi(a) = \phi(a)^k\phi(a) = \phi(a)^{k+1}.$$

Dengan demikian untuk $n > 0$ benar bahwa $\phi(a^n) = \phi(a)^n$. Selanjutnya, untuk $n < 0$ maka $-n > 0$. Didapat

$$\phi((a^{-1})^n) = \phi(a^{-n}) = \phi(a)^{-n} = (\phi(a)^{-1})^n = \phi(a^{-1})^n.$$

Terlihat bahwa untuk $n < 0$ benar bahwa $\phi(a^n) = \phi(a)^n$.

(4) Misalkan $|a| = n$, maka menggunakan hasil (3) dan (1) didapat

$$\phi(a)^n = \phi(a^n) = \phi(e) = e'.$$

Selanjutnya dengan menggunakan Akibat 2.3.1 didapat $|\phi(a)|$ membagi $|a| = n$.

(5) Diberikan sebarang $u, v \in \phi(H) = \{w \in G' \,|\, w = \phi(x)$ untuk beberapa $x \in H\}$, pilih $x, y \in H$ yang memenuhi $u = \phi(x)$ dan $v = \phi(y)$. Maka $xy^{-1} \in H$ sebab H subgrup dan

$$uv^{-1} = \phi(x)\phi(y)^{-1} = \phi(x)\phi(y^{-1}) = \phi(xy^{-1}) \in \phi(H) \;\; (\text{sebab } xy^{-1} \in H).$$

Jadi $\phi(H)$ adalah subgrup dari G'.

(6) Misalkan $x, y \in \phi^{-1}(K)$, didapat

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(x)\phi(y)^{-1} \in K.$$

Terlihat bahwa $xy^{-1} \in \phi^{-1}(K)$, jadi $\phi^{-1}(K)$ adalah subgrup dari G.

Proposisi 3.2.3 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma grup. Maka $\ker(\phi)$ adalah suatu subgrup dari G.

Bukti Himpunan $K = \{e'\}$ dimana e' adalah elemen netral di G' adalah subgrup dari G', maka menurut menurut Proposisi 3.2.2 bagian (6) $\phi^{-1}(K)$ adalah subgrup dari G. Tetapi

$$\phi^{-1}(K) = \{x \in G \,|\, \phi(x) \in K\} = \{x \in G \,|\, \phi(x) = e'\} = \ker(\phi).$$

Dengan demikian $\ker(\phi)$ adalah subgrup dari G.

Proposisi 3.2.4 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma grup. Maka ϕ adalah satu-satu bila dan hanya bila $\ker(\phi) = \{e\}$, dimana e adalah elemen netral di G.

Bukti ($\Rightarrow$) Misalkan ϕ satu-satu dan sebarang elemen $x \in \ker(\phi)$. Maka $\phi(x) = e' = \phi(e)$. Jadi $x = e$, dengan demikian $\ker(\phi) = \{e\}$. ($\Leftarrow$) Misalkan $\ker(\phi) = \{e\}$ dan untuk beberapa $x, y \in G$ bila $\phi(x) = \phi(y)$. Maka

$$\phi(xy^{-1}) = \phi(x)\phi(y^{-1}) = \phi(y)\phi(y)^{-1} = e'.$$

Terlihat bahwa $xy^{-1} \in \ker(\phi) = \{e\}$. Jadi $xy^{-1} = e$ atau $x = y$. Dengan demikian ϕ adalah satu-satu.

Definisi 3.2.3 Suatu homomorpisma grup $\phi : G \to G'$ dimana ϕ adalah satu-satu dan pada dinamakan suatu **isomorpisma**. Dalam hal ini G dan G' adalah **isomorpik** dan ditulis $G \cong G'$.

Untuk menunjukkan bahwa dua grup G dan G' isomorpik, diperlukan empat hal:

(1) definisikan suatu pemetaan $\phi : G \to G'$.

(2) Tunjukkan bahwa ϕ adalah suatu homomorpisma grup.

(3) Tunjukkan bahwa ϕ satu-satu.

(4) Tunjukkan bahwa ϕ adalah pada.

Contoh berikut mengilustrasikan empat langkah tersebut.

Contoh 3.2.12 Grup $\mathbb{Z}$ dan $3\mathbb{Z}$ adalah isomorpik. Untuk menunjukkan hal ini, digunakan empat langkah berikut:

(1) definisikan pemetaan $\phi : \mathbb{Z} \to 3\mathbb{Z}$ oleh $\phi(x) = 3x, \ \forall x \in \mathbb{Z}$.

(2) Didapat, untuk sebarang $x, y \in \mathbb{Z}$, maka $\phi(x + y) = 3(x + y) = 3x + 3y = \phi(x) + \phi(y)$. Jadi ϕ adalah homomorpisma grup.

(3) $\phi(x) = 0$ bila dan hanya bila $3x = 0$ bila dan hanya bila $x = 0$. Jadi $\ker(\phi) = \{0\}$, dengan demikian ϕ adalah satu-satu.

(4) Diberikan sebarang $u \in 3\mathbb{Z}$ dapat dipilih $x \in \mathbb{Z}$ yang memenuhi $u = 3x$. Jadi $u = \phi(x)$, dengan demikian ϕ adalah pada.

Jadi $\mathbb{Z} \cong 3\mathbb{Z}$. ●

Contoh 3.2.13 Diberikan grup $\mathbb{R}$ dengan operasi biner penjumlahan dan grup

$$R^+ = \{x \in \mathbb{R} \mid x > 0\}$$

dengan operasi biner perkalian. Maka $\mathbb{R}$ dan $\mathbb{R}^+$ adalah isomorpik, sebab

(1) Misalkan $\phi : \mathbb{R} \to \mathbb{R}^+$ adalah fungsi yang diberikan oleh $\phi(x) = \exp(x) = e^x$, $\forall x \in \mathbb{R}$.

(2) $\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$, $\forall x, y \in \mathbb{R}$. Jadi ϕ adalah homomorpisma grup.

(3) Elemen netral di $\mathbb{R}$ adalah 1. Jadi bila sebarang elemen $x \in \ker(\phi)$, maka $\phi(x) = e^x = 1$. Hal ini berkibat $x = 0$. Dengan demikian $\ker(\phi) = \{0\}$. Jadi ϕ satu-satu.

(4) Diberikan sebarang $u \in \mathbb{R}^+$, pilih $x \in \mathbb{R}$ dimana $x = \ln(u)$. Didapat $u = e^x = \phi(x)$, dengan demikian ϕ adalah pada.

Jadi $\mathbb{R} \cong \mathbb{R}^+$. ●

Contoh 3.2.14 Dalam Contoh 3.2.12, pemetaan $\phi^{-1} : 3\mathbb{Z} \to \mathbb{Z}$ dimana

$$\phi^{-1}(u) = u/3, \ \forall u \in 3\mathbb{Z}$$

adalah suatu isomorpisma dari $3\mathbb{Z}$ ke $\mathbb{Z}$. Begitu juga dalam Contoh 3.2.13, pemetaan

$$\phi^{-1} : \mathbb{R}^+ \to \mathbb{R},$$

dimana $\phi^{-1}(u) = \ln(u)$, $\forall u \in \mathbb{R}^+$ adalah suatu isomorpisma grup dari $\mathbb{R}^+$ ke $\mathbb{R}$. ●

Proposisi 3.2.5 Misalkan $\phi : G \to G'$ dan $\psi : G' \to G''$ adalah isomorpisma. Maka

(1) Komposisi $\psi \circ \phi : G \to G''$ adalah isomorpisma.

(2) Pemetaan identitas $\phi : G \to G$ adalah isomorpisma

(3) Invers $\phi^{-1} : G' \to G$ adalah isomorpisma.

Bukti

(1) Dengan menggunakan Proposisi 3.2.1, maka komposisi $\psi \circ \phi$ adalah homomorpisma. Juga, dengan menggunakan Teorema 1.1.2 bagian (2) dan (3), maka komposisi $\psi \circ \phi$ adalah satu-satu dan pada. Jadi komposisi $\psi \circ \phi$ adalah isomorpisma grup dari G ke G''.

(2) Berdasarkan Proposisi 1.1.2 pemetaan identitas ϕ adalah satu-satu dan pada. Untuk sebarang $x, y \in G$ didapat $\phi(xy) = xy = \phi(x)\phi(y)$. Jadi ϕ adalah homomorpisma. Dengan demikian pemetaan identitas ϕ adalah isomorpisma.

(3) Karena ϕ satu-satu dan pada, maka diberikan sebarang $u, v \in G'$ dapat dipilih dengan tunggal $x, y \in G$ yang memenuhi $u = \phi(x)$ dan $v = \phi(y)$. Didapat $\phi^{-1}(u) = x$ dan $\phi^{-1}(v) = y$ juga $uv = \phi(x)\phi(y) = \phi(xy)$. Hal ini berakibat

$$\phi^{-1}(uv) = \phi^{-1}(\phi(xy)) = (\phi^{-1} \circ \phi)(xy) = xy = \phi^{-1}(u)\phi^{-1}(v).$$

Terlihat bahwa ϕ^{-1} adalah suatu homomorpisma dari G' ke G. Lagi, karena ϕ satu-satu dan pada, maka diberikan sebarang $x \in G$ dapat dipilih dengan tunggal $u \in G'$ yang memenuhi $u = \phi(x)$ sehingga didapat $\phi^{-1}(u) = x$. Jadi ϕ^{-1} adalah pemetaan satu-satu dan pada.

Proposisi 3.2.6 Misalkan $G \cong G'$. Maka

(1) $|a| = |\phi(a)|$ untuk sebarang $a \in G$ dan ϕ adalah suatu isomorpisma grup dari G ke G'.

(2) $|G| = |G'|$.

(3) G komutatif bila dan hanya bila G' komutatif.

(4) G siklik bila dan hanya bila G' siklik.

(5) G mempunyai k elemen yang berorder n bila dan hanya bila G' mempunyai k elemen yang berorder n.

Bukti Misalkan $\phi : G \to G'$ adalah suatu isomorpisma grup dari G ke G'.

(1) Misalkan sebarang elemen $a \in G$ dimana $|a| = n$ dan $|\phi(a)| = m$, maka dengan menggunakan Proposisi 3.2.2 bagian (4) didapat $|\phi(a)| = m$ membagi $|a| = n$. Dengan demikian

$$n = k_1 m, \text{ untuk beberapa bilangan bulat positip } k_1. \tag{3.1}$$

Tetapi, karena $\phi(a^m) = \phi(a)^m = e'$ dengan e' adalah elemen netral di G' dan kerana ϕ satu-satu, maka haruslah $a^m = e$. Dengan demikian $|a| = n$ membagi m. Didapat

$$m = k_2 n, \text{ untuk beberapa bilangan bulat positip } k_2. \tag{3.2}$$

Dari Persamaan 3.1 dan 3.2 didapat

$$n = k_1 m = k_1(k_2 n) = (k_1 k_2) n,$$

hal ini berakibat $1 = k_1 k_2$. Tetapi k_1 dan k_2 keduanya adalah bilangan bulat positip, jadi haruslah $k_1 = k_2 = 1$. Dengan demikian $n = k_1 m = m$ atau $|a| = |\phi(a)|$.

(2) Karena ϕ adalah satu-satu dan pada, maka $|G| = |G'|$.

(3) Misalkan G komutatif dan sebarang elemen $u, v \in G'$. Karena ϕ pada, maka dapat dipilih $x, y \in G$ yang memenuhi $\phi(x) = u$ dan $\phi(y) = v$. Maka didapat

$$uv = \phi(x)\phi(y) = \phi(xy) = \phi(yx) = \phi(y)\phi(x) = vu.$$

Jadi G' adalah komutatif. Bila G' komutatif, maka

$$\phi(xy) = \phi(x)\phi(y) = \phi(y)\phi(x) = \phi(yx),$$

karena ϕ satu-satu, maka haruslah $xy = yx$. Jadi G komutatif.

(4) Bila $G = \langle a \rangle$ siklik, maka dari hasil (1) didapat

$$|\phi(a)| = |a| = |G| = |G'|,$$

jadi $G' = \left\langle \phi(a) \right\rangle$ adalah siklik. Sebaliknya bila $G' = \langle b \rangle$ siklik dan karena ϕ pada, maka dapat dipilih elemen $a \in G$ yang memenuhi $\phi(a) = b$. Didapat

$$|a| = |\phi(a)| = |b| = |G'| = |G|$$

dan akibatnya $\langle a \rangle = G$, dengan demikian G adalah siklik.

(5) Misalkan $a_1, a_2, \ldots, a_k$ elemen-elemen yang berbeda di G dengan order n. Karena ϕ satu-satu, maka $\phi(a_1), \phi(a_2), \ldots, \phi(a_k)$ adalah elemen-elemen berbeda di G' dan dari hasil (1) elemen-elemen tersebut mempunyai order n. Bila $a_1, a_2, \ldots, a_k$ adalah semua elemen di G dengan order n, maka $\phi(a_1), \phi(a_2), \ldots, \phi(a_k)$ adalah semua elemen di G' dengan order n. Selanjutnya, untuk sebarang elemen yang lain $u \in G'$, karena ϕ pada, maka dapat dipilih $x \in G$ yang memenuhi $u = \phi(x)$ dan tentunya u berbeda dengan semua $\phi(a_i)$. Juga, x berbeda dengan semua a_i. Karena a_i adalah semua elemen di G dengan order n, didapat

$$|u| = |\phi(x)| = |x| \neq n. \qquad \checkmark$$

Lemma 3.2.1 Misalkan G dan H adalah grup siklik dengan order yang sama yaitu n, dan misalkan sebarang elemen generator $a \in G$ dan sebarang generator $b \in H$. Maka ada suatu isomorpisma $\phi : G \to H$ dengan $\phi(a) = b$.

Bukti Diketahui $G = \langle a \rangle$ dan $|G| = n$, gunakan Akibat 2.3.2 didapat

$$G = \langle a \rangle = \{e, a, a^2, \cdots, a^{n-1}\},$$

dimana semua elemen-elemen a^i adalah berbeda. Didefinisikan pemetaan $\phi : G \to H$ oleh $\phi(a^i) = b^i$ untuk $0 \leq i < n$, maka untuk sebarang a^{i_0}, a^{i_1} di G dimana $0 \leq i_0, i_1 < n$ didapat

$$\begin{aligned}
\phi(a^{i_0}a^{i_1}) &= \phi(a^{[i_0]_n}a^{[i_1]_n}) \\
&= \phi(a^{[i_0+i_1]_n}) \\
&= b^{[i_0+i_1]_n} \\
&= b^{[i_0]_n+[i_1]_n} \\
&= b^{[i_0]_n}b^{[i_1]_n} \\
&= b^{i_0}b^{i_1} \\
&= \phi(a^{i_0})\phi(a^{i_1}).
\end{aligned}$$

Jadi ϕ adalah homomorpisma grup dari G ke H. Selanjutnya misalkan sebarang elemen $a^j \in \ker(\phi)$ dimana $0 \leq j < n$, didapat

$$\phi(a^j) = b^j = e_H = b^0,$$

hal ini berkibat bahwa $j = 0$. Jadi $a^j = a^0 = e_G$. Dengan demikian $\ker(\phi) = \{e_G\}$, gunakan Proposisi 3.2.4 didapat ϕ adalah satu-satu dan kerena $|G| = n = |H|$, maka ϕ pada. Jadi ϕ adalah isomorpisma grup dari G ke H. $\checkmark$

Proposisi 3.2.7 Misalkan $G = \langle a \rangle$ adalah suatu grup siklik. Maka

(1) Bila $|G| = \infty$, maka $G \cong \mathbb{Z}$.

(2) Bila $|G| = n$, maka $G \cong \mathbb{Z}_n$.

Bukti

(1) Bila $G = \langle a \rangle$ dimana $|G| = \infty$, misalkan $\phi : \mathbb{Z} \to G$ didefinisikan oleh $\phi(k) = a^k$, $\forall k \in \mathbb{Z}$. Karena $|a| = \infty$, $a^k = e$ bila dan hanya bila $k = 0$. Jadi $\ker(\phi) = \{0\}$, dengan demikian ϕ satu-satu. Karena G siklik, diberikan sebarang $u \in G$, dapat dipilih $k \in \mathbb{Z}$ yang memenuhi $u = a^k = \phi(k)$. Jadi ϕ adalah pada. Dengan demikian ϕ adalah homomorpisma dari $\mathbb{Z}$ ke G. Tetapi, dengan menggunakan Proposisi 3.2.5 bagian (3), maka ϕ^{-1} adalah isomorpisma dari G ke $\mathbb{Z}$. Jadi $G \cong \mathbb{Z}$.

(2) Langsung gunakan Lemma 3.2.1 didapat $G \cong \mathbb{Z}_n$. ✓

Contoh 3.2.15 D_4 dan $\mathbb{Z}_8$ tidak isomorpik, sebab D_4 bukan grup komutatif, sedangkan $\mathbb{Z}_8$ grup komutatif.

Contoh 3.2.16 Diberikan grup

$$\mathbb{U}(10) = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}$$

dan

$$\mathbb{U}(12) = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\},$$

maka $\mathbb{U}(10)$ dan $\mathbb{U}(12)$ tidak isomorpik sebab $\mathbb{U}(10)$ siklik dan $\mathbb{U}(12)$ tidak siklik.

Contoh 3.2.17 Grup $\mathbb{Q}$ dengan operasi biner penjumlahan dan grup $\mathbb{Q}^*$ dengan operasi biner perkalian tidak isomorpik. Sebab, bila ada suatu isomorpisma $\phi : \mathbb{Q} \to \mathbb{Q}^*$, karena ϕ pada, maka diberikan $2 \in \mathbb{Q}^*$ dapat $a \in \mathbb{Q}$ yang memenuhi $\phi(a) = 2$. Perhatikan bilangan rasional $r = \phi(a/2)$ dan menggunakan ϕ adalah homomorpisma didapat

$$r^2 = \phi(a/2)\phi(a/2) = \phi(a/2 + a/2) = \phi(a) = 2.$$

Suatu hal yang tidak mungkin, sebab bila mungkin berakibat bahwa $r = \pm\sqrt{2}$ adalah irasional.

Sebelum mengakhiri bagian ini diberikan suatu teorema yang penting. Penemuan Arthur Cayley sekitar 100 tahun yang lalu tentang keisomorpikan sebarang grup memberikan hasil berikut.

Teorema 3.2.1 Setiap grup dengan order hingga isomorpik dengan suatu grup permutasi.

Bukti
Misalkan G suatu grup dengan order hingga. Untuk sebarang $g \in G$ tetap didefinisikan fungsi

$$f_g : G \to G \quad \text{oleh} \quad f_g(a) = ga, \forall a \in G.$$

Pemetaan f_g adalah satu-satu, sebab untuk sebarang $f_g(b), f_g(c) \in G$ (kodomain) dengan $f_g(b) = f_g(c)$, maka $gb = gc$ atau $b = c$. Juga, pemetan f_g pada sebab untuk sebarang

$y \in G$ (kodomain) selalu bisa dipilih $x = g^{-1}y \in G$ (domain) yang memenuhi $f_g(x) = g(g^{-1}y) = (gg^{-1})y = ey = y$. Jadi f_g adalah suatu permutasi dari G. Selanjutnya didefinisikan $\bar{G} \stackrel{\text{def}}{=} \{f_g \mid g \in G\}$. Bila komposisi di $\bar{G}$ didefinisikan oleh $f_a f_b \stackrel{\text{def}}{=} f_{ab}, \forall a, b \in G$, jelas bahwa dengan operasi biner komposisi tsb. $\bar{G}$ adalah suatu grup. Selanjutnya buat suatu pemetaan $\phi : G \to \bar{G}$ dengan $\phi(x) \stackrel{\text{def}}{=} f_x, \forall x \in G$. Didapat

$$\phi(xy) = f_{xy} = f_x f_y = \phi(x)\phi(y), \forall x, y \in G.$$

Jadi ϕ adalah suatu homomorpisma grup. Selanjutnya, bila diberikan sebarang $f_g \in \bar{G}$, selalu dapat dipilih $g \in G$ yang memenuhi $\phi(g) = f_g$. Jadi ϕ adalah pemetaan pada. Juga, bila $\phi(a) = \phi(b)$ didapat $f_a = f_b$ atau $f_a(x) = f_b(x), \forall x \in G$,jadi $ax = bx$ atau $a = b$. Terlihat bahwa ϕ satu-satu. Pemetaan ϕ adalah homomorpisma dan satu-satu pada (bijektif), jadi ϕ adalah suatu isomorpisma grup dari G ke $\bar{G}$, dengan demikian $G \cong \bar{G}$. ✓

Teorema 3.2.1 yang baru saja dibahas akan dibahas lagi tetapi pembuktian digunakan dengan pengertian tindakan suatu grup.

Latihan

Latihan 3.2.1 Pada latihan berikut tentukan apakah pemetaan ϕ adalah homomorpisma atau tidak. Bila ϕ homomorpisma maka tentukan ker(ϕ).

1. $\phi : \mathbb{Z} \to \mathbb{Z}$, dimana $\phi(n) = n - 1, \ \forall n \in \mathbb{Z}$.
2. $\phi : \mathbb{Z} \to \mathbb{Z}$, dimana $\phi(n) = 3n, \ \forall n \in \mathbb{Z}$.
3. $\phi : \mathbb{R}^* \to \mathbb{R}^*$ (terhadap operasi perkalian), dimana $\phi(x) = |x|, \ \forall x \in \mathbb{R}^*$.
4. $\phi : \mathrm{GL}(2, \mathbb{R}) \to \mathbb{R}^*$, dimana $\mathrm{GL}(2, \mathbb{R})$ adalah grup linier umum matriks ukuran 2×2 yang mempunyai invers dan $\phi(A) = \det(A), \ \forall A \in \mathrm{GL}(2, \mathbb{R})$.
5. $\phi : S_3 \to \mathbb{Z}_2$, dimana
$$\phi(\sigma) = \begin{cases} [0]_2, & \text{bila } \sigma \text{ permutasi genap} \\ [1]_2, & \text{bila } \sigma \text{ permutasi ganjil.} \end{cases}$$
6. $\phi : D_4 \to \mathbb{Z}_4$, dimana
$$D_4 = \{\rho_0, \rho, \rho^2, \rho^3, \tau, \rho\tau, \rho^2\tau, \rho^3\tau\}$$
adalah dihedral grup dan $\phi(\rho^i) = 0, \phi(\rho^i\tau) = 1, \ \text{untuk semua } i, 0 \le i \le 3$.
7. $\phi : \mathbb{R} \to \mathrm{GL}(2, \mathbb{R})$, $\mathbb{R}$ adalah grup himpunan bilangan riil dengan operasi penjumlahan dan
$$\phi(x) = \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}, \ \forall x \in \mathbb{R}.$$
8. $\phi : G \to G$, dimana G adalah sebarang grup dan $\phi(x) = x^{-1}, \ \forall x \in G$.
9. $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2$, dimana $\phi([x]_6) = [x]_2, \ \forall [x]_6 \in \mathbb{Z}_6$.

10. $\phi : \mathbb{Z}_7 \to \mathbb{Z}_2$, dimana $\phi([x]_7) = [x]_2,\ \forall [x]_7 \in \mathbb{Z}_7$.

Latihan 3.2.2 Hitung nilai homomorpisma ϕ berikut:

1. $\phi(27)$ dimana $\phi : \mathbb{Z} \to \mathbb{Z}_5$, dengan $\phi(n) = [n]_5,\ \forall n \in \mathbb{Z}$.
2. $\phi(27)$ dimana $\phi : \mathbb{Z} \to \mathbb{Z}_3$, dengan $\phi(m) = [m]_3,\ \forall m \in \mathbb{Z}$.
3. $\phi((1\ 2)(2\ 3\ 1)(2\ 3))$ dimana $\phi : S_3 \to \mathbb{Z}_2$ dan ϕ didefinisikan oleh $\phi(\tau) = [0]_2$ bila τ permutasi genap dan $\phi(\tau) = [1]_2$ bila τ permutasi ganjil.
4. $\phi(5)$ dan $\phi(10)$ dimana $\phi : \mathbb{Z}_{15} \to \mathbb{Z}_3$, dengan $\phi(1) = 2$.

Latihan 3.2.3 Dapatkan semua homomorpisma yang mungkin dari $\mathbb{Z}$ ke $\mathbb{Z}$.

Latihan 3.2.4 Dapatkan semua homomorpisma yang mungkin dari $\mathbb{Z}$ pada $\mathbb{Z}$.

Latihan 3.2.5 Dapatkan semua homomorpisma yang mungkin dari $\mathbb{Z}_3$ ke $\mathbb{Z}_6$.

Latihan 3.2.6 Diberikan suatu relasi $\mathcal{R}$ pada klas dari semua grup didefinisikan oleh $G\mathcal{R}G'$ bila dan hanya bila G dan G' isomorpik. Tunjukkan bahwa $\mathcal{R}$ adalah relasi ekivalen.

Latihan 3.2.7 Konstruksi suatu contoh dari suatu homomorpisma taktrivial diantara dua grup berikut bila hal ini mungkin, bila tidak mengapa hal ini tidak mungkin.

1. $\phi : S_3 \to S_5$.
2. $\phi : \mathbb{Z}_3 \to \mathbb{Z}_5$.
3. $\phi : \mathbb{Z}_4 \to \mathbb{Z}_{12}$.
4. $\phi : \mathbb{Z}_5 \to \mathbb{Z}_{12}$.
5. $\phi : D_4 \to S_5$.
6. $\phi : \mathbb{Z} \to \mathbb{Z}_7$.
7. $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_8$.
8. $\phi : S_5 \to \mathbb{Z}_2$.

Latihan 3.2.8 Misalkan $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_3$ adalah suatu homomorpisma dengan

$$\ker(\phi) = \{[0]_{12}, [3]_3, [6]_{12}, [9]_{12}\}$$

dan $\phi([4]_{12}) = [2]_3$. Dapatkan semua $x \in \mathbb{Z}_{12}$ yang memenuhi $\phi(x) = [1]_3$, dan tunjukkan bahwa himpunan $\{x \in \mathbb{Z}\}_{12} \,|\, \phi(x) = [1]_3\}$ suatu koset dari $\ker(\phi)$ dalam $\mathbb{Z}_{12}$.

Latihan 3.2.9 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma dimana $|G| = 9$. Dapatkan $|\ker(\phi)|$ bila ϕ adalah:
(a) trivial (b) satu-satu (c) bukan keduanya.

Latihan 3.2.10 Diberikan suatu grup G, $a \in G$ dan $\phi : \mathbb{Z} \to G$ adalah homomorpisma yang diberikan oleh $\phi(n) = a^n,\ \forall n \in \mathbb{Z}$. Uraikan semua $\ker(\phi)$ yang mungkin.

Latihan 3.2.11 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma dimana $\ker(\phi) = K$ dan $a \in G$. Tunjukkan bahwa

$$\{x \in G \mid \phi(x) = \phi(a)\} = aK.$$

Latihan 3.2.12 Tentukan apakah pemetaan ϕ berikut adalah isomorpisma, terangkan jawaban saudara.
(a) $\phi : 2\mathbb{Z} \to 3\mathbb{Z}$, dimana $\phi(2n) = 3n$ (b) $\phi : \mathbb{U}(10) \to \mathbb{Z}_4$, dimana $\phi([3]_{10}) = [3]_4$
(c) $\phi : \mathbb{U}(10) \to \mathbb{Z}_4$, dimana $\phi([3]_{10}) = [2]_4$ (d) $\phi : \mathbb{Z} \to \mathbb{Z}$, dimana $\phi(n) = 3n$.

Latihan 3.2.13 Tunjukkan bahwa $\mathbb{U}(8)$ dan $\mathbb{U}(12)$ isomorpik.

Latihan 3.2.14 Dalam $\mathbb{C}^*$, subgrup $\langle i \rangle$ isomorpik dengan $\mathbb{Z}_4$.

Latihan 3.2.15 Tunjukkan bahwa $\mathbb{Z}_4$ dan grup-4 Klein V tidak isomorpik.

Latihan 3.2.16 Tunjukkan bahwa $\mathbb{U}(14) \cong \mathbb{U}(18)$.

Latihan 3.2.17 Tunjukkan bahwa dua grup dihedral D_4 dan grup quaternion Q_8 tidak isomorpik.

Latihan 3.2.18 Dapatkan empat subgrup berbeda dari grup S_4 yang isomorpik dengan dengan S_3.

Latihan 3.2.19 Tunjukkan bahwa grup alternating A_4 memuat suatu subgrup yang isomorpik dengan grup-4 Klein V.

Latihan 3.2.20 Tunjukkan bahwa grup dihedral D_4 memuat suatu subgrup yang isomorpik dengan grup-4 Klein V.

Latihan 3.2.21 Diberikan grup $\mathrm{GL}(2, \mathbb{Z}_2)$, tunjukkan bahwa grup G isomorpik dengan grup S_3.

3.3 Subgrup Normal

Telah dibahas bahwa untuk sebarang homomorpisma $\phi : G \to G'$, kernel $\ker(\phi)$ adalah suatu subgrup dari G. Pada bagian ini ditunjukkan bahwa $\ker(\phi)$ adalah suatu subgrup dengan suatu sifat khusus yang berkaitan dengan koset-kosetnya. Pembahasan dimulai dengan subgrup khusus tersebut yang dinamakan subgrup *normal*.

Contoh 3.3.1 Diberikan pemetaan $\phi : S_3 \to \mathbb{Z}_2$, dimana

$$\phi(\sigma) = \begin{cases} 0, & \text{bila } \sigma \text{ permutasi genap} \\ 1, & \text{bila } \sigma \text{ permutasi ganjil.} \end{cases}$$

Maka $\ker(\phi) = A_3 = \{\rho_0, \rho, \rho^2\}$. Koset kiri dari A_3 adalah:
$A_3 = \{\rho_0, \rho, \rho^2\}$ $\mu_1 A_3 = \{\mu_1, \mu_1\rho, \mu_1\rho^2\} = \{\mu_1, \mu_2, \mu_3\}$.
Sedangkan koset kanan dari A_3 adalah:
$A_3 = \{\rho_0, \rho, \rho^2\}$ $A_3\mu_1 = \{\mu_1, \rho\mu_1, \rho^2\mu_1\} = \{\mu_1, \mu_3, \mu_2\}$.
Terlihat bahwa koset kiri dari A_3 sama dengan koset kanan dari A_3. Perhatikan persamaan $\mu_1 A_3 = A_3\mu_1$ tidak berarti bahwa μ_1 komutatif dengan setiap elemen-elemen dari A_3, sebab $\mu_1\rho = \mu_2 \neq \mu_3 = \rho\mu_1$.

Contoh 3.3.2 Diberikan quaternion grup $Q_8 = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$. Misalkan pemetaan $\phi : Q_8 \to \mathbb{Z}_2$ didefinisikan oleh $\phi(\pm 1) = \phi(\pm \mathbf{i}) = [0]_2$ dan $\phi(\pm \mathbf{j}) = \phi(\pm \mathbf{k}) = [1]_2$. Maka ϕ adalah suatu homomorpisma grup dengan $\ker(\phi) = K = \{\pm 1, \pm \mathbf{i}\}$. Maka koset kiri dari K adalah:
$K = \{1, -1, \mathbf{i}, -\mathbf{i}\}$ $\mathbf{j}K = \{\mathbf{j}, -\mathbf{j}, \mathbf{ji} = -\mathbf{k}, \mathbf{j}(-\mathbf{i}) = \mathbf{k}\}$
Sedangkan koset kanan dari K adalah:
$K = \{1, -1, \mathbf{i}, -\mathbf{i}\}$ $K\mathbf{j} = \{\mathbf{j}, -\mathbf{j}, \mathbf{ij} = \mathbf{k}, (-\mathbf{i})\mathbf{j} = -\mathbf{k}\}$.
Terlihat bahwa koset kiri dan kanan dari K sama. tetpai perlu diingat bahwa walaupun $\mathbf{j}K = K\mathbf{j}$ hal ini tidak berakibat $\mathbf{j}$ komutatif dengan semua elemen-elemen dari K, sebab $\mathbf{ji} = -\mathbf{k} \neq \mathbf{k} = \mathbf{ij}$.

Dua contoh yang telah dibahas mengilustrasikan suatu sifat penting kernel dari suatu homomorpisma.

Proposisi 3.3.1 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma dan $K = \ker(\phi)$. Maka untuk semua $g \in G$ didapat $gK = Kg$.

Bukti Misalkan $x \in gK$, maka $x = gk_1$ untuk beberapa $k_1 \in K$. Jadi

$$\phi(x) = \phi(gk_1) = \phi(g)\phi(k_1) = \phi(g)e' = e'\phi(g).$$

Didapat

$$e' = \phi(x)\phi(g)^{-1} = \phi(x)\phi(g^{-1}) = \phi(xg^{-1}).$$

Terlihat bahwa $xg^{-1} \in K$, misalkan $k_2 = xg^{-1}$, untuk beberapa $k_2 \in K$, didapat $x = k_2 g \in Kg$. Jadi $gK \subseteq Kg$. Dengan cara yang sejalan, misalkan $y \in Kg$, maka $y = k_0 g$ untuk beberapa $k_0 \in K$. Jadi

$$\phi(y) = \phi(k_0 g) = \phi(k_0)\phi(g) = e'\phi(g) = \phi(g)e'.$$

Didapat

$$e' = \phi(g)^{-1}\phi(y) = \phi(g^{-1})\phi(x) = \phi(g^{-1}y).$$

Terlihat bahwa $g^{-1}y \in K$, misalkan $k_1 = g^{-1}y$, untuk beberapa $k_1 \in K$, didapat $y = gk_1 \in gK$. Jadi $Kg \subseteq gK$. Karena $gK \subseteq Kg$ dan$Kg \subseteq gK$, maka $gK = Kg$.

Subgrup kernel mempunyai sifat penting sebagaimana telah dibuktikan pada proposisi yang baru saja dibahas dan berperan penting dalam memahami struktur dari grup.

Definisi 3.3.1 Diberikan grup G dan H adalah subgrup dari G. Bila untuk semua $g \in G$ berlaku $gH = Hg$, maka H dinamakan subgrup **normal** dari G dan ditulis $H \lhd G$.

Akibat 3.3.1 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma dan $K = \ker(\phi)$, maka $K \lhd G$.

Bukti Hal ini adalah akibat langsung dari Proposisi 3.3.1.

Contoh 3.3.3 Dalam Contoh 3.3.1 $A_3 \lhd S_3$ juga dalam Contoh 3.3.2 $\{\pm 1, \pm \mathbf{i}\} \lhd Q_8$.

Proposisi 3.3.2 Bila G adalah suatu grup komutatif, setiap subgrup dari G adalah subgrup normal dari G.

Bukti Langsung dari definisi 3.3.1.

Contoh 3.3.4 Karena $\mathbb{Z}$ adalah grup komutatif, maka subgrup $n\mathbb{Z} \lhd \mathbb{Z}$ untuk $n \geq 1$ begitu juga setiap subgrup dari $\mathbb{Z}_n$ adalah subgrup normal di $\mathbb{Z}_n$. ●

Contoh 3.3.5 Dalam A_4, tinjau subgrup

$$H = \{\rho_0, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Didapat $|A_4| = 12$ dan $|H| = 4$, jadi indeks $[A_4 : H] = 3$. Ada tiga koset kiri dari H, yaitu H sendiri dan

$$(1\ 2\ 3)H = \{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\}$$
$$(1\ 3\ 2)H = \{(1\ 3\ 2), (2\ 3\ 4), (1\ 2\ 4), (1\ 4\ 3)\}.$$

Juga ada tiga koset kanan dari H yaitu H sendiri dan

$$H(1\ 2\ 3) = \{(1\ 2\ 3), (2\ 4\ 3), (1\ 4\ 2), (1\ 3\ 4)\}$$
$$H(1\ 3\ 2) = \{(1\ 3\ 2), (1\ 4\ 3), (2\ 3\ 4), (1\ 2\ 4)\}.$$

Terlihat bahwa $(1\ 2\ 3)H = H(1\ 2\ 3)$ dan $(1\ 3\ 2)H = H(1\ 3\ 2)$, jadi $H \lhd A_4$. ●

Teorema berikut memberikan suatu cara untuk mengkonstruksi contoh-contoh subgrup normal.

Teorema 3.3.1 Diberikan suatu grup G dan H adalah suatu subgrup dari G dengan indeks $[G : H] = 2$. Maka H adalah subgrup normal dari G.

Bukti Karena $[G : H] = 2$, hal ini berakibat banyaknya koset kiri dan kanan adalah dua. Karena H sendiri adalah koset kiri dan sekaligus kanan dari H dan untuk sebarang $g \notin H$, maka dua koset kiri dari H yang berbeda adalah H dan gH dan dua koset kanan dari H yang berbeda adalah H dan Hg. Karena koset menentukan suatu partisi dari G, maka haruslah

$$gH = \{k \in G \,|\, k \notin H\} = Hg,$$

dengan demikian $H \lhd G$. ●

Contoh 3.3.6 Karena $[S_n : A_n] = 2$, maka subgrup alternating $A_n \lhd S_n$ untuk semua $n \geq 3$. ●

Contoh 3.3.7 Subgrup $H = \langle \rho \rangle$ dari grup dihedral D_4 mempunyai order empat, maka indeks $[D_4 : H] = 2$. Jadi $H \lhd D_4$. ●

Teorema berikut memberikan suatu cara mudah untuk membedakan suatu subgrup adalah subgrup normal atau bukan.

Teorema 3.3.2 (**Test Subgrup Normal**) Diberikan suatu grup G dan H adalah suatu subgrup dari G. Maka kondisi berikut ekivalen:

(1) $H \lhd G$,

(2) $gHg^{-1} \subseteq H$ untuk semua $g \in G$,

(3) $gHg^{-1} = H$ untuk semua $g \in G$

Bukti (1) $\Rightarrow$ (2) Misalkan $g \in G$ dan $x \in gHg^{-1}$, maka $x = ghg^{-1}$ untuk beberapa $h \in H$. Menggunakan hipotisis (1), maka $gH = Hg$. Karena $gh \in gH$ didapat $gh \in Hg$. Jadi $gh = h'g$ untuk beberapa $h' \in H$. Dengan demikian

$$x = ghg^{-1} = h'gg^{-1} = h' \in H.$$

Jadi $gHg^{-1} \subseteq H$. Selanjutnya (2) $\Rightarrow$ (3), menggunakan hipotesis (2) didapat $yHy^{-1} \subseteq H$, hal ini berakibat $H \subseteq yHy^{-1}$ untuk semua $y \in G$. Diberikan sebarang $g \in G$, misalkan $y = g^{-1}$. Maka, didapat

$$gHg^{-1} \subset H \subseteq y^{-1}Hy = gHg^{-1}.$$

Jadi $gHg^{-1} = H$. Berikutnya (3) $\Rightarrow$ (1) misalkan $g \in G$ dan $x \in gH$. Jadi $x = gh$ untuk beberapa $h \in H$. Sehingga didapat $xg^{-1} = ghg^{-1} \in gHg^{-1}$, tetapi menggunakan hipotisis (3), didapat $xg^{-1} \in H$. Akibatnya $x \in Hg$. Jadi $gH \subseteq Hg$. Dengan cara yang sejalan, bila dimulai dengan $y \in Hg$ dapat ditunjukkan $g^{-1}y \in H$. Jadi $y \in gH$, dengan demikian $gH = Hg$ untuk semua $g \in G$. Jadi $H \lhd G$. ✓

Catatan pada bagian (2) Teorema 3.3.2 pernyataan $gHg^{-1} \subseteq H$ untuk semua $g \in G$ bila dan hanya bila $ghg^{-1} \in H$ untuk semua $g \in G$ dan semua $h \in H$ bila dan hanya bila $g^{-1}h'g \in H$ untuk semua $g \in G$ dan semua $h' \in H$.

Contoh 3.3.8 Diberikan $G = \mathrm{GL}(2, \mathbb{R})$ dan $H = \mathrm{SL}(2, \mathbb{R})$. Maka $H \lhd G$, sebab bila $A \in G$ dan $B \in H$, didapat

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(A) \cdot 1 \cdot \det(A^{-1}) = \det(A)\det(A^{-1}) = 1,$$

jadi $ABA^{-1} \in H$. ●

Contoh 3.3.9 Diberikan $Z(G)$ senter dari grup G, maka $Z(G)$ subgrup normal dari G sebab elemen-elemen dari $Z(G)$ komutatif dengan semua elemen dari G. ●

Contoh 3.3.10 Dalam S_3, tinjau subgrup $H = \langle \mu_1 \rangle$. Bila dihitung $\rho H \rho^{-1}$ didapat subgrup $\langle \mu_2 \rangle$. Bila dihitung $\rho^2 H \rho^{-2}$ didapat subgrup $\langle \mu_3 \rangle$. Dalam hal ini H, $\rho H \rho^{-1}$ dan $\rho^2 H \rho^{-2}$ adalah tiga subgrup yang berbeda dari S_3 berorder dua dan ketiganya taksatupun merupakan subgrup normal. ●

Teorema 3.3.3 Misalkan H adalah subgrup dari suatu grup G. Maka untuk sebarang $g \in G$

(1) gHg^{-1} adalah subgrup dari G.

(2) $\left|gHg^{-1}\right| = |H|$.

Bukti

(1) Bila $x, y \in gHg^{-1}$, maka $x = gh_1g^{-1}$ dan $y = gh_2g^{-1}$ untuk beberapa $h_1, h_2 \in H$. Jadi

$$xy^{-1} = gh_1g^{-1}(gh_2g^{-1})^{-1} = gh_1g^{-1}gh_2^{-1}g^{-1} = gh_1h_2^{-1}g^{-1}.$$

Karena H adalah subgrup, maka $h = h_1h_2^{-1} \in H$. Jadi $xy^{-1} = ghg^{-1} \in gHg^{-1}$. Dengan demikian gHg^{-1} adalah subgrup dari G.

(2) Buat suatu pemetaan berikut

$$f : H \to gHg^{-1}$$

diberikan oleh $f(h) = ghg^{-1}$, $\forall h \in H$. Untuk $f(h_1) = f(h_2)$, didapat

$$\cancel{g} h_1 \cancel{g^{-1}} = \cancel{g} h_2 \cancel{g^{-1}},$$

dengan menggunakan hukum kanselasi kiri dan kanan didapat $h_1 = h_2$. Jadi f adalah satu-satu. Selanjutnya, diberikan sebarang $y \in gHg^{-1}$, maka $y = ghg^{-1}$ untuk beberapa $h \in H$. Hal ini berakibat $f(h) = ghg^{-1} = y$. Jadi f adalah pada, dengan demikian f satu-satu dan pada. Jadi $|H| = \left|gHg^{-1}\right|$.

Akibat 3.3.2 Misalkan H adalah suatu subgrup dari suatu grup G. Bila H adalah hanya satu-satunya subgrup dari G yang berorder $|H|$, maka $H \lhd G$.

Bukti Karena H adalah satu-satunya subgrup dari grup G dan menggunakan Teorema 3.3.3 didapat $H = gHg^{-1}$ untuk semua $g \in G$. Menurut Teorema Test Subgrup Normal maka $H \lhd G$.

Contoh 3.3.11 Dalam D_4 tinjau subgrup $H = \langle \tau \rangle = \{\rho_0, \tau\}$ dan $N = \{\rho_0, \rho^2, \tau, \rho^2\tau\}$. Karena $[N : H] = 2 = [D_4 : N]$, maka $H \lhd N$ dan $N \lhd D_4$. Tetapi, H bukan subgrup normal dari D_4. Faktanya, N adalah subgrup terbesar dari D_4 yang memuat H sebagai suatu subgrup normal.

Definisi 3.3.2 Misalkan H adalah suatu subgrup dari suatu grup G, maka

$$N_G(H) \stackrel{\text{def}}{=} \left\{g \in G \,|\, gHg^{-1} = H\right\}$$

dinamakan **normalisir** dari H dalam G.

Teorema 3.3.4 Misalkan H adalah suatu subgrup dari suatu grup G. Maka

(1) $N_G(H)$ adalah suatu subgrup dari G.

(2) $H \lhd N_G(H)$.

(3) Bila K suatu subgrup dari G dan $H \lhd K$, maka K adalah subgrup dari $N_G(H)$.

(4) $H \lhd G$ bila dan hanya bila $N_G(H) = G$.

Bukti

(1) Misalkan $a, b \in N_G(H)$, didapat $aHa^{-1} = H = bHb^{-1}$. Hal ini berakibat

$$(a^{-1}b)H(b^{-1}a) = H \quad \text{atau} \quad (a^{-1}b)H(a^{-1}b)^{-1} = H.$$

Jadi $a^{-1}b \in N_G(H)$, dengan demikian $N_G(H)$ adalah subgrup dari G.

(2) Misalkan sebarang $h \in H$, didapat $hHh^{-1} = H$. Jadi $h \in N_G(H)$ dengan demikian $H \subset N_G(H)$. Diberikan sebarang $g \in N_G(H)$, didapat $gHg^{-1} = H$ untuk semua $g \in N_G(H)$ dan menurut Teorema Test Subgrup Normal, maka $H \lhd N_G(H)$.

(3) Misalkan $H \lhd K$ dan diberikan sebarang $g \in K$, maka $gHg^{-1} = H$. Hal ini menunjukkan bahwa $g \in N_G(H)$, akibatnya $K \subset N_G(H)$. Karena K subgrup dari G dan $K \subset N_G(H)$ hal ini berakibat K adalah subgrup dari $N_G(H)$.

(4) ($\Rightarrow$) Misalkan $H \lhd G$ dan untuk sebarang $g \in G$, didapat $gHg^{-1} = H$. Jadi $g \in N_G(H)$, dengan demikian $G \subset N_G(H)$. Tetapi $N_G(H) \subset G$, jadi $N_G(H) = G$. ($\Leftarrow$) Misalkan $N_G(H) = G$, maka untuk sebarang $g \in G$ didapat $g \in N_G(H)$. Akibatnya, $gHg^{-1} = H$ untuk semua $g \in G$. Jadi $H \lhd G$. ✓

Diberikan dua subgrup H dan K dari suatu subgrup G, didefinisikan himpunan

$$HK \stackrel{\text{def}}{=} \{hk \,|\, h \in H, k \in K\}.$$

Himpunan HK mungkin subgrup dari G mungkin tidak. Proposisi berikut memberikan syarat bahwa HK adalah subgrup dari G.

Proposisi 3.3.3 Misalkan H dan K adalah subgrup dari suatu grup G dan $H \lhd G$. Maka HK adalah suatu subgrup dari G.

Bukti Misalkan $a, b \in HK$, maka $a = h_1k_1$ dan $b = h_2k_2$ untuk beberapa $h_1, h_2 \in H$ dan $k_1, k_2 \in K$. Didapat

$$ab^{-1} = h_1k_1(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1kh_2^{-1},$$

dimana $k = k_1k_2^{-1} \in K$ (sebab K subgrup). Selanjutnya, tinjau elemen kh_2^{-1}, elemen ini berada di kH. Karena $H \lhd G$, maka $kH = Hk$. Jadi $kh_2^{-1} \in Hk$, dengan demikian $kh_2^{-1} = h_3k$ untuk beberapa $h_3 \in H$. Sehingga didapat

$$ab^{-1} = h_1kh_2^{-1} = h_1h_3k = hk,$$

dimana $h = h_1h_3 \in H$ (sebab H subgrup dari G). Terlihat bahwa, $ab^{-1} \in HK$. Jadi HK adalah subgrup dari grup G. ✓

Akibat 3.3.3 Bila H dan K adalah subgrup dari suatu grup komutatif G, maka HK adalah subgrup dari G.

Bukti Karena G grup komutatif, maka $H \lhd G$. Gunakan Proposisi 3.3.3 didapat HK subgrup dari G. ✓

Teorema 3.3.5 Bila H dan K adalah subgrup berhingga dari suatu grup G, maka

$$|HK| = |H|\,|K|/|H \cap K|.$$

Bukti Misalkan m adalah indeks $[K : H \cap K]$ dan

$$(H \cap K)k_1, (H \cap K)k_2, \cdots, (H \cap K)k_m$$

adalah m koset yang berbeda dari $H \cap K$ dalam K. Koset-koset ini membentuk partisi dalam K dan setiap elemen dari K tepat berada pada satu koset tersebut. Karena

$$m = [K : H \cap K] = |K|/|H \cap K|,$$

maka tinggal menunjukkan $|HK| = |H|\,m$ sebagai berikut. Tinjau

$$Hk_1, Hk_2, \ldots, Hk_m,$$

adalah koset-koset kanan dari H yang semuanya berbeda. Sebab bila tidak, yaitu $Hk_i = Hk_j$ untuk beberapa $i \neq j$ dengan $1 \leq i, j \leq m$, maka $k_i k_j^{-1} \in H$, tetapi $k_i k_j^{-1} \in K$ (sebab K subgrup). Jadi $k_i k_j^{-1} \in (H \cap K)$. Akibatnya, $(H \cap K)k_i = (H \cap K)k_j$ dengan $i \neq j$. Hal ini bertentangan dengan kenyataan koset $(H \cap K)k_s$ dengan $1 \leq s \leq m$ semuanya berbeda. Bila diberikan sebarang elemen $hk \in HK$ dan karena $(H \cap K)k_s$ dengan $1 \leq s \leq m$ adalah koset-koset yang berbeda dari $(H \cap K)$ dalam K, maka $k \in (H \cap K)k_s$ untuk beberapa $1 \leq s \leq m$, dengan demikian hk terletak pada salah satu koset Hk_s. Jadi Hk_s mempartisi HK dan $|Hk_s| = |H|$. Sehingga didapat $|HK| = |Hk_s|\,m = |H|\,|K|/|H \cap K|$.

Latihan

Latihan 3.3.1 Tentukan apakah subgrup berikut adalah subgrup normal.

1. A_3 dalam S_3
2. A_3 dalam S_4
3. $3\mathbb{Z}$ dalam $\mathbb{Z}$
4. $\langle \rho \rangle$ dalam D_4
5. $\langle \rho\tau \rangle$ dalam D_4
6. $\{\pm 1, \pm \mathbf{j}\}$ dalam Q_8
7. $K = \{\rho_0, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ dalam S_4
8. $\langle (1\,2\,3) \rangle$ dalam S_4.

Latihan 3.3.2 Tunjukkan bahwa pemetaan $\phi : Q_8 \to \mathbb{Z}_2$ didefinisikan oleh

$$\phi(\pm 1) = \phi(\pm \mathbf{i}) = [0]_2$$

dan

$$\phi(\pm \mathbf{j}) = \phi(\pm \mathbf{k}) = [1]_2$$

adalah suatu homomorpisma.

Latihan 3.3.3 Dapatkan semua subgrup normal dalam $\mathrm{Gl}(2, \mathbb{Z})$.

Latihan 3.3.4 Dapatkan semua subgrup normal dalam D_4.

Latihan 3.3.5 Untuk $r \in \mathbb{R}^*$, misalkan $rI = \begin{bmatrix} r & 0 \\ 0 & r \end{bmatrix}$. Tunjukkan bahwa $H = \{rI \mid r \in \mathbb{R}^*\}$ adalah suatu subgrup normal dari $\mathrm{GL}(2, \mathbb{R})$.

Latihan 3.3.6 Diberikan suatu homomorpisma $\phi : G \to G'$ dan $H' \lhd G'$. Tunjukkan bahwa $H = \phi^{-1}(H') \lhd G$.

Latihan 3.3.7 Berikan suatu contoh grup G dimana dua subgrup $H \leq K \leq G$ memenuhi $H \lhd K$ dan $K \lhd G$, tetapi H bukan subgrup normal dalam G.

Latihan 3.3.8 Tunjukkan bahwa bila $H \lhd G$ dan $K \lhd G$, maka $(H \cap K) \lhd G$.

Latihan 3.3.9 Misalkan H adalah suatu subgrup dari grup G dan untuk setiap $a \in G$ ada $b \in G$ yang memenuhi $aH = Hb$. Tunjukkan bahwa $H \lhd G$.

Latihan 3.3.10 Tunjukkan bahwa bila $H \lhd G$ dan $K \lhd G$, maka $HK \lhd G$.

Latihan 3.3.11 Dapatkan normalisir dari subgrup berikut.

1. A_3 dalam S_3 2. $\langle \mu_1 \rangle$ dalam S_3 3. $\langle \tau \rangle$ dalam D_4 4. $\langle \mathbf{j} \rangle$ dalam Q_8.

Latihan 3.3.12 Misalkan H dan K adalah subgrup dari suatu grup G. Tunjukkan bahwa HK adalah suatu subgrup dari G bila dan hanya bila $HK = KH$.

Latihan 3.3.13 Misalkan G adalah suatu grup dengan order pq dimana p dan q adalah dua bilangan prima yang berbeda. Bila G mempunyai suatu subgrup tunggal berorder p dan suatu subgrup tunggal berorder q, maka tunjukkan bahwa G siklik.

Latihan 3.3.14 Misalkan G suatu grup yang mempunyai dua subgrup tunggal berorder m dan berorder n dimana $\text{fpb}(m, n) = 1$. Tunjukkan bahwa G mempunyai suatu subgrup normal berorder mn.

Latihan 3.3.15 Misalkan $K \lhd G$ dan H adalah suatu subgrup dari G. Tunjukkan bahwa $(K \cap H) \lhd H$.

3.4 Grup Kuasi

Dalam bagian sebelumnya sudah ditunjukkan bahwa bila subgrup K dari suatu grup G adalah kernel

$$\ker(\phi) = \{g \in G \mid \phi(g) = e\}$$

dari suatu homomorpisma $\phi : G \to G'$, maka $gK = Kg$ untuk semua $g \in G$ dan subgrup K dengan sifat yang demikian dinamakan subgrup normal. Dalam bagian ini dibahas image dari suatu homomorpisma. Selanjutnya ditunjukkan sebaliknya, yaitu bila K adalah suatu subgrup normal dari suatu grup G, maka K adalah kernel suatu homomorpisma ϕ dari G ke grup lainnya G'. Kenyataannya, ditunjukkan bagaimana mengkonstruksi grup G' dan homomorpisma ϕ bila diberikan grup G dan subgrup normal K dari G. Pengkonstruksian ini dinamakan pengkonstruksian grup kuasi. Grup ini sangat penting dalam pemahaman struktur dari grup.

Contoh 3.4.1 Dalam $\mathbb{Z}$ tinjau subgrup $7\mathbb{Z}$ dan himpunan dengan elemen-elemen di koset-koset dari $7\mathbb{Z}$ dalam $\mathbb{Z}$. Karena $m + 7\mathbb{Z} = n + 7\mathbb{Z}$ bila dan hanya bila $m \equiv n \mod 5$, maka himpunan dengan elemen-elemen adalah koset-koset dari $7\mathbb{Z}$ dalam $\mathbb{Z}$ adalah

$$G' = \{0 + 7\mathbb{Z}, 1 + 7\mathbb{Z}, 2 + 7\mathbb{Z}, 3 + 7\mathbb{Z}, 4 + 7\mathbb{Z}, 5 + 7\mathbb{Z}, 6 + 7\mathbb{Z}\}.$$

Ada suatu cara wajar untuk mendefinisikan suatu operasi pada G', misalnya

$$(m + 7\mathbb{Z}) + (n + 7\mathbb{Z}) = (m + n) + 7\mathbb{Z} \stackrel{\text{def}}{=} (m \boxplus_7 n) + 7\mathbb{Z},$$

dimana $m \boxplus_7 n \stackrel{\text{def}}{=} [m + n]_7$ adalah operasi penjumlahan modulo 7. Dengan operasi ini himpunan G' isomorpik dengan $\mathbb{Z}_7$ dengan koset $m+7\mathbb{Z}$ berkaitan dengan elemen $\phi(m) \in \mathbb{Z}_7$, dimana $\phi(m)$ adalah sisa dari $m \mod 7$. Elemen netral adalah $7\mathbb{Z} = 0+7\mathbb{Z}$, invers dari $2+7\mathbb{Z}$ adalah $5 + 7\mathbb{Z}$, invers dari $3 + 7\mathbb{Z}$ adalah $4 + 7\mathbb{Z}$.

Diberikan suatu subgrup H dari suatu grup G, meniru cara pengkosntruksian contoh sebelumnya dan didefinisikan suatu operasi koset dari H dalam G, yaitu $(aH)(bH) = (ab)H$. Tetapi untuk definisi mempunyai makna, atau dikatakan bahwa operasi ini terdefinisi secara baik (well defined). Maka diperluhkan bahwa bila a_1H dan a_2H adalah koset yang sama dan bila b_1H dan b_2H adalah koset yang sama, maka $(a_1b_1)H$ dan $(a_2b_2)H$ adalah koset yang sama. Dengan kata lain diperluhkan bahwa hasil operasi tidak bergantung pada elemen yang mana a_1 atau a_2 yang dipilih untuk mewakili koset yang pertama dan pada elemen yang mana b_1 atau b_2 yang dipilih untuk mewakili koset yang kedua. Lemma berikut menjelaskan kondisi apa yang dibahas ini.

Lemma 3.4.1 Misalkan H adalah suatu subgrup dari suatu grup G. Maka $H \lhd G$ bila dan hanya bila $(aH)(bH) = (ab)H$ adalah operasi pada koset dari H terdefinisi secara baik.

Bukti ($\Rightarrow$) Asumsikan $H \lhd G$ dan misalkan $a_1H = a_2H$ dan $b_1H = b_2H$. Hal ini berarti bahwa $a_1 = a_2h$ dan $b_1 = b_2h'$ untuk beberapa $h, h' \in H$. Maka

$$a_1b_1 = (a_2h)(b_2h') = a_2(hb_2)h'.$$

Karena $H \lhd G$, maka $b_2H = Hb_2$, jadi $hb_2 = b_2h''$ untuk beberapa $h'' \in H$. Sehingga didapat

$$a_1b_1 = a_2(hb_2)h' = a_2(b_2h'')h' = a_2b_2(h''h'),$$

dimana $h''h' \in H$ (sebab H subgrup). Dengan demikian $(a_1b_1)H = (a_2b_2)H$ sebagai mana yang dibutuhkan untuk menunjukkan bahwa operasi perkalian koset dari H adalah terdefinisi secara baik. ($\Leftarrow$) Asumsikan operasi perkalian koset dari H terdefinisi secara baik, misalkan sebarang $g \in G$ dan sebarang $h \in H$. Karena $gH = (gh)H$ dan operasi terdefinisi secara baik, maka untuk $ghg^{-1} \in gHg^{-1}$ didapat

$$(ghg^{-1})H = (gh)H\,g^{-1}H = gH\,g^{-1}H = (gg^{-1})H = eH = H.$$

Jadi $ghg^{-1} \in H$, dengan demikian $gHg^{-1} \subseteq H$ untuk semua $g \in G$. Gunakan test subgrup normal pada Teorema 3.3.2 didapat bahwa $H \lhd G$.

Teorema 3.4.1 Misalkan H adalah suatu sungrup normal dari grup G. Maka himpunan koset-koset dari H dalam G membentuk suatu grup terhadap operasi $(aH)(bH) = (ab)H$.

Bukti Operasi "perkalian" koset $(aH)(bH) = (ab)H$ menurut Lemma 3.4.1 terdefinisi secara baik. Sifat tertutup, didapat langsung dari "perkalian" koset $(aH)(bH)$ menghasilkan lagi suatu koset $(ab)H$. Sifat assosiatif,

$$aH(bH\,cH) = aH[(bc)H] = a(bc)H = (ab)cH = (ab)H\,cH = (aH\,bH)cH.$$

Sifat elemen netral, untuk sebarang koset aH, didapat $aH\,H = aH\,eH = (ae)H = aH$, sejalan dengan hal ini didapat $H\,aH = eH\,aH = (ea)H = aH$. Jadi $eH = H$ adalah elemen netral. Sifat invers, diberikan sebarang koset aH, didapat $aH\,a^{-1}H = (aa^{-1})H = eH = H$ juga $a^{-1}H\,aH = (a^{-1}a)H = eH = H$. Terlihat bahwa invers dari aH adalah $a^{-1}H$.

Definisi 3.4.1 Misalkan H adalah subgrup normal dari G. Maka grup himpunan koset-koset dari H dalam G dengan operasi $(aH)(bH) = (ab)H$ dinamakan **grup kuasi** dari G oleh H ditulis G/H.

Contoh 3.4.2 Sebagaimana telah dibahas dalam Contoh 3.4.1 $Z/7\mathbb{Z} \cong \mathbb{Z}_7$. Sejalan dengan ini, secara umum didapat $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. ●

Contoh 3.4.3 Dalam $\mathbb{Z}_6$, tinjau subgrup $\langle [3]_6 \rangle$. Himpunan koset dari $\langle [3]_6 \rangle$ adalah

$$\{\langle [3]_6 \rangle, [1]_6 + \langle [3]_6 \rangle, [2]_6 + \langle [3]_6 \rangle\}$$

dan $\mathbb{Z}_6/\langle [3]_6 \rangle$ adalah grup berorder 3. Grup ini isomorpik dengan $\mathbb{Z}_3$. Jadi didapat $\mathbb{Z}_6/\langle [3]_6 \rangle \cong \mathbb{Z}_3$. Catatan bahwa $[1]_6 + \langle [3]_6 \rangle$ membangun grup kuasi $\mathbb{Z}_6/\langle [3]_6 \rangle$. ●

Contoh 3.4.4 Dalam $\mathbb{Z}_{12}$, tinjau subgrup

$$\langle [8]_{12} \rangle = \{[0]_{12}, [4]_{12}, [8]_{12}\}.$$

order grup kuasi $|\mathbb{Z}_{12}/\langle [8]_{12} \rangle|$ adalah banyaknya koset dari $\langle [8]_{12} \rangle$ atau indeks dari $\langle [8]_{12} \rangle$ dalam $\mathbb{Z}_{12}$, yaitu $[\mathbb{Z}_{12} : \langle [8]_{12} \rangle] = |\mathbb{Z}_{12}/\langle [8]_{12} \rangle| = 12/3 = 4$. Setiap grup berorder 4 isomorpik dengan $\mathbb{Z}_4$ atau V grup-4 Klein. Dihitung order elemen $1+\langle [8]_{12} \rangle$ dalam $\mathbb{Z}_{12}/\langle [8]_{12} \rangle$. Didapat

$$2(1 + \langle [8]_{12} \rangle) = 2 + \langle [8]_{12} \rangle, 3(1 + \langle [8]_{12} \rangle) = 3 + \langle [8]_{12} \rangle, 4(1 + \langle [8]_{12} \rangle) = 4 + \langle [8]_{12} \rangle = \langle [8]_{12} \rangle.$$

Jadi order $|1 + \langle [8]_{12} \rangle| = 4$. Dengan demikian $|1 + \langle [8]_{12} \rangle| = |\mathbb{Z}_{12}/\langle [8]_{12} \rangle| = 4$ dan $\mathbb{Z}_{12}/\langle [8]_{12} \rangle$ adalah siklik berorder 4. Jadi $\mathbb{Z}_{12}/\langle [8]_{12} \rangle \cong \mathbb{Z}_4$. ●

Contoh 3.4.5 Dalam D_4 tinjau subgrup $\left\langle \rho^2 \right\rangle = \{\rho_0, \rho^2\}$. Karena $\rho^2 \in Z(D_4)$, senter dari D_4, maka $\left\langle \rho^2 \right\rangle$ adalah suatu subgrup normal. Indeks $[D_4 : \left\langle \rho^2 \right\rangle] = 8/2 = 4$, jadi grup kuasi $D_4/\left\langle \rho^2 \right\rangle$ mempunyai order $[D_4 : \left\langle \rho^2 \right\rangle] = 4$. Grup kuasi

$$D_4/\left\langle \rho^2 \right\rangle = \left\{\left\langle \rho^2 \right\rangle, \rho\left\langle \rho^2 \right\rangle, \tau\left\langle \rho^2 \right\rangle, \rho\tau\left\langle \rho^2 \right\rangle\right\},$$

semua elemen dari $D_4/\left\langle \rho^2 \right\rangle$ yang bukan $\left\langle \rho^2 \right\rangle$ mempunyai order 2, jadi $D_4/\left\langle \rho^2 \right\rangle \cong V$, dimana V adalah grup-4 Klein. ●

Dua contoh yang baru saja dibahas memberikan beberapa fakta penting tentang grup kuasi yang dinyatakan dalam proposisi berikut.

Proposisi 3.4.1 Misalkan H suatu subgrup normal dari suatu grup G. Maka

(1) order dari suatu elemen aH dalam G/H adalah bilangan positip terkecil k yang memenuhi $a^k \in H$.

(2) Bila G berhingga, maka $|G/H| = |G|/|H|$.

(3) Bila G grup komutatif, maka G/H komutatif.

(4) Bila G siklik, maka G/H siklik.

Bukti

(1) Misalkan $aH \in G/H$. Karena H adalah elemen netral di G/H order dari elemen aH adalah bilangan positip terkecil k yang memenuhi $(aH)^k = H$, tetapi $(aH)^k = a^kH$. Hal ini berakibat $a^kH = H$ bila dan hanya bila $a^k \in H$

(2) Dengan menggunakan Teorema Lagrange 3.1.4 didapat $|G| = |H|\,[G : H]$, tetapi $|G/H| = [G : H]$. Sehingga didapat

$$|G| = |H|\,[G : H] = |H|\,|G/H|.$$

Jadi $|G/H| = |G|/|H|$.

(3) Misalkan G komutatif dan $aH, bH \in G/H$, didapat

$$aH\,bH = (ab)H = (ba)H = bH\,aH.$$

Terlihat bahwa G/H komutatif.

(4) Misalkan G siklik dan $\langle a\rangle$, dibuat pemetaan $\phi : G \to G/H$ diberikan oleh $\phi(x) = xH$, $\forall x \in G$. Pemetaan ϕ adalah homomorpisma. Sebab, diberikan sebarang $x, y \in G$, maka $x = a^i$, $y = a^j$ untuk beberapa $i, j \in \mathbb{Z}$. Didapat

$$\phi(xy) = \phi(a^i a^j) = \phi(a^{i+j}) = a^{i+j}H = (a^i)(a^j)H = a^iH\,a^jH = xH\,yH.$$

Selanjutnya, diberikan sebarang $zH \in G/H$, maka $z = a^n$ untuk beberapa $n \in \mathbb{Z}$, didapat $\phi(a^n) = a^nH = (aH)^n$. Tetapi $zH = a^nH$. Jadi $zH = (aH)^n \in \langle aH\rangle$. Dengan demikian $G/H \subseteq \langle aH\rangle$. Jelas bahwa $\langle aH\rangle \subseteq G/H$ sebab $\langle aH\rangle$ adalah subgrup dari G/H. Jadi $G/H = \langle aH\rangle$. Dengan demikian G/H adalah siklik. ✓

Kebalikan proposisi bagian (3) dan (4) yang baru saja dibahas tidak benar sebagaimana diberikan pada contoh berikut.

Contoh 3.4.6 Diberikan subgrup A_3 dalam S_3. Indeks $[S_3 : A_2] = 2$. Jadi grup kuasi S_3/A_3 mempunyai order 2, maka dari itu $S_3/A_3 \cong \mathbb{Z}_2$. Sebagaimana telah diketahui $\mathbb{Z}_2$ komutatif dan siklik, sedangkan S_3 tidak komutatif dan tidak siklik. ●

Misalkan $\phi : \mathbb{Z} \to \mathbb{Z}_7$ adalah homomorpisma dimana $\phi(n) = [n]_7$, $\forall n \in \mathbb{Z}$. Maka $\ker(\phi) = 7\mathbb{Z}$. Dikonstruksi grup kuasi $\mathbb{Z}/7\mathbb{Z}$ sebagaimana dalam Contoh 3.4.1, didapat $\mathbb{Z}/7\mathbb{Z} \cong \mathbb{Z}_7$. Diinginkan memahami lebih baik informasi isomorpisma ini melalui hubungan diantara suatu homomorpisma, image dan kernelnya serta grup kuasi.

Bila $\phi : G \to G'$ sebarang pemetaan, maka untuk sebarang himpunan bagian $X \subseteq G$ image dari X oleh ϕ dinotasikan sebagai $\phi(X)$, yaitu

$$\phi(X) = \{x' \in G' \,|\, x' = \phi(x), \text{ untuk beberapa } x \in X\}.$$

Sejalan dengan ini, untuk sebarang himpunan bagian $Y \subseteq G'$ preimage dari Y dinotasikan sebagai $\phi^{-1}(Y)$ diberikan oleh

$$\phi^{-1}(Y) = \{x \in G \,|\, \phi(x) \in Y\}.$$

Contoh 3.4.7 Dipilih $17 \in \mathbb{Z}$ dan gunakan homomorpisma

$$\phi : \mathbb{Z} \to \mathbb{Z}_7,\ \phi(n) = [n]_7,\ \forall n \in \mathbb{Z}.$$

Dihitung ϕ^{-1} sebagai berikut:

$$\phi(17) = [17]_7 = [3]_7 \text{ dan } \phi^{-1}(\phi(17)) = [3]_7 + 7\mathbb{Z}.$$

Himpunan $[3]_7 + 7\mathbb{Z}$ adalah koset dari kernel dari ϕ, yaitu $7\mathbb{Z}$ dimana $[17]_7$ berada pada $[17]_7 + 7\mathbb{Z} = [3]_7 + 7\mathbb{Z}$. Hubungan ini berlaku untuk elemen yang lain di $\mathbb{Z}$. Catatan, khususnya bahwa $\phi^{-1}(\phi(0)) = 7\mathbb{Z} = \ker(\phi)$.

Proposisi 3.4.2 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma dengan $\ker(\phi) = K$. Maka untuk sebarang $g \in G$ didapat $\phi^{-1}(\phi(g)) = gK$.

Bukti Pilih $y \in G'$ yang memenuhi

$$\phi^{-1}(y) = \{x \in G \,|\, \phi(x) = y\}.$$

Hal ini berakibat bahwa untuk sebarang $g \in G$, maka $x \in \phi^{-1}(\phi(g))$ bila dan hanya bila $\phi(x) = \phi(g)$. Kondisi ini ekivalen dengan $\phi(g)^{-1}\phi(x) = e'$, dimana e' adalah elemen netral dari G'. Karena $\phi(g)^{-1}\phi(x) = \phi(g^{-1}x)$. Hal ini berakibat bahwa $x \in \phi^{-1}(\phi(g))$ bila dan hanya bila $\phi(g^{-1}x) = e'$, dengan kata lain bila dan hanya bila $g^{-1}x \in \ker(\phi) = K$. Kondisi ini ekivalen dengan $x \in gK$. Didapat $\phi^{-1}(\phi(g)) \subseteq gK$ dan $gK \subseteq \phi^{-1}(\phi(g))$. Jadi $\phi^{-1}(\phi(g)) = gK$

Akibat 3.4.1 Diberikan suatu homomorpisma $\phi : G \to G'$. Maka $\phi^{-1}(\phi(e)) = \ker(\phi)$.

Bukti Hal ini adalah akibat langsung dari Proposisi 3.4.2, karena $eK = K$.

Definisi 3.4.2 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma. Image

$$\phi(G) = \{\phi(x) \,|\, x \in G\}$$

sebagaimana telah diketahui adalah subgrup dari G' dan sama dengan G' bila ϕ pemetaan pada. Dalam hal ini G' dinamakan suatu **Image Homomorpik** dari G.

Teorema berikut menunjukkan bahwa ada suatu korespondensi diantara subgrup dan image homomorpik dari suatu grup.

Teorema 3.4.2 (**Teorema Isomorpisma Pertama**) Diberikan suatu homomorpisma

$$\phi : G \to G'$$

dengan $\ker(\phi) = K$. Maka

$$G/K \cong \phi(G).$$

Bukti Dikonstruksi suatu pemetaan $\chi : G/K \to \phi(G)$ sebagai berikut. Diberikan sebarang elemen $gK \in G/K$, maka gK adalah suatu koset dari K dalam G untuk beberapa $g \in G$. Juga, sebarang elemen dari $y \in \phi(G)$ memenuhi $y = \phi(g)$ untuk beberapa $g \in G$. Dengan demikian cara yang wajar untuk mendefinisikan suatu pemetaan yang dikonstruksi adalah

$$\chi(gK) = \phi(g), \ \forall gK \in G/K.$$

Perlu diselidiki bahwa pemetaan ini terdefinisi secara baik, dengan kata lain bila $g_1K = g_2K$, maka haruslah $\phi(g_1) = \phi(g_2)$. Untuk melihat hal ini, bila $g_1K = g_2K$, maka $g_2^{-1}g_1 \in K$. Hal ini berakibat

$$\phi(g_2)^{-1}\phi(g_1) = \phi(g_2^{-1}g_1) = e',$$

didapat $\phi(g_1) = \phi(g_2)$. Selanjutnya diberikan sebarang $g_1K, g_2K \in G/K$. Maka

$$\chi(g_1K\, g_2K) = \chi(g_1g_2K) = \phi(g_1g_2) = \phi(g_1)\phi(g_2) = \chi(g_1K)\chi(g_2K).$$

Terlihat bahwa χ adalah suatu homomorpisma. Berikutnya, diberikan sebarang elemen $g_1K, g_2K \in G/K$ dan misalkan $\chi(g_1K) = \chi(g_2K)$. Karena $\chi(g_1K) = \phi(g_1)$ dan $\chi(g_2K) = \phi(g_2)$, didapat $\phi(g_1) = \phi(g_2)$. Jadi, dengan menggunakan Proposisi 3.4.2 didapat

$$g_1K = \phi^{-1}(\phi(g_1)) = \phi^{-1}(\phi(g_2)) = g_2K$$

Hal ini menunjukkan bahwa χ satu-satu. Akhirnya, diberikan sebarang $y \in \phi(G)$ dapat dipilih $x \in G$ yang memenuhi $y = \phi(x)$. Karena $\chi(xK) = \phi(x)$, maka $y = \chi(xK)$. Hal ini menunjukkan bahwa χ adalah pada.

Contoh 3.4.8 Tentukan apa bentuk dari grup kuasi $\mathbb{R}/\mathbb{Z}$? Untuk menjawab pertanyaan ini konstruksi suatu pemetaan $\phi : \mathbb{R} \to S^1$ diberikan oleh $\phi(x) = \cos 2\pi x + i \sin 2\pi x$, $\forall x \in \mathbb{R}$ dimana S' grup diberikan dalam Contoh 2.1.15. Pemetaan ϕ adalah homomorpisma sebab, diberikan sebarang $x, y \in \mathbb{R}$ didapat

$$\begin{aligned}
\phi(x+y) &= \cos(2\pi(x+y)) + i\sin(2\pi(x+y)) \\
&= \cos(2\pi x + 2\pi y) + i\sin(2\pi x + 2\pi y) \\
&= (\cos 2\pi x + i \sin 2\pi x)(\cos 2\pi y + i \sin 2\pi y) \\
&= \phi(x)\phi(y).
\end{aligned}$$

Pemetaan ϕ adalah pada sebab diberikan sebarang $(\cos 2\pi x + i \sin 2\pi x) \in S^1$ dapat dipilih $x \in \mathbb{R}$ yang memenuhi $\phi(x) = \cos 2\pi x + i \sin 2\pi x$, jadi $\phi(\mathbb{R}) = S^1$. Kernel dari ϕ adalah

$$\ker(\phi) = \{x \in \mathbb{R} \,|\, \cos 2\pi x + i \sin 2\pi x = 1\} = \{x = n \in \mathbb{Z}\} = \mathbb{Z}.$$

Dengan menggunakan teorema isomorpisma pertama didapat $\mathbb{R}/\mathbb{Z} \cong S^1$.

Implikasi dari Teorema Isomorpisma Pertama adalah manifold. Misalnya, diinginkan mendapatkan semua homomorpisma yang mungkin dari suatu grup G ke grup G' yang berbeda dengan G. Tinjau subgrup normal K dari G dan tentukan dari masing-masing homomorpisma apakah G/K isomorpik dengan suatu subgrup dari G'.

Contoh 3.4.9 Misalkan ditentukan untuk mendapatkan semua homomorpisma taktrivial yang mungkin dari $\phi : S_3 \to \mathbb{Z}_4$. Kondisi bahwa ϕ taktrivial berarti bahwa diinginkan $\ker(\phi) = K$ suatu subgrup sejati dari S_3. Subgrup normal sejati dari S_3 hanya $\{e\}$ dan A_3. Tetapi $K = \{e\}$ suatu hal yang takmungkin, sebab $S_3/K = S_3$ dan fakta bahwa $S_3/K \cong \phi(S_3)$ berakibat $|\phi(S_3)| = 6$. Hal ini suatu yang mustahil, karena $\phi(S_3) \subseteq \mathbb{Z}_4$. Jadi yang mungkin hanya $K = A_3$. Dalam kasus ini, $\phi(S_3) \cong S_3/A_3$ adalah grup berorder 2. Grup $\mathbb{Z}_4$ adalah siklik, mempunyai subgrup tunggal berorder 2, yaitu $\langle [2]_4 \rangle = \{[0]_4, [2]_4\}$. Dengan demikian pemetaan ϕ diberikan oleh

$$\phi(\sigma) = \begin{cases} [0]_4, & \text{bila } \sigma \in A_3 \\ [2]_4, & \text{bila } \sigma \notin A_3 \end{cases}$$

adalah suatu homomorpisma.

Contoh 3.4.10 Misalkan dicari semua homomorpisma taktrivial yang mungkin dari pemetaan $\phi : S_3 \to \mathbb{Z}_3$. Argumentasi dari contoh sebelumnya menunjukkan bahwa kemungkinan suatu subgrup dari $\mathbb{Z}_3$ adalah $\phi(S_3)$ dengan order 2. Tetapi $\mathbb{Z}_3$ tidak mempunyai subgrup yang berorder 2. Jadi tidak akan mungkin bisa dikonstruksi suatu homomorpisma dari S_3 ke $\mathbb{Z}_3$. ●

Contoh terakhir memberikan gambaran bagaimana dalam kasus grup berhingga bisa didapat bahwa akibat memanfaatkan teorema isomorpisma pertama; diberikan dua grup yang berbeda tidak akan mungkin bisa dikonstruksi suatu homomorpisma grup.

Proposisi 3.4.3 Misalkan G dan G' adalah grup berhingg a dan $\phi : G \to G'$ adalah suatu homomorpisma. Maka $|\phi(G)|$ membagi $|G|$ dan $|G'|$.

Bukti Himpunan $\phi(G)$ adalah subgrup dari G', dengan menggunakan teorema Lagrange didapat $|\phi(G)|$ membagi $|G'|$. Dari teorema isomorpisma pertama didapat $|\phi(G)| = |G/\ker(\phi)|$, tetapi $|G/\ker(\phi)| = |G|/|\ker(\phi)|$. Jadi $|\phi(G)| = |G|/|\ker(\phi)|$ atau $|G| = |\phi(G)||\ker(\phi)|$. Dengan demikian $|\phi(G)|$ membagi $|G|$. ●

Diberikan suatu grup G dan suatu homomorpisma $\phi : G \to G'$, maka $K = \ker(\phi)$ adalah subgrup normal dari G. Teorema berikut membahas hal yang sebaliknya juga benar.

Teorema 3.4.3 Diberikan suatu grup G dan suatu subgrup normal K dari G, ada suatu homomorpisma pada $\pi : G \to G/K$ dimana $\ker(\pi) = K$. Pemetaan π dinamakan **natural** homomorpisma.

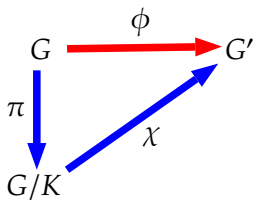
Bukti Dikonstruksi π sebagai berikut: untuk setiap $g \in G$ berlaku $\pi(g) = gK \in G/K$. Karena $K \lhd G$. Sebagaimana telah diketahui G/K adalah grup dengan operasi $g_1K\,g_2K = g_1g_2K$. Maka π adalah suatu homomorpisma, sebab

$$\pi(g_1g_2) = g_1g_2K = (g_1K)(g_2K) = \pi(g_1)\pi(g_2),\ \forall g_1, g_2 \in G.$$

Dalam grup G/K elemen netral adalah K. Sehingga didapat $x \in \ker(\pi)$ bila dan hanya bila $\pi(x) = K$ dan karena $\pi(x) = xK$, didapat $x \in \ker(\pi)$ bila dan hanya bila $xK = K$. Hal ini ekivalen dengan $x \in K$. Jadi $\ker(\pi) = K$. Pemetaan π adalah pada, sebab setiap elemen dari G/K mempunyai bentuk gK untuk beberapa $g \in G$. ●

Teorema terakhir yang baru saja dibahas memfaktorkan sebarang homomorpisma dalam dua langkah. Diberikan suatu homomorpisma $\phi : G \to G'$ dengan $\ker(\phi) = K$, misalkan $\pi : G \to G/K$ adalah homomorpisma dari Teorema 3.4.3 dan $\chi : G/K \to G'$ adalah homomorpisma dalam bukti dari Teorema 3.4.2. Maka karena untuk sebarang $g \in G$ didapat $\chi(\pi(g)) = \chi(gK) = \phi(g)$, maka $\phi = \chi \circ \pi$ atau diagram diberikan oleh Gambar 3.1 adalah komutatif. Pada akhir bagian ini dibahas teorema Cauchy khusus hanya untuk grup Abel (komutatif). Teorema Cauchy yang umum menyatakan bila G suatu grup G mempunyai order berhingga dan p adalah bilangan prima yang membagi order G, maka G mempunyai suatu elemen berorder p. Teorema ini dibahas pada bab yang lainnya.

Teorema 3.4.4 (**Teorema Cauchy untuk grup komutatif**) Diberikan G suatu grup komutatif mempunyai order berhingga dan p adalah bilangan prima yang membagi order G, maka G mempunyai suatu elemen berorder p.



Gambar 3.1: Diagram Komutatif

Bukti Digunakan induksi pada $|G|$. Bila $|G| = 1$ tidak ada yang perlu dibuktikan. Bila $|G| = 2$ atau 3, maka G siklik, dan pernyataan dalam teorema benar. Asumsikan pernyataan benar untuk semua grup komutatif yang mempunyai order lebih kecil dari $|G|$. Bila G tidak mempunyai subgrup sejati tak-trivial, maka G adalah siklik, maka menurut Teorema 2.3.4 pernyataan teorema benar. Selanjutnya, misalkan H adalah suatu subgrup sejati tak-trivial dari G. Bila p membagi $|H|$, maka karena H adalah grup komutatif yang memenuhi $|H| < |G|$, menurut hipotisis induksi ada suatu elemen $a \in H \subset G$ yang berorder p. Dengan demikian benar pernyataan teorema. Berikutnya asumsikan bahwa p tidak membagi $|H|$. Karena G komutatif, maka $H \lhd G$ dan G/H adalah suatu grup komutatif yang memenuhi $|G/H| = |G|/|H|$. Karena H taktrivial, maka $|G|/|H| < |G|$ dan karena p membagi $|G|$ dan tidak membagi $|H|$, maka p membagi $|G|/|H|$. Jadi dengan hipotisis induksi ada suatu elemen $X \in G/H$ yang mempunyai order p. Himpunan X mempunyai bentuk bH untuk beberapa $b \in G$, dimana $bH \neq H$ dan $(bH)^p = H$. Jadi $b \notin H$, tetapi karena $b^pH = (bH)^p = H$, maka $b^p \in H$. Misalkan $c = b^{|H|} \in G$. Maka

$$c^p = \left(b^{|H|}\right)^p = (b^p)^{|H|} = e \text{ (karena } b^p \in H).$$

Tinggal menunjukkan bahwa $c \neq e$. Andaikan $c = e$, maka $e = b^{|H|}$ sehingga didapat

$$H = eH = b^{|H|}H = (bH)^{|H|}$$

dan menurut Akibat 2.3.1, maka p harus membagi $|H|$. Hal ini bertentangan dengan kenyataan asumsi bahwa p tidak membagi $|H|$. Jadi haruslah $c \neq e$ dan $|c| = p$. Lengkap sudah bukti. ✓

Teorema 3.4.5 (**Teorema Isomorpisma Kedua**) Bila H dan K adalah subgrup dari suatu grup G dengan $H \lhd G$, maka $H \cap K \lhd K$ dan

$$K/(H \cap K) \cong HK/H.$$

Bukti Menurut Proposisi 3.3.3, maka HK adalah subgrup dari G. Jelas bahwa $H < HK$, selanjutnya ditunjukkan bahwa $H \lhd HK$ sebagai berikut: Bila $H \leq S \leq G$, maka karena $H \lhd G$ dengan menggunakan Teorema 3.3.2 didapat $gHg^{-1} \subseteq H$ untuk semua $g \in G$, juga khususnya $gHg^{-1} \subseteq H$ untuk semua $g \in S$. Jadi $H \lhd S$. Dengan demikian untuk $S = HK$ didapat $H \lhd HK$. Diberikan sebarang $xH \in HK/H$, maka $xH = (hk)H$ untuk beberapa $h \in H$ dan beberapa $k \in K$. Tetapi

$$hk = (kk^{-1})hk = k(k^{-1}hk) = kh'$$

dimana $k^{-1}hk = h' \in H$ sebab $H \lhd HK$. Sehingga didapat

$$xH = (hk)H = kh'H = k(h'H) = kH, \text{ untuk beberapa } k \in K.$$

Dengan demikian pemetaan $\phi : K \to HK/H$ didefinisikan oleh $\phi(k) = kH$, $\forall k \in K$ adalah pemetaan pada. Pemetaan ϕ adalah pembatasan dari pemetaan natural $\pi : G \to G/H$. Jadi $\phi(k) = \pi(k) = kH, \forall k \in K \subseteq G$. Dengan demikian ϕ adalah homomorpisma. Karena $\ker(\pi) = H$, maka $\ker(\phi) = H \cap K$. Jadi $H \cap K \lhd K$. Dengan menggunakan teorema isomorpisma pertama didapat $K/(H \cap K) \cong HK/H$.

Teorema isomorpisma kedua menghasilkan $K/(H \cap K) \cong HK/H$ hal berakibat

$$|K/(H \cap K)| = |HK/H| \text{ atau } |HK| = |H||K|/|H \cap K|.$$

Hal ini sesuai dengan hasil dalam Teorema 3.3.5.

Teorema 3.4.6 (**Teorema Isomorpisma Ketiga**) Bila H dan K adalah subgrup normal dari suatu grup G dan $K \leq H$, maka $H/K \lhd G/K$ dan

$$(G/K)/(H/K) \cong G/H.$$

Bukti definisikan pemetaan $\phi : G/K \to G/H$ oleh $\phi(aK) = aH$, $\forall aK \in G/K$, pemetaan ini terdefinisi dengan baik sebab: bila untuk $a' \in G$ dan $a'K = aK$, maka $a^{-1}a' \in K \subseteq H$. Jadi $a^{-1}a' \in H$ akibatnya $a'H = aH$. Dengan demikian bila $aK = a'K$, maka

$$\phi(a'K) = a'H = aH = \phi(aK).$$

Jadi ϕ terdefinisi dengan baik. Selanjutnya diberikan sebarang $aK, bK \in G/K$ didapat

$$\phi(aK\, bK) = \phi((ab)K) = (ab)H = aH\, bH = \phi(aK)\phi(bK).$$

Jadi ϕ adalah homomorpisma. Diberikan sebarang $aH \in G/H$, dapat dipilih $aK \in G/K$ yang memenuhi $\phi(aK) = aH$. Jadi ϕ adalah homomorpisma pada dengan demikian $\phi(G/K) = G/H$. Karena $aH = H$ bila dan hanya bila $a \in H$, maka $\ker(\phi) = H/K$. Jadi $H/K \lhd G/H$ dengan menggunakan teorema isomorpisma pertama didapat

$$(G/K)/(H/K) \cong G/H.$$

Latihan

Latihan 3.4.1 Tentukan nilai n sedemikian hingga $\mathbb{Z}_n$ isomorpik dengan grup kuasi siklik berikut:

1. $\mathbb{Z}_6/\langle [2]_6 \rangle$ 2. $\mathbb{Z}_{12}/\langle [8]_{12} \rangle$ 3. $\mathbb{Z}_{15}/\langle [6]_{15} \rangle$ 4. S_4/A_4 5. $D_4/\langle \rho \rangle$ 6. $Q_8/\langle \mathbf{j} \rangle$.

Latihan 3.4.2 Dapatkan order elemen dari grup kuasi berikut:

1. $[3]_{12} + \langle [8]_{12} \rangle$ dalam $\mathbb{Z}_{12}/\langle [8]_{12} \rangle$.

2. $[3]_{15} + \langle [6]_{15} \rangle$ dalam $\mathbb{Z}_{15}/\langle [6]_{15} \rangle$.

3. $[2]_{15} + \langle [6]_{15} \rangle$ dalam $\mathbb{Z}_{15}/\langle [6]_{15} \rangle$.

4. $\mathbf{i}\langle \mathbf{j} \rangle$ dalam $Q_8/\langle \mathbf{j} \rangle$.

5. $\rho \left\langle \rho^2 \right\rangle$ dalam $D_4/\left\langle \rho^2 \right\rangle$.

Latihan 3.4.3 Dapatkan semua homomorpisma taktrivial yang mungkin dari grup berikut:

1. $\phi : S_3 \to \mathbb{Z}_6$.

2. $\phi : D_4 \to \mathbb{Z}_4$.

3. $\phi : \mathbb{Z}_5 \to \mathbb{Z}_{10}$.

4. $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_5$.

Latihan 3.4.4 Misalkan $\phi : G \to G'$ adalah suatu homomorpisma pada dengan $\ker(\phi) = K$ dan H' adalah suatu subgrup dari G'. Tunjukkan bahwa ada suatu subgrup H dari G sedemikian hingga $K \subseteq H$ dan $H/K \cong H'$.

Latihan 3.4.5 Misalkan H dan K adalah subgrup dari suatu grup G sedemikian hingga $H \lhd G$, $K \lhd G$, $[G : H] = 5$ dan $[G : K] = 3$. Tunjukkan bahwa untuk semua elemen-elemen $g \in G$ didapat $g^{15} \in H \cap K$.

Latihan 3.4.6 Diberikan dihedral grup

$$D_6 = \{\rho^i \tau^j \,|\, 0 \leq i < 6, 0 \leq j < 2\},$$

dimana $\rho^6 = \tau^2 =$ identitas dan $\rho\tau = \tau\rho^{-1}$. Tunjukkan bahwa
(a). $\left\langle \rho^3 \right\rangle \lhd D_6$. (b). $D_6/\left\langle \rho^3 \right\rangle \cong S_3$.

Latihan 3.4.7 Diberikan dihedral grup

$$D_n = \{\rho^i \tau^j \,|\, 0 \leq i < n, 0 \leq j < 2\},$$

dimana $\rho^n = \tau^2 =$ identitas dan $\rho\tau = \tau\rho^{-1}$. Untuk sebarang k pembagi dari n tunjukkan bahwa
(a). $\left\langle \rho^k \right\rangle \lhd D_n$. (b). $D_n/\left\langle \rho^k \right\rangle \cong D_k$.

Latihan 3.4.8 Misalkan $Z(G)$ adalah senter dari suatu grup G. Tunjukkan bahwa
(a). $Z(G) \lhd G$ (b). Bila $G/Z(G)$ siklik, maka G adalah komutatif.

Latihan 3.4.9 Misalkan $Z(G)$ adalah senter dari suatu grup G. Tunjukkan bahwa bila $[G : Z(G)] = p$ dengan p adalah prima, maka G adalah komutatif.

Latihan 3.4.10 Misalkan G adalah suatu grup dan $S \subset G$ dengan $S \neq \emptyset$. Didefinisikan $\langle S \rangle$ adalah subgrup terkecil dari G yang memuat S dinamakan subgrup dari G **dibangun** oleh S. Tunjukkan bahwa $\langle S \rangle$ exist.

Latihan 3.4.11 Tunjukkan bahwa dalam S_4 subgrup yang dibangun oleh $S = \{(1\ 2), (1\ 2\ 3\ 4)\}$ adalah S_4.

Latihan 3.4.12 Misalkan G adalah suatu grup dan

$$S = \left\{ xyx^{-1}y^{-1} \mid x, y \in G \right\}.$$

Misalkan $N = \langle S \rangle$, dalam hal ini N dinamakan subgrup **komutator** dari G. Maka tunjukkan bahwa:

(a) $N \lhd G$.

(b) G/N komutatif.

(c) Bila H suatu normal subgrup dari G dan G/H komutatif, maka $N \subseteq H$.

(d) Bila H suatu subgrup dari G dengan $N \subseteq H$, maka $H \lhd G$.

Latihan 3.4.13 Dapatkan semua subgrup komutator dari S_3.

Latihan 3.4.14 Dapatkan semua subgrup komutator dari D_4.

Digraf Cayley

Misalkan G suatu grup berhingga dan S suatu himpunan bagian dari G yang membangun G. Suatu himpunan dari persamaan yang dipenuhi oleh generator yaitu secara lengkap menentukan tabel operasi biner dari G dinamakan himpunan **relasi penentu**.

Contoh, D_4 dibangun oleh $S = \{\rho, \tau\}$ dengan relasi penentu $\rho^4 = \tau^2 = \rho_0$ dan $\rho\tau = \tau\rho^{-1}$. Grup kuoternion $Q_8 = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{ij}\}$ dibangun oleh $S = \{\mathbf{i}, \mathbf{j}\}$ dengan relasi penentu $\mathbf{i}^4 = 1, \mathbf{i}^2 = \mathbf{j}^2$ dan $\mathbf{ij} = -\mathbf{ji}$.

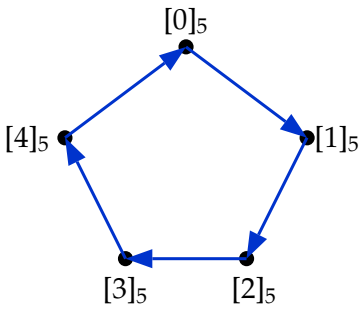
Diberikan suatu himpunan S yang membangun suatu grup berhingga G. Dikonstruksi suatu **graf berarah** atau **digraf Cayley** dari G yang berkaitan dengan S sebagai berikut:

(1) Masing-masing elemen dari G disajikan oleh titik.

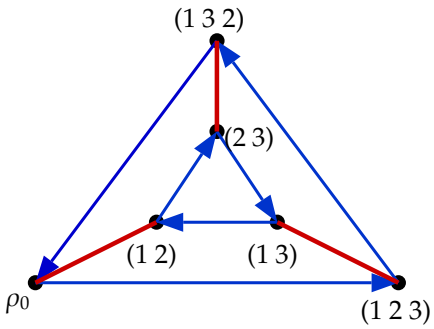
(2) Masing-masing elemen dari S disajikan oleh garis berarah.

(3) Bila $c \in S$ disajikan oleh garis berarah $\rightarrow$, maka untuk $a, b \in G$, $a\bullet \rightarrow \bullet b$ mempunyai arti $ac = b$ di G.

(4) Bila $c \in S$ dengan $c^{-1} = c$, maka tanda panah dihapus dari garis yang menyajikan c.



Digraf Cayley dari $\mathbb{Z}_5$ dengan $S = \{[1]_5\}$ dan $\rightarrow$ representasi dari $[1]_5$.



Digraf Cayley dari grup simetri S_3 dengan $S = \{(1\,2), (1\,2\,3)\}$ dan $\rightarrow$ representasi dari $(1\,2\,3)$, sedangkan $-$ representasi dari $(1\,2)$.

Perhatikan bahwa dari gambar diagram terlihat bahwa grup simetri S_3 tidak komutatif.

Latihan

Latihan 3.4.15 Tunjukkan bahwa digraf Cayley dari suatu grup harus memenuhi empat kondisi berikut:

(1) Untuk setiap pasangan titik x dan y ada suatu lintasan yaitu suatu barisan garis terhubung yang mulai dari x berakhir pada y.

(2) Setidaknya ada satu garis dari suatu titik x ke suatu titik y.

(3) Pada masing-masing titik x ada tepat satu garis dari masing-masing jenis garis yang dimulai dari x dan ada tepat satu garis dari masing-masing macam garis yang berakhir pada x.

(4) Bila dua lintasan berbeda dimulai dari suatu titik x dan keduanya berakhir pada titik y, maka dua lintasan yang sama dimulai dari sebarang titik z akan berakhir pada titik yang sama yaitu w.

Latihan 3.4.16 Konstruksi digraf Cayley dari grup G dan himpunan pembangun S berikut:

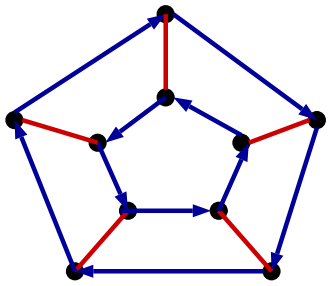
(1) $G = \mathbb{Z}_6$, $S = \{[1]_6\}$.

(2) $G = \mathbb{Z}_6$, $S = \{[2]_6, [3]_6\}$.

(3) $G = S_3$, $S = \{(1\ 2), (2\ 3)\}$.

(4) $G = D_4$, $S = \{\rho, \tau\}$.

(5) $G = A_4$, $S = \{(1\ 2\ 3), (1\ 2)(3\ 4)\}$.



Gambar 3.2: Digraf Cayley

Latihan 3.4.17 Identifikasi grup dan himpunan pembangun dan relasi penentu yang merepresentasikan digraf Cayley diberikan oleh Gambar 3.2.

3.5 Automorpisma

Telah dikaji isomorpisma diantara satu grup dan grup lainnya. Pada bagian ini ditinjau isomorpisma diantara suatu grup dan grup itu sendiri. Suatu hal yang akan dibahas bahwa himpunan isomorpisma ini membentuk suatu grup dalam suatu cara yang wajar.

Contoh 3.5.1 Misalkan akan ditentukan semua isomorpisma yang mungkin dari $\phi : \mathbb{Z}_6 \to \mathbb{Z}_6$. Sebagaimana telah diketahui $\mathbb{Z}_6$ adalah siklik dan $[1]_6$ adalah suatu generator dari $\mathbb{Z}_6$, yaitu $\mathbb{Z}_6 = \langle [1]_6 \rangle$. Maka menurut Proposisi 3.2.6 didapat, bila ϕ adalah suatu isomorpisma dari G ke G', maka $|\phi(a)| = |a|$ untuk semua $a \in G$. Jadi $|\phi([1]_6)| = |[1]_6| = 6$. Dengan demikian $\phi([1]_6)$ haruslah suatu generator dari $\mathbb{Z}_6$, maka dari itu $\phi([1]_6) = [1]_6$ atau $\phi([1]_6) = [5]_6$. Juga, sekali $\phi([1]_6)$ diketahui, maka ϕ secara lengkap dapat ditentukan; sebab $\phi([2]_6) = 2\phi([1]_6), \phi([3]_6) = 3\phi([1]_6)$ dan seterusnya. Jadi, ada tepat dua isomorpisma. Misalkan ϕ_0 adalah pemetaan identitas, yaitu

$$\phi_0([n]_6) = [n]_6, \ \forall [n]_6 \in \mathbb{Z}_6$$

dan ϕ_1 adalah isomorpisma yang diberikan oleh

$$\phi_1([n]_6) = 5[n]_6, \ \forall [n]_6 \in \mathbb{Z}_6.$$

Sekarang, tinjau himpunan $\{\phi_0, \phi\}$ dengan operasi komposisi fungsi, didapat $\phi_0 \circ \phi_0 = \phi_0$ dan $\phi_0 \circ \phi_1 = \phi_1 \circ \phi_0 = \phi_1$. Lalu bagaimana komposisi $\phi_1 \circ \phi_1$? Untuk menjawab pertanyaan ini cukup ditentukan nilai dari $[1]_6$ terhadap $\phi_1 \circ \phi_1$ sebagai berikut:

$$\phi_1 \circ \phi_1([1]_6) = \phi_1(\phi_1([1]_6)) = \phi_1([5]_6) = 5[5]_6 = [25]_6 = [1]_6 = \phi_0([1]_6).$$

Jadi, $\phi_1 \circ \phi_1 = \phi_0$. Dengan demikian himpunan $\{\phi_0, \phi_1\}$ terhadap operasi biner komposisi fungsi adalah grup siklik berorder 2. ●

Definisi 3.5.1 Misalkan G adalah suatu grup. Suatu isomorpisma $\phi : G \to G$ dinamakan **automorpisma** dari G dan himpunan dari semua automorpisma dari G dinotasikan oleh $\text{Aut}(G)$. ✓

Telah ditunjukkan dalam Contoh 3.5.1 bahwa himpunan $\text{Aut}(G)$ adalah suatu grup. Teorema berikut dibuktikan bahwa automorpisma dari suatu grup selalu membentuk suatu grup.

Teorema 3.5.1 Misalkan G adalah suatu grup. Maka $\text{Aut}(G)$ membentuk suatu grup terhadap operasi komposisi fungsi.

Bukti Sifat tertutup, misalkan $\phi_1, \phi_2 \in \text{Aut}(G)$ dan tinjau $\phi_1 \circ \phi_2$. Dalam Teorema 1.1.2 telah ditunjukkan bahwa komposisi dari fungsi satu-satu menghasilkan fungsi satu-satu dan komposisi dari fungsi pada menghasilkan fungsi pada. Jadi komposisi $\phi_1 \circ \phi_2$ adalah satu-satu pada dengan demikian untuk menunjukkan $\phi_1 \circ \phi_2 \in \text{Aut}(G)$ tinggal menunjukkan $\phi_1 \circ \phi_2$ adalah homomorpisma. Tetapi hal ini telah ditunjukkan dalam Proposisi 3.2.5. Sifat assosiatif juga telah ditunjukkan dalam Teorema 1.1.2 bahwa komposisi dari fungsi adalah asosiatif. Sifat identitas, misalkan ϕ_0 fungsi identitas pada G, yaitu $\phi_0(a) = a, \ \forall a \in G$. Juga dalam Proposisi 3.2.5 telah ditunjukkan bahwa, pemetaan identitas adalah suatu isomorpisma grup pada G. Jadi $\phi_0 \in \text{Aut}(G)$ dan memenuhi $\phi \circ \phi_0 = \phi = \phi_0 \circ \phi, \ \forall \phi \in \text{Aut}(G)$. Sifat invers, untuk $\phi \in \text{Aut}(G)$, maka menurut Teorema 1.1.4 $\phi^{-1} : G \to G$ dijamin ada dan satu-satu pada yang memenuhi $\phi \circ \phi^{-1} = \phi_0 = \phi^{-1} \circ \phi$. Tinggal menunjukkan bahwa ϕ^{-1} adalah suatu homomorpisma. Misalkan $a, b \in G$ dan $c = \phi^{-1}(a), d = \phi^{-1}(b)$. Didapat $\phi(c) = a, \phi(d) = b$. Karena ϕ homomorpisma, maka $\phi(cd) = \phi(c)\phi(d) = ab$. Hal ini berakibat $\phi^{-1}(ab) = cd = \phi^{-1}(a)\phi^{-1}(b)$. Hal ini menunjukkan bahwa ϕ^{-1} adalah suatu homomorpisma sebagaimana yang diinginkan. Dengan demikian lengkap sudah bukti. ✓

Contoh 3.5.2 Akan ditentukan Aut($\mathbb{Z}_8$). Karena $\mathbb{Z}_8$ siklik dengan generator $[1]_8$, maka bila ϕ sebarang automorpisma haruslah $|\phi([1]_8)| = |[1]_8| = 8$ dan $\phi([1]_8)$ juga suatu generator dari $\mathbb{Z}_8$. Yaitu $\phi([1]_8) = [1]_8$ atau $\phi([1]_8) = [3]_8$ atau $\phi([1]_8) = [5]_8$ atau $\phi([1]_8) = [7]_8$. Tetapi, karena sekali nilai $\phi([1]_8)$ ditentukan, maka ϕ secara lengkap dapat ditentukan. Sebab secara umum $\phi([n]_8) = n\phi([1]_8)$ dan pemetaan ini adalah isomorpisma. Jadi terdapat tepat empat automorpisma. Yaitu pemetaan identitas $\phi_1([n]_8) = [n]_8$, $\forall [n]_8 \in \mathbb{Z}_8$, pemetaan $\phi_3([n]_8) = 3[n]_8$, $\forall [n]_8 \in \mathbb{Z}_8$, pemetaan $\phi_5([n]_8) = 5[n]_8$, $\forall [n]_8 \in \mathbb{Z}_8$ dan pemetaan $\phi_7([n]_8) = 7[n]_8$, $\forall [n]_8 \in \mathbb{Z}_8$. Dalam hal ini, didapat

$$\phi_3 \circ \phi_5([n]_8) = \phi_3(\phi_5([n]_8)) = \phi_3(5[n]_8) = 15[n]_8 = 7[n]_8.$$

Jadi $\phi_3 \circ \phi_5 = \phi_7 \in$ Aut($\mathbb{Z}_8$). Secara umum, didapat bahwa bila $ij \equiv k \mod 8$, maka $\phi_i \circ \phi_j = \phi_k \in$ Aut($\mathbb{Z}_8$). Dari apa yang dibahas ini, pemetaan $T(\phi_i) = i$ memberikan suatu isomorpisma diantara Aut($\mathbb{Z}_8$) dengan grup perkalian $\mathbb{U}(8)$. ●

Contoh yang baru saja dibahas dapat digeneralisasi untuk sebarang grup siklik G sebagaimana ditunjukkan dalam teorema berikut.

Teorema 3.5.2 Diberikan grup siklik G dengan order n. Maka Aut(G) $\cong \mathbb{U}(n)$.

Bukti Didefinisikan suatu pemetaan T : Aut(G) $\to \mathbb{U}(n)$ sebagai berikut. Misalkan $G = \langle a \rangle$ dimana $|a| = n$. Tinjau $\phi \in$ Aut(G), maka untuk sebarang $g \in G$ didapat $g = a^i$ untuk beberapa bilangan bulat i dengan $0 \leq i < n$ dan $\phi(g) = \phi(a^i) = \phi(a)^i$. Terlihat bahwa sekali nilai a ditetapkan maka ϕ secara lengkap dapat ditentukan. Sehingga didapat $|\phi(a)| = |a| = n$. Terlihat bahwa $\phi(a)$ adalah suatu generator dari G. Maka dari itu menurut Akibat 2.3.4 $\phi(a) = a^r$ untuk berapa r dimana fpb$(n, r) = 1$ selanjutnya gunakan Teorema 2.3.1 didapat $a^r = a^s$ bila dan hanya bila $s \equiv r \mod n$. Jadi ada suatu $s \in \{q \mid \text{fpb}(n, q) = 1, 0 \leq q < n\} = \mathbb{U}(n)$ yang memenuhi $\phi(a) = a^s$. Dari yang telah dibahas, dapat ditentukan $T(\phi) = s$, $\forall \phi \in$ Aut(G), dimana $\phi(a) = s$ dan $s \in \mathbb{U}(n)$. Berikutnya ditunjukkan bahwa T suatu homomorpisma. Bila $\phi, \psi \in$ Aut(G) dengan $\phi(a) = a^s$ dan $\psi(a) = a^t$ dimana $s, t \in \mathbb{U}(n)$, maka didapat

$$\psi \circ \phi(a) = \psi(\phi(a)) = \psi(a^s) = a^{st} = a^u,$$

dimana $u \equiv st \mod n$. Jadi

$$T(\psi \circ \phi) = u = st \mod n = ts \mod n = T(\psi)T(\phi).$$

Pemetaan T adalah satu-satu, sebab bila $T(\phi) = T(\psi)$, maka

$$\phi(a) = a^{T(\phi)} = a^{T(\psi)} = \psi(a),$$

jadi $\phi = \psi$. Juga, pemetaan T adalah pada, sebab diberikan sebarang $s \in \mathbb{U}(n)$, maka a^s adalah suatu generator dari G, dengan menggunakan Lemma 3.2.1 dapat dipilih pemetaan ϕ yang memenuhi $\phi(a^i) = a^{is} = (a^i)^s$ adalah suatu isomorpisma. Dari sini kita memperoleh $T(\phi) = s$. ∎

Untuk suatu grup siklik G telah diketahui apa bentuk dari Aut(G). Untuk grup komutatif taksiklik situasinya lebik kompleks. Untuk grup takkomutatif, proposisi berikut menunjukkan bagaimana mengkonstruksi berbagai contoh automorpisma.

Proposisi 3.5.1 Misalkan G adalah suatu grup, $g \in G$ dan $T_g : G \to G$ pemetaan yang didefinisikan oleh $T_g(x) = gxg^{-1}$, $\forall x \in G$. Maka $T_g \in \text{Aut}(G)$.

Bukti Pemetaan T_g adalah homomorpisma, sebab untuk semua $x, y \in G$ didapat

$$T_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = T_g(x)T_g(y).$$

Pemetaan T_g adalah satu-satu, sebab diberikan sebarang $x \in \ker(\phi)$ didapat

$$T_g(x) = gxg^{-1} = e,$$

maka $x = g^{-1}eg = g^{-1}g = e$. Jadi $\ker(\phi) = \{e\}$. Dengan demikian T_g satu-satu. Selanjutnya diberikan sebarang $y \in G$, pilih $x = g^{-1}yg \in G$ didapat $T_g(x) = gxg^{-1} = gg^{-1}ygg^{-1} = y$. Jadi T_g adalah pada. ✓

Definisi 3.5.2 Misalkan G adalah suatu grup dan $g \in G$. Maka automorpisma T_g yang didefinisikan oleh $T_g(x) = gxg^{-1}$, $\forall x \in G$ dinamakan suatu **inner automorpisma**. Himpunan semua inner automorpisma dinotasikan oleh $\text{Inn}(G)$. ✓

Proposisi 3.5.2 Misalkan G adalah suatu grup. Maka $\text{Inn}(G)$ adalah suatu subgrup dari $\text{Aut}(G)$.

Bukti Inner automorpisma T_e adalah elemen identitas, sebab untuk sebarang $x \in G$ didapat $T_e(x) = exe^{-1} = x$. Diberikan sebarang $T_g, T_h \in \text{Inn}(G)$ dan sebarang $x \in G$ didapat

$$T_g \circ T_h(x) = T_g(T_h(x)) = T_g(hxh^{-1}) = (gh)x(h^{-1}g^{-1}) = (gh)x(gh)^{-1} = T_{gh}(x).$$

Jadi $T_g \circ T_h = T_{gh} \in \text{Inn}(G)$. Diberikan sebarang $T_g \in \text{Inn}(G)$, maka

$$T_{g^{-1}} \circ T_g(x) = T_{g^{-1}}(T_g(x)) = T_{g^{-1}}(gxg^{-1}) = g^{-1}gxg^{-1}g = x$$

dan

$$T_g \circ T_{g^{-1}} = T_g(T_{g^{-1}}(x)) = T_g(g^{-1}xg) = gg^{-1}xgg^{-1} = x.$$

Jadi $T_{g^{-1}} \circ T_g = T_e = T_g \circ T_{g^{-1}}$. Dengan demikian $T_{g^{-1}}$ adalah invers dari T_g. ✓

Contoh 3.5.3 Akan ditentukan $\text{Inn}(D_4)$. Perhatikan bahwa bila $g \in Z(D_4)$ dimana $Z(D_4)$ adalah senter dari D_4, maka T_g adalah identitas, sebab

$$T_g(x) = gxg^{-1} = gg^{-1}x = ex = x, \text{ untuk semua } x \in D_4.$$

Sebagaimana telah diketahui, senter $Z(D_4) = \{\rho_0, \rho^2\}$. Bila g sebarang elemen di D_4, didapat $T_{g\rho^2} = T_g \circ T_{\rho^2} = T_g$ (sebab T_{ρ^2} adalah identitas). Dapat dihitung

$$\begin{aligned}
T_\rho(\rho^i\tau) &= \rho(\rho^i\tau)\rho^{-1} = \rho\rho^i(\tau\rho^{-1}) = \rho\rho^i(\rho\tau) = \rho^{i+2}\tau \\
T_\tau(\rho^i\tau) &= \tau(\rho^i\tau)\tau^{-1} = \tau\rho^i = \rho^{-i}\tau \\
T_{\rho\tau}(\rho^i\tau) &= \rho\tau(\rho^i\tau)\tau^{-1}\rho^{-1} = \rho\tau\rho^{i-1} = \rho^{-i+2}\tau = T_\rho(\rho^{-i}\tau) = T_\rho(T_\tau(\rho^i\tau)) = T_\rho \circ T_\tau(\rho^i\tau).
\end{aligned}$$

Bila pemetaan identitas dinotasikan oleh T_0, maka $T_0, T_\rho, T_\tau, T_{\rho\tau}$ adalah inner automorpisma dari D_4. Perlu diperhatikan bahwa

$$D_4/Z(D_4) = \{Z(D_4), \rho Z(D_4), \tau Z(D_4), \rho\tau Z(D_4)\}.$$

Terlihat ada keterkaitan diantara inner automorpisma dari D_4 dengan koset dari senter $Z(D_4)$. Kenyataannya keterkaitan ini adalah suatu isomorpisma. ●

Hubungan diantara $\text{Inn}(G)$ dan $Z(G)$ yang baru saja dibahas dalam contoh sebelumnya berlaku secara umum untuk sebarang grup.

Teorema 3.5.3 Untuk sebarang grup G, maka $\text{Inn}(G) \cong G/Z(G)$ dimana $Z(G)$ adalah senter dari G.

Bukti Misalkan $\chi : G \to \text{Inn}(G)$ adalah pemetaan didefinisikan oleh $\chi(g) = T_g \in \text{Inn}(G)$ untuk semua $g \in G$. Dengan menggunakan teorema isomorpisma pertama, cukup ditunjukkan bahwa χ adalah homomorpisma pada dan $\ker(\chi) = Z(G)$. Pemetaan χ sebagaimana telah dibahas dalam Proposisi 3.5.2 adalah homomorpisma, sebab untuk sebarang $g, h \in G$ didapat

$$\chi(gh) = T_{gh} = T_g \circ T_h = \chi(g)\chi(h).$$

Lagipula, χ adalah pada sebab $\chi \in \text{Inn}(G)$. Akhirnya, $g \in \ker(\chi)$ bila dan hanya bila $\chi(g) = T_g$ adalah pemetaan identitas. Kondisi ini ekivalen dengan $gxg^{-1} = x$ atau $xg = gx$ untuk semua $x \in G$. Jadi $g \in \ker(\chi)$ bila dan hanya bila g komutatif dengan setiap elemen $x \in G$, hal ini berarti bahwa $g \in Z(G)$. ✓

Latihan

Latihan 3.5.1 Misalkan $\phi_1, \phi_3, \phi_5, \phi_7$ adalah automorpisma dari $\mathbb{Z}_8$ sebagaimana dalam Contoh 3.5.2. Tunjukkan bahwa bila $ij = k \mod 8$, maka $\phi_i \circ \phi_j = \phi_k$. ✓

Latihan 3.5.2 Dengan notasi sebagaimana diberikan dalam Latihan 3.5.1, tunjukkan bahwa pemetaan $T : \text{Aut}(G) \to \mathbb{U}(8)$ didefinisikan oleh $T(\phi_i) = i$ adalah suatu isomorpisma. ✓

Latihan 3.5.3 Misalkan $G = \langle a \rangle$ adalah suatu grup siklik berorder 10. Uraikan secara langsung elemen-elemen dari $\text{Aut}(G)$. ✓

Latihan 3.5.4 Misalkan G adalah suatu grup komutatif. Tunjukkan bahwa suatu pemetaan $\phi : G \to G$ didefinisikan oleh $\phi(x) = x^{-1}$ untuk semua $x \in G$ adalah suatu automorpisma dari G. ✓

Latihan 3.5.5 Tentukan $\text{Aut}(\mathbb{Z})$. ✓

Latihan 3.5.6 Tunjukkan bahwa pemetaan $\phi : S_3 \to S_3$ didefinisikan oleh $\phi(x) = x^{-1}$ untuk semua $x \in S_3$ bukan suatu automorpisma. ✓

Latihan 3.5.7 Misalkan G adalah suatu grup, $H \lhd G$ dan $\phi \in \text{Aut}(G)$. Tunjukkan bahwa $\phi(H) \lhd G$. ✓

Latihan 3.5.8 Untuk sebarang grup G, tunjukkan bahwa $\text{Inn}(G) \lhd \text{Aut}(G)$. ✓

Latihan 3.5.9 Tunjukkan bahwa $\text{Inn}(S_3) \cong S_3$. ✓

Latihan 3.5.10 Untuk sebarang p prima, tunjukkan bahwa $\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$. ✓

Latihan 3.5.11 Misalkan Q_8 grup kuoternion. Tunjukkan bahwa $\text{Inn}(Q_8) \cong V$ grup-4 Klein. (Petunjuk: tentukan dulu $Z(Q_8)$). ✓

Latihan 3.5.12 Tunjukkan bahwa $\text{Inn}(D_4) \cong V$ grup-4 Klein.

Latihan 3.5.13 Tunjukkan bahwa $|\text{Aut}(D_4)| \leq 8$.

Latihan 3.5.14 Bila V adalah grup-4 Klein, maka tunjukkan bahwa

$$\text{Aut}(V) \cong \text{Gl}(2, \mathbb{Z}_2).$$

Latihan 3.5.15 Tunjukkan bahwa $\text{Aut}(D_4) \cong D_4$.

Latihan 3.5.16 Tunjukkan bahwa $\text{Aut}(Q_8) \cong S_4$.

Latihan 3.5.17 Tunjukkan bahwa $\text{Aut}(S_3) \cong S_3$.

Latihan 3.5.18 Untuk suatu grup G, suatu subgrup H dari G dinamakan suatu subgrup **karakteristik** dari G bila untuk semua $\phi \in \text{Aut}(G)$ didapat $\phi(H) = H$.

1. Tunjukkan bahwa bila H adalah suatu subgrup karakteristik dari G, maka $H \lhd G$.
2. Tunjukkan bahwa bila H hanyalah subgrup dari G berorder n, maka H adalah subgrup karakteristik dari G.
3. Misalkan G adalah suatu grup, H suatu subgrup normal dari G dan K suatu subgrup karakteristik dari H. Tunjukkan bahwa K adalah subgrup normal dari G.
4. Misalkan G adalah suatu grup, H adalah suatu subgrup karakteristik dari G dan K adalah suatu subgrup karakteristik dari H. Tunjukkan bahwa K adalah suatu subgrup karakteristik dari G.

Bab 4

Produk Langsung dan Grup Abelian

Dalam Bab 2 sudah dipelajari apa grup dan dibahas contoh-contoh khusus dari berbagai grup penting seperti $\mathbb{Z}_n, \mathbb{U}(n), S_n, A_n, D_n, V$ dan Q_8. Selain itu juga grup matriks $\mathrm{GL}(2,\mathbb{R})$ dan $\mathrm{SL}(2,\mathbb{R})$. Dalam Bab 3 dibahas pemetaan diantara grup yang dinamakan homomorpisma grup setelah pembahasan teorema Lagrange. Dibahas peran subgrup normal dan hubungannya dengan homomorpisma grup dan grup kuasi. Dalam bab ini dibahas bagaimana mengkonstruksi grup baru dari grupyang sudah dikenal. Juga diidentifikasi grup yang terbentuk ini yang berkaitan dengan grup komutatif dan siklik dengan menggunakan teorema-teorema yang telah dibahas dalam Bab 2. Suatu teorema yang sangat penting diturunkan yang berguna untuk mendapatkan semua grup komutatif dari suatu grup berhingga.

4.1 Contoh-contoh dan definisi

Digunakan grup yang telah dibahas sebelumnya untuk mengkonstruksi grup baru dan dipelajari sifat-sifat grup baru ini yang diwarisi dari grup aslinya. Dimulai dari beberapa contoh berikut.

Contoh 4.1.1 Tinjau himpunan $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(a,b) \mid a \in \mathbb{Z}_2, b \in \mathbb{Z}_3\}$. Elemen (a,b) adalah suatu pasangan dengan komponen pertama adalah $a = [0]_2$ atau $[1]_2$, sedangkan komponen kedua $b = [0]_3, [1]_3$ atau $[2]_3$. Jadi $\mathbb{Z}_2 \times \mathbb{Z}_3$ mempunyai tepat enam elemen,

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{([0]_2,[0]_3),([0]_2,[1]_3),([0]_2,[2]_3),([1]_2,[0]_3),([1]_2,[1]_3),([1]_2,[2]_3)\}.$$

Dikenakan operasi secara komponen yang besesuaian pada himpunan ini, yaitu

$$(a,b) + (c,d) \stackrel{\text{def}}{=} (a+c, b+d).$$

Jadi

$$([1]_2,[2]_3) + ([1]_2,[2]_3) = ([1+1]_2,[2+2]_3) = ([0]_2,[1]_3),$$
$$([1]_2,[2]_3) + ([1]_2,[1]_3) = ([1+1]_2,[2+1]_3) = ([0]_2,[0]_3)$$

dan

$$([0]_2,[0]_3) + ([1]_2,[2]_3) = ([0+1]_2,[0+2]_3) = ([1]_2,[2]_3).$$

Jelas bahwa sifat tertutup dipenuhi, elemen $([0]_2,[0]_3)$ adalah elemen netral dan invers dari (a,b) adalah $(-a,-b)$. ●

Contoh 4.1.2 Diberikan himpunan $\mathbb{Z} \times \mathbb{Z} = \{(a,b), | a,b \in \mathbb{Z}\}$, himpunan ini adalah tak-berhingga. Seperti dalam Contoh 4.1.1, operasi pada himpunan ini didefinisikan secara komponen yang bersesuaian. Maka sifat tertutup dipenuhi, elemen netral adalah $(0,0)$ dan invers dari (a,b) adalah $(-a,-b)$. ●

Contoh 4.1.3 Tinjau himpunan $\mathbb{Z}_2 \times S_3 = \{(a,\sigma) | a \in \mathbb{Z}_2, \sigma \in S_3\}$. Disini operasi juga diberlakukan secara komponen yang bersesuaian, yaitu:

$$(a,\sigma) * (b,\tau) \stackrel{\text{def}}{=} (a+b, \sigma \circ \tau).$$

Misalnya $([1]_2,\rho) * ([1]_2,\mu_1) = ([0]_2,\rho\mu_1) = ([0]_2,\mu_3)$. Elemen netral adalah $([0]_2,\rho_0)$ dan $([1]_2,\rho)^{-1} = ([1]_2,\rho_2), ([1]_2,\mu_i)^{-1} = ([1]_2,\mu_i)$. ●

Untuk sebarang grup G_1 dan G_2, mengikuti pembahasan contoh-contoh yang telah diberikan, maka himpunan pasangan dari elemen G_1 dan G_2 membentuk suatu grup sebagaimana dibuktikan dalam teorema berikut.

Teorema 4.1.1 Misalkan $\langle G_1, \circ\rangle$ dan $\langle G_2, \diamond\rangle$ grup dan

$$G = G_1 \times G_2 = \{(a_1,a_2) | a_1 \in G_1, a_2 \in G_2\}.$$

Didefinisikan operasi $*$ pada $G_1 \times G_2$ secara komponen yang bersesuaian oleh

$$(a_1,a_2) * (b_1,b_2) \stackrel{\text{def}}{=} (a_1 \circ b_1, a_2 \diamond b_2),\ \forall (a_1,a_2),(b_1,b_2) \in G_1 \times G_2.$$

Maka $\langle G, *\rangle$ adalah suatu grup.

Bukti (Tertutup) Diberikan $(a_1,a_2),(b_1,b_2) \in G_1 \times G_2$, dengan sifat tertutup untuk G_1 dan G_2 didapat $a_1 \circ b_1 \in G_1$ dan $a_2 \diamond b_2 \in G_2$. Jadi

$$(a_1,a_2) * (b_1,b_2) = (a_1 \circ b_1, a_2 \diamond b_2) \in G_1 \times G_2.$$

(Asosiatif) Diberikan sebarang $(a_1,a_2),(b_1,b_2)$ dan (c_1,c_2) di $G_1 \times G_2$, menggunakan sifat asosiatif untuk G_1 dan G_2 didapat

$$\begin{aligned}
[(a_1,a_2) * (b_1,b_2)] * (c_1,c_2) &= (a_1 \circ b_1, a_2 \diamond b_2) * (c_1,c_2) \\
&= ((a_1 \circ b_1) \circ c_1, (a_2 \diamond b_2) \diamond c_2) \\
&= (a_1 \circ (b_1 \circ c_1), a_2 \diamond (b_2 \diamond c_2)) \\
&= (a_1,a_2) * ((b_1 \circ c_1), (b_2 \diamond c_2)) \\
&= (a_1,a_2) * [(b_1,b_2) * (c_1,c_2)]
\end{aligned}$$

(Elemen netral) Misalkan e_1 elemen netral dari G_1 dan e_2 elemen netral dari G_2. Maka diberikan sebarang elemen $(a_1,a_2) \in G_1 \times G_2$ didapat

$$(e_1,e_2) * (a_1,a_2) = (e_1 \circ a_1, e_2 \diamond a_2) = (a_1,a_2) = (a_1 \circ e_1, a_2 \diamond e_2) = (a_1,a_2) * (e_1,e_2).$$

Jadi (e_1,e_2) adalah elemen netral dari $G_1 \times G_2$. (invers) Diberikan sebarang $(a_1,a_2) \in G_1 \times G_2$, misalkan a_1^{-1} invers dari a_1 di G_1 dan a_2^{-1} adalah elemen invers dari a_2 di G_2. Didapat

$$(a_1,a_2) * (a_1^{-1},a_2^{-1}) = (a_1 \circ a_1^{-1}, a_2 \diamond a_2^{-1}) = (e_1,e_2) = (a_1^{-1} \circ a_1, a_2^{-1} \diamond a_2) = (a_1^{-1},a_2^{-1}) * (a_1,a_2).$$

Jadi invers dari (a_1,a_2) adalah (a_1^{-1},a_2^{-1}). ●

Definisi 4.1.1 Diberikan dua grup G_1 dan G_2, grup $G_1 \times G_2$ dengan operasi didefinisikan sebagaimana dalam Teorema 4.1.1 dinamakan **produk langsung** dari G_1 dan G_2.

Pengkonstruksian produk langsung dapat dilakukan pada lebih dari dua grup. Bila G_1, G_2 dan G_3 adalah grup, maka dari Teorema 4.1.1 didapat $G_1 \times G_2$ adalah suatu grup terhadap operasi komponen yang bersesuaian. Lagi, Teorema 4.1.1 dapat digunakan pada dua grup $G_1 \times G_2$ dan G_3, didapat $(G_1 \times G_2) \times G_3$ terhadap operasi komponen yang bersesuaian adalah suatu grup. Proses dapat dilanjutkan untuk sebanyak berhingga grup sebagaimana dinyatakan dalam proposisi berikut.

Proposisi 4.1.1 Misalkan $G_1, G_2, \ldots, G_n$ dengan n berhingga adalah grup. Maka

$$G_1 \times G_2 \times \cdots \times G_n = \{(a_1, a_2, \ldots, a_n) \,|\, a_i \in G_i, 1 \leq i \leq n\}$$

adalah grup terhadap operasi komponen yang bersesuaian

$$(a_1, a_2, \ldots, a_n) * (b_1, b_2, \ldots, b_n) \stackrel{\text{def}}{=} (a_1 b_1, a_2 b_2 \ldots, a_n b_n).$$

Bukti Dilakukan secara induksi untuk$n$. Untuk $n = 1$ tidak ada yang perlu dibuktikan. Untuk $n = 2$ sudah terbukti dalam Teorema 4.1.1. Misalkan benar untuk $n = k$, maka $G = G_1 \times G_2 \times \cdots G_k$ adalah grup. Selanjutnya tinjau grup G dan G_{k+1}, maka menurut Teorema 4.1.1 didapat $G \times G_{k+1}$ adalah grup atau

$$(G_1 \times G_2 \times \cdots \times G_k) \times G_{k+1} = G_1 \times G_2 \times \cdots \times G_k \times G_{k+1}$$

adalah grup. Jadi pernyataan benar untuk $n = k + 1$.

Perlu diperhatikan bahwa dalam pembahasan produk langsung berkaitan dengan sebanyak berhingga grup. Untuk sebanyak takhingga grup, konstruksi dapat dilakukan dengan cara yang sama. Tentunya hal ini lebih kompleks.

Berikut ini dibahas sifat-sifat dasar dari produk langsung $G_1 \times G_2$.

Proposisi 4.1.2 Misalkan G_1 dan G_2 adalah grup. Maka $G_1 \times G_2 \cong G_2 \times G_1$.

Bukti Misalkan pemetaan $\phi : G_1 \times G_2 \to G_2 \times G_1$ didefinisikan oleh

$$\phi((a, b)) = (b, a), \ \forall (a, b) \in G_1 \times G_2.$$

Pemetaan ϕ adalah homomorpisma, sebab untuk sebarang $(a, b), (c, d) \in G_1 \times G_2$ didapat

$$\phi((a, b)(c, d)) = \phi((ac, bd)) = (bd, ac) = (b, a)(d, c) = \phi((a, b))\phi((c, d)).$$

Pemetaan ϕ satu-satu, sebab untuk $(a, b) \in \ker(\phi)$ bila dan hanya bila $(b, a) = (e_2, e_1)$. Jadi $\ker(\phi) = \{(e_1, e_2)\}$. Pemetaan ϕ adalah pada, hal ini langsung dari definisi ϕ.

Proposisi yang baru saja dibahas menjelaskan bahwa urutan untuk produk langsung tidak jadi masalah. Hal ini benar untuk mengkonstruksi produk langsung lebih dari dua grup. Proposisi berikut menjelaskan syarat untuk grup produk langsung adalah komutatif.

Proposisi 4.1.3 Misalkan G_1 dan G_2 adalah grup. Maka $G_1 \times G_2$ komutatif bila dan hanya bila G_1 dan G_2 keduanya komutatif.

Bukti Diberikan sebarang (a, b) dan (c, d) di $G_1 \times G_2$, maka $(a, b)(c, d) = (ac, bd)$ dan $(c, d)(a, b) = (ca, db)$. Jadi untuk semua pasangan dari elemen-elemen di $G_1 \times G_2$,

$$(a, b)(c, d) = (c, d)(a, b)$$

bila dan hanya bila $ac = ca$ untuk semua pasangan dari elemen-elemen di G_1 dan $bd = db$ untuk semua pasangan elemen-elemen di G_2.

Contoh berikut membahas subgrup dari produk langsung $G_1 \times G_2$.

Contoh 4.1.4 Tinjau lagi grup $\mathbb{Z}_2 \times S_3$ yang diberikan dalam Contoh 4.1.3. Misalkan $H = \mathbb{Z}_2 \times \{\rho_0\}$, dimana ρ_0 adalah elemen netral dari S_3 Jadi $H = \{([0]_2, \rho_0), ([1]_2, \rho_0)\}$, dimana $([0]_2, \rho_0)$ adalah elemen netral dari $\mathbb{Z}_2 \times S_3$. Karena $([1]_2, \rho_0)([1]_2, \rho_0) = ([0]_2, \rho_0)$, maka H adalah suatu subgrup dari $\mathbb{Z}_2 \times S_3$, faktanya adalah subgrup normal, sebab bila $(a, \sigma) \in \mathbb{Z}_2 \times S_3$, maka

$$\begin{aligned}(a, \sigma)([0]_2, \rho_0)(-a, \sigma^{-1}) &= ([0]_2, \rho_0) \in H \\ (a, \sigma)([1]_2, \rho_0)(-a, \sigma^{-1}) &= ([1]_2, \rho_0) \in H\end{aligned}$$

Juga dapat dikonstruksi himpunan

$$K = \{[0]_2\} \times S_3 = \{([0]_2, \rho_0), ([0]_2, \rho), ([0]_2, \rho^2), ([0]_2, \mu_1), ([0]_2, \mu_2), ([0]_2, \mu_3)\}.$$

Himpunan K adalah subgrup dari $\mathbb{Z}_2 \times S_3$, sebab untuk sebarang $([0]_2, \sigma_1), ([0]_2, \sigma_2) \in K$ didapat

$$([0]_2, \sigma_1)([0]_2, \sigma_2)^{-1} = ([0]_2, \sigma_1)([0]_2, \sigma_2^{-1}) = ([0]_2, \sigma_1\sigma_2^{-1}) \in K.$$

Selanjutnya, untuk sebarang $([0]_2, \sigma) \in K$ dan sebarang $(a, \tau) \in \mathbb{Z}_2 \times S_3$ didapat

$$(a, \tau)([0]_2, \sigma)(a, \tau)^{-1} = (a, \tau)([0]_2, \sigma)(-a, \tau^{-1}) = ([0]_2, \tau\sigma\tau^{-1}) \in K.$$

Jadi K adalah subgrup normal dari $\mathbb{Z}_2 \times S_3$.

Subgrup khusus dari produk langsung yang dibahas dalam Contoh 4.1.4 selalu merupakan subgrup normal. Hal ini ditunjukkan dalam proposisi berikut.

Proposisi 4.1.4 Diberikan grup G_1 dan G_2 dengan e_i adalah elemen netral dari G_i untuk $i = 1, 2$. Maka

(1) $G_1 \times \{e_2\} \lhd G_1 \times G_2$ dan $\{e_1\} \times G_2 \lhd G_1 \times G_2$

(2) $(G_1 \times G_2)/(G_1 \times \{e_2\}) \cong G_2$ dan $(G_1 \times G_2)/(\{e_1\} \times G_2) \cong G_1$

Bukti

(1) Misalkan $H = G_1 \times \{e_2\}$ dan $(a, e_2), (b, e_2) \in H$. Maka

$$(a, e_2)(b, e_2)^{-1} = (a, e_2)(b^{-1}, e_2) = (ab^{-1}, e_2) \in H.$$

Jadi H adalah suatu subgrup dari $G_1 \times G_2$. Selanjutnya misalkan sebarang elemen $(a_1, a_2) \in G_1 \times G_2$ dan sebarang elemen $(b, e_2) \in H$, didapat

$$(a_1, a_2)(b, e_2)(a_1, a_2)^{-1} = (a_1, a_2)(b, e_2)(a_1^{-1}, a_2^{-1}) = (a_1 b a^{-1}, e_2) \in H.$$

Jadi $H \lhd G_1 \times G_2$. Sejalan dengan apa yang telah dilakukan dapat ditunjukkan $\{e_1\} \times G_2 \lhd G_1 \times G_2$.

(2) Tinjau pemetaan $\phi : G_1 \times G_2 \to G_2$ didefinisikan oleh $\phi((a_1, a_2)) = a_2$, $\forall (a_1, a_2) \in G_1 \times G_2$. Maka ϕ adalah suatu homomorpisma, sebab untuk sebarang $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ didapat

$$\phi((a_1, a_2)(b_1, b_2)) = \phi((a_1 b_1, a_2 b_2)) = a_2 b_2 = \phi((a_1, a_2))\phi((b_1, b_2)).$$

Pemetaan ϕ adalah pada, sebab diberikan sebarang $y \in G_2$ dapat dipilih $(x, y) \in G_1 \times G_2$ untuk semua $x \in G_1$ yang memenuhi $\phi((x, y)) = y$. Terakhir, $(a_1, a_2) \in \ker(\phi)$ bila dan hanya bila $a_2 = e_2$ bila dan hanya bila $(a_1, a_2) \in G_1 \times \{e_2\}$. Dengan demikian $\ker(\phi) = H$. Jadi, dengan menggunakan teorema isomorpisma pertama didapat $(G_1 \times G_2)/\ker(\phi) \cong G_2$. Bukti bagian kedua dapat dilakukan dengan cara yang sama.

Latihan

Latihan 4.1.1 Untuk sebarang dua grup berhinggagrup!berhingga G_1 dan G_2, maka tentukan order dari $G_1 \times G_2$.

Latihan 4.1.2 Misalkan V adalah grup-4 Klein.Tunjukkan bahwa $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Latihan 4.1.3 Tunjukkan bahwa D_4 dan $\mathbb{Z}_2 \times \mathbb{Z}_4$ tidak isomorpik.

Latihan 4.1.4 Tunjukkan bahwa A_4 dan $\mathbb{Z}_2 \times S_3$ tidak isomorpik.

Latihan 4.1.5 Tunjukkan bahwa $(\mathbb{Z} \times \mathbb{Z})/\langle (1,1) \rangle \cong \mathbb{Z}$. (Catatan bahwa: $\langle (1,1) \rangle = \{(a, a) \mid a \in \mathbb{Z}\}$).

Latihan 4.1.6 Tunjukkan bahwa $(\mathbb{Z} \times \mathbb{Z})/\langle (1,2) \rangle \cong \mathbb{Z}$.

Latihan 4.1.7 Dalam grup produk langsung $\mathbb{Z}_2 \times \mathbb{Z}_4$ dapatkan suatu subgrup H sedemikian hingga $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Latihan 4.1.8 Dalam D_4 dapatkan suatu subgrup H yang memenuhi $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Latihan 4.1.9 Dalam $\mathbb{Z}_4 \times \mathbb{Z}_4$ dapatkan subgrup H dan K yang mempunyai order 4 yang memenuhi H tidak isomorpik dengan K, tetapi $(\mathbb{Z}_4 \times \mathbb{Z}_4)/H \cong (\mathbb{Z}_4 \times \mathbb{Z}_4)/K$.

Latihan 4.1.10 Tunjukkan bahwa $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle (1,1,1) \rangle \cong \mathbb{Z} \times \mathbb{Z}$.

Latihan 4.1.11 Misalkan $G_1, G_2, \ldots, G_n$ adalah grup dan ϕ suatu permutasi di S_n. Tunjukkan bahwa

$$G_1 \times G_2 \times \cdots \times G_n \cong G_{\phi(1)} \times G_{\phi(2)} \times \cdots \times G_{\phi(n)}.$$

Latihan 4.1.12 Misalkan G_1 dan G_2 adalah grup. Tunjukkan bahwa

$$Z(G_1 \times G_2) \cong Z(G_1) \times Z(G_2).$$

Latihan 4.1.13 Misalkan $H \lhd G_1$ dan $K \lhd G_2$. Tunjukkan bahwa

(a) $H \times K$ adalah suatu subgrup dari $G_1 \times G_2$.

(b) $H \times K \lhd G_1 \times G_2$.

(c) $(G_1 \times G_2)/(H \times K) \cong G_1/H \times G_2/K$.

Latihan 4.1.14 Dapatkan suatu subgrup bormal dari $\mathbb{Z}_4 \times Q_8$.

Latihan 4.1.15 Misalkan fpb$(r,s) = 1$. Tunjukkan bahwa $\mathbb{U}(rs) \cong \mathbb{U}(r) \times \mathbb{U}(s)$.

Latihan 4.1.16 Tunjukkan bahwa $\mathbb{U}(105) \cong \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_6$.

Latihan 4.1.17 Tunjukkan bahwa $\mathbb{U}(8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Latihan 4.1.18 Dapatkan bilangan bulat r, s, t, u yang memenuhi

$$\mathbb{U}(360) \cong \mathbb{Z}_r \times \mathbb{Z}_s \times \mathbb{Z}_t \times \mathbb{Z}_u.$$

4.2 Komputasi order

Sebagaimana telah diketahui dalam Bab 3, bila dua grup adalah isomorpik maka kedua grup tersebut mempunyai banyak elemen yang sama dengan suatu order yang diberikan. Maka dari itu penting untuk mengetahui order elemen dari suatu grup. Dalam bagian ini dibahas bagaimana menghitung order dari suatu elemen dalam produk langsung dari berbagai grup dengan istilah order dari komponen.

Contoh 4.2.1 Dalam $\mathbb{Z}_4 \times \mathbb{Z}_6$ tinjau elemen $([2]_4, [5]_6)$. order elemen ini adalah bilangan bulat positip terkecil n yang memenuhi $n([2]_4, [5]_6) = ([2n]_4, [5n]_6) = ([0]_4, [0]_6)$. Jadi $[2n]_4 = [0]_4$ dan $[5n]_6 = [0]_6$. tetapi $|[2]_4| = 2$, maka dengan menggunakan Kesimpulan 2.3.1 didapat 2 membagi n. Juga karena $|[5]_6| = 6$, maka 6 membagi n. Jadi n adalah kelipatan persekutan dari 2 dan 6. Didapat

$$n = k_1 \,\text{kpk}(2,6) = k_1\, 6, \quad k_1 = 1, 2, \ldots$$

Tetapi

$$6|([2]_4, [5]_6) = ([12]_4, [30]_6) = ([0]_4, [0]_6),$$

maka dengan menggunakan Kesimpulan 2.3.1 didapat n membagi 6 atau

$$6 = k_2 n, \quad k_2 = 1, 2, \ldots$$

Sehingga didapat

$$6 = k_2 n = k_2 k_1\, 6, \quad k_1, k_2 = 1, 2, \ldots$$

Akibatnya

$$1 = k_2 k_1, \quad k_1, k_2 = 1, 2, \ldots.$$

Jadi $k_1 = k_2 = 1$. Dengan demikian $n = k_1\, 6 = 6$. Sehingga didapat

$$|([2]_4, [5]_6)| = n = 6.$$

Contoh 4.2.2 Dalam $S_3 \times S_5$, tinjau elemen $(\rho, \sigma) \in S_3 \times S_5$, dimana $\rho = (1\ 2\ 3) \in S_3$ dan $\sigma = (1\,2\,4)(3\,5) \in S_5$, maka $|\rho| = 3$ dalam S_3 dan $|\sigma| = 6$ dalam S_5. Seperti halnya dalam contoh sebelumnya, didapat $|(\rho, \sigma)| = \text{kpk}(3, 6) = 6$.

Teorema 4.2.1 Misalkan G_1dan G_2 adalah grup dan $(a_1, a_2) \in G_1 \times G_2$. Maka

$$|(a_1, a_2)| = \text{kpk}(|a_1|, |a_2|).$$

Bukti Misalkan $n = |(a_1, a_2)|$ dan $r = \text{kpk}(|a_1|, |a_2|)$. Karena $|a_1|$ membagi r dan juga $|a_2|$ membagi r, maka

$$(a_1, a_2)^r = (a_1^r, a_2^r) = (e_1, e_2).$$

Dengan menggunakan Akibat 2.3.1 didapat n membagi r. Jadi

$$r = k_1 n, \quad k_1 = 1, 2, \ldots. \tag{4.1}$$

Dilain pihak

$$(a_1^n, a_2^n) = (a_1, a_2)^n = (e_1, e_2).$$

Didapat $a_1^n = e_1$ dan $a_2^n = e_2$, hal ini berakibat $|a_1|$ membagi n dan $|a_2|$ membagi n. Jadi n adalah kelipatan persekutuan dari $|a_1|$ dan $|a_2|$. Dengan demikian

$$n = k_2\, \text{kpk}(|a_1|, |a_2|) = k_2 r, \quad k_2 = 1, 2, \ldots \tag{4.2}$$

Dari Persamaan (4.1) dan (4.2) didapat

$$r = k_1 n = k_1 k_2 r, \quad k_1, k_2 = 1, 2, \ldots$$

Akibatnya $1 = k_1 k_2$, $k_1, k_2 = 1, 2, \ldots$. Didapat $k_1 = k_2 = 1$, dengan demikian

$$\text{kpk}(|a_1|, |a_2|) = r = k_1 n = n.$$

Akibat 4.2.1 Misalkan $G = G_1 \times G_2 \times \cdots \times G_n$ adalah produk langsung dari sebanyak berhingga grup. Maka order suatu elemen dalam G diberikan oleh

$$|(a_1, a_2, \ldots, a_n)| = \text{kpk}(|a_1|, |a_2|, \ldots, |a_n|).$$

Bukti Digunakan induksi untuk n. Untuk $n = 1$ tidak ada yang perlu dibuktikan. Untuk $n = 2$ sudah dibuktikan dalam Teorema 4.2.1. Jadi, misalkan Kesimpulan benar untuk produk dari k grup, dan tinjau suatu produk $k + 1$ grup berikut

$$G_1 \times G_2 \times \cdots \times G_k \times G_{k+1} = (G_1 \times G_2 \times \cdots \times G_k) \times G_{k+1}.$$

Untuk melengkapi bukti, dari Teorema 4.2.1 didapat

$$\begin{aligned} |(a_1, a_2, \ldots, a_k, a_{k+1})| &= \text{kpk}(|(a_1, a_2, \ldots, a_k)|, |a_{k+1}|) \\ &= \text{kpk}(\text{kpk}(|a_1|, |a_2|, \ldots, |a_k|), |a_k|) \quad \text{(benar untuk produk dari } k \text{ grup)} \\ &= \text{kpk}(|a_1|, |a_2|, \ldots, |a_k|, |a_{k+1}|). \end{aligned}$$

Contoh 4.2.3 Misalnya akan ditentukan order $|([10]_{12}, [10]_{18})$ dalam $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$. Pertama secara terpisah ditentukan dulu order dari komponen-komponennya. Dengan menggunakan Teorema 2.3.2 didapat

$$|[10]_{12}| = 12/\text{fpb}(12, 10) = 12/2 = 6$$

dan

$$|[10]_{18}| = 18/\text{fpb}(18, 10) = 18/2 = 9.$$

Selanjutnya, gunakan Teorema 4.2.1 didapat

$$|([10]_{12}, [10]_{18})| = \text{kpk}(6, 9) = 18.$$

Akibat 4.2.2 Misalkan sebarang elemen $(r, s) \in \mathbb{Z}_n \times \mathbb{Z}_m$. Maka

$$|(r, s)| = \text{kpk}(n/\text{fpb}(n, r), m/\text{fpb}(m, s)).$$

Bukti Hal ini langsung didapat dari Teorema 2.3.2 dan Teorema 4.2.1.

Akibat 4.2.3 Misalkan sebarang elemen $(r, s) \in \mathbb{Z}_n \times \mathbb{Z}_m$. Maka

$$|(r, s)| \leq |([1]_n, [1]_m)| = \text{kpk}(n, m).$$

Bukti Dalam $\mathbb{Z}_n$, maka $|r|$ membagi n dan dalam $\mathbb{Z}_m$, $|s|$ membagi m. Jadi sebarang kelipatan persekutuan dari n dan m adalah suatu kelipatan persekutuan dari $|r|$ dan $|s|$, didapat

$$|(r, s)| = \text{kpk}(|r|, |s|) \leq \text{kpk}(n, m).$$

Selain itu, $|[1]_n| = n$ dan $|[1]_m| = m$, sehingga dengan menggunakan Teorema 4.2.1 didapat $|([1]_n, [1]_m)| = \text{kpk}(|[1]_n|, |[1]_m|) = \text{kpk}(n, m)$.

Teorema berikut hasil dari beberapa kesimpulan yang telah dibahas dan memainkan suatu peranan yang penting dalam mengklasifikasikan grup komutatif berhingga.

Teorema 4.2.2 Grup produk langsung $\mathbb{Z}_n \times \mathbb{Z}_m$ isomorpik dengan grup siklik $\mathbb{Z}_{nm}$ bila dan hanya $\text{fpb}(n, m) = 1$.

Bukti ($\Rightarrow$) Bila $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$, maka $\mathbb{Z}_n \times \mathbb{Z}_m$ adalah siklik. Dari Akibat 4.2.3 didapat $([1]_n, [1]_m)$ adalah suatu generator dari $\mathbb{Z}_n \times \mathbb{Z}_m$. Jadi haruslah $|([1]_n, [1]_m)| = nm$. Tetapi, lagi digunakan Akibat 4.2.3 didapat

$$|([1]_n, [1]_m)| = \text{kpk}(n, m) = nm/\text{fpb}(n, m),$$

dari yang didapat ini haruslah $\text{fpb}(n, m) = 1$. ($\Leftarrow$) Bila $\text{fpb}(n, m) = 1$, maka

$$|([1]_n, [1]_m)| = \text{kpk}(n, m) = nm/\text{fpb}(n, m) = nm,$$

terlihat bahwa elemen $([1]_n, [1]_m)$ membangun keseluruhan elemen-elemen dari $\mathbb{Z}_n \times \mathbb{Z}_m$. Jadi $\mathbb{Z}_n \times \mathbb{Z}_m$ adalah siklik. Dengan demikian isomorpik dengan grup $\mathbb{Z}_{nm}$.

Akibat 4.2.4 $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s} \cong \mathbb{Z}_{n_1 n_2 \cdots n_s}$ bila dan hanya bila untuk semua $1 \leq i < j \leq s$, $\text{fpb}(n_i, n_j) = 1$.

Bukti Sebagai latihan (lihat Latihan 4.2.8).

Contoh 4.2.4 Tinjau grup kuasi $(\mathbb{Z}_4 \times \mathbb{Z}_4)/\langle([1]_4,[1]_4)\rangle$. Karena $|\mathbb{Z}_4 \times \mathbb{Z}_4| = 16$ dan

$$|\langle([1]_4,[1]_4)\rangle| = |([1]_4,[1]_4)| = \text{kpk}(4,4) = 4,$$

didapat

$$|(\mathbb{Z}_4 \times \mathbb{Z}_4)/\langle([1]_4,[1]_4)\rangle| = 16/4 = 4.$$

Jadi kemungkinannya $(\mathbb{Z}_4 \times \mathbb{Z}_4)/\langle([1]_4,[1]_4)\rangle$ isomorpik dengan $\mathbb{Z}_4$ atau dengan grup-4 Klein V. Tetapi elemen $([1]_4,[0]_4) + \langle([1]_4,[1]_4)\rangle$ bila dihitung berorder 4. Jadi grup kuasi $(\mathbb{Z}_4 \times \mathbb{Z}_4)/\langle([1]_4,[1]_4)\rangle$ adalah siklik, dengan demikian isomorpik dengan $\mathbb{Z}_4$. ●

Contoh 4.2.5 Diberikan

$$\mathbb{U}(10) = \{[1]_{10},[3]_{10},[7]_{10},[9]_{10}\}$$

dan

$$\mathbb{U}(12) = \{[1]_{12},[5]_{12},[7]_{12},[11]_{12}\},$$

jadi $|\mathbb{U}(10) \times \mathbb{U}(12)| = 16$. Misalkan $H = \langle([7]_{10},[7]_{12})\rangle$ subgrup dari $\mathbb{U}(10) \times \mathbb{U}(12)$. Didapat

$$H = \{([1]_{10},[1]_{12}),([7]_{10},[7]_{12}),([9]_{10},[1]_{12}),([3]_{10},[7]_{12})\}$$

dan

$$|(\mathbb{U}(10) \times \mathbb{U}(12))/H| = 16/4 = 4$$

Bila dihitung didapat

$$(\mathbb{U}(10) \times \mathbb{U}(12))/H = \{H,([3]_{10},[1]_{12})H,([3]_{10},[5]_{12})H,([3]_{10},[11]_{12})H\}$$

dan

$$([3]_{10},[1]_{12})^2 = ([3]_{10},[5]_{12})^2 = ([3]_{10},[11]_{12})^2 = ([9]_{10},[1]_{12}) \in H.$$

Jadi semua elemen di $(\mathbb{U}(10)\times\mathbb{U}(12))/H$ yang bukan H mempunyai order 2. Dengan demikian

$$(\mathbb{U}(10) \times \mathbb{U}(12))/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$ ●

Latihan

Latihan 4.2.1 Dapatkan order elemen dari grup berikut.

(a) $([4]_6,[6]_8) \in \mathbb{Z}_6 \times \mathbb{Z}_8$.

(b) $([15]_{20},[15]_{27}) \in \mathbb{Z}_{20} \times \mathbb{Z}_{27}$.

(c) $(\rho,[7]_{12}) \in S_3 \times \mathbb{U}_{12}$.

(d) $(\rho,[7]_{12}) \in D_4 \times \mathbb{U}_{12}$.

(e) $(\rho,\mathbf{i}) \in S_3 \times Q_8$.

(f) $((2\ 3\ 4),[15]_{18}) \in A_4 \times \mathbb{Z}_{18}$. ●

Latihan 4.2.2 Dapatkan semua koset yang berbeda dari subgrup dalam grup berikut.

(a) $H = \langle([8]_{10},[2]_4)\rangle$ dalam $\mathbb{Z}_{10} \times \mathbb{Z}_4$.

(b) $H = \langle([3]_{10}, [5]_{12})\rangle$ dalam $\mathbb{U}_{10} \times \mathbb{U}_{12}$.

(c) $H = \langle(6, 8)\rangle$ dalam $3\mathbb{Z} \times 2\mathbb{Z}$.

(d) $H = \langle(\rho, \tau)\rangle$ dalam $D_4 \times D_4$.

Latihan 4.2.3 Dapatkan order elemen dari grup kuasi berikut.

(a) $([1]_{10}, [1]_4) + \langle([8]_{10}, [2]_4)\rangle$ dalam $(\mathbb{Z}_{10} \times \mathbb{Z}_4)/\langle([8]_{10}, [2]_4)\rangle$.

(b) $([7]_{10}, [7]_{12})\langle([3]_{10}, [5]_{12})\rangle$ dalam $(\mathbb{U}_{10} \times \mathbb{U}_{12})/\langle([3]_{10}, [5]_{12})\rangle$.

(c) $(3, 2) + \langle(6, 8)\rangle$ dalam $(3\mathbb{Z} \times 2\mathbb{Z})/\langle(6, 8)\rangle$.

(d) $(\rho^3, \tau)\langle(\rho, \tau)\rangle$ dalam $(D_4 \times D_4)/\langle(\rho, \tau)\rangle$.

Latihan 4.2.4 Tunjukkan bahwa $\mathbb{Z}_9 \times \mathbb{Z}_9$ tidak isomorpik dengan $\mathbb{Z}_{27} \times \mathbb{Z}_3$.

Latihan 4.2.5 Tunjukkan bahwa $\mathbb{C} \cong \mathbb{R} \times \mathbb{R}$.

Latihan 4.2.6 Dapatkan oder terbesar dari sebarang elemen di $\mathbb{Z}_{21} \times \mathbb{Z}_{35}$.

Latihan 4.2.7 Dapatkan semua elemen yang berorder 4 dalam $\mathbb{Z}_4 \times \mathbb{Z}_4$.

Latihan 4.2.8 Buktikan Akibat 4.2.4.

Latihan 4.2.9 Dapatkan semua homomorpisma grup dari $\mathbb{Z}_6$ ke $\mathbb{Z}_2 \times \mathbb{Z}_3$ dan tentukan yang mana merupakan isomorpisma.

Latihan 4.2.10 Tunjukkan bahwa bila G adalah suatu grup berhingga sedemikian hingga untuk semua $g \in G$ didapat $g^2 = e$, maka

(a) G komutatif.

(b) $|G| = 2^n$ untuk beberapa bilangan bulat positip n.

(c) $G \cong \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \times \mathbb{Z}_2}_{n}$.

4.3 Jumlahan Langsung

Telah dibahas produk langsung untuk mengkonstruksi grup baru. Berikut ini digunakan istilah yang mirip yaitu jumlahan langsung dan mendekomposisi beberapa grup untuk dijadikan sebagai jumlahan langsung dari subgrup normal tertentu. Hal ini akan meningkatkan pemahaman mengenai grup tersebut.

Sebagaimana akan dibahas dalam bagian ini, dekomposisi yang dibicarakan dapat digunakan secara lengkap untuk mengkarakteristik semua grup komutatif berhingga.

Pertama, diberikan ilustrasi dari pengertian melalui suatu contoh.

Contoh 4.3.1 Dalam $\mathbb{Z}_{12}$, misalkan subgrup

$$H = \langle [3]_{12} \rangle = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$$

dan

$$K = \langle [4]_{12} \rangle = \{[0]_{12}, [4]_{12}, [8]_{12}\}.$$

Karena $\mathbb{Z}_{12}$ komutatif, maka H dan K keduanya subgrup normal dari $\mathbb{Z}_{12}$. Menurut Proposisi 3.3.3, maka

$$H + K = \{h + k \,|\, h \in H, k \in K\}$$

adalah subgrup dari $\mathbb{Z}_{12}$. Perlu diperhatikan bahwa $H \cap K = \{[0]_{12}\}$ dan menggunakan Teorema 3.3.5 didapat

$$|H + K| = |H|\,|K|/|H \cap K| = 4(3)/1 = 12.$$

Jadi $\mathbb{Z}_{12} = H + K$. Lagi pula, fakta bahwa $H \cap K = \{[0]_{12}\}$ berakibat bahwa setiap elemen $a \in \mathbb{Z}_{12}$ dapat dituliskan secara tunggal sebagai $a = h + k$ dimana $h \in H$ dan $k \in K$. Sebab bila $a = h_1 + k_1 = h_2 + k_2$, maka $h_1 - h_2 = k_2 - k_1 \in H \cap K = \{[0]_{12}\}$. Akibatnya $h_1 = h_2$ dan $k_1 = k_2$. Faktanya dapat ditunjukkan bahwa $\mathbb{Z}_{12} \cong H \times K \cong \mathbb{Z}_4 \times \mathbb{Z}_3$. Berikutnya, misalkan subgrup

$$L = \langle [2]_{12} \rangle = \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}.$$

Dengan mudah bisa diselidiki bahwa $\mathbb{Z}_{12} = H + L$. Dengan demikian setiap elemen $a \in \mathbb{Z}_{12}$ dapat ditulis sebagai $a = h + l$ dimana $h \in H$ dan $l \in L$. Tetapi penulisan ini tidak tunggal, misalnya

$$[7]_{12} = [3]_{12} + [4]_{12} = [9]_{12} + [10]_{12},$$

dimana $[3]_{12}, [9]_{12} \in H$ dan $[4]_{12}, [10]_{12} \in L$. Dalam kasus ini perhatikan bahwa

$$H \cap L = \{[0]_{12}, [6]_{12}\} \neq \{[0]_{12}\}. \quad \bullet$$

Contoh 4.3.2 Dalam S_3 subgrup A_3 adalah subgrup normal. Bila $H = A_3$ dan $K = \langle \mu_1 \rangle$, maka lagi gunakan Proposisi 3.3.3 didapat HK adalah subgrup dari S_3. Juga, lagi gunakan Teorema 3.3.5 didapat

$$|HK| = |H|\,|K|/|H \cap K| = 3(2)/1 = 6.$$

Jadi $S_3 = HK$. Tetapi, jelas bahwa S_3 tidak isomorpik dengan $H \times K \cong \mathbb{Z}_3 \times \mathbb{Z}_2$, sebab S_3 tidak komutatif. Apa yang "salah" dalam kasus ini adalah bahwa $K = \langle \mu_1 \rangle$ bukan subgrup normal dari S_3. $\bullet$

Teorema berikut memberikan karakterisasi yang terbaik dalam pemahaman pengertian yang telah dikenalkan lewat dua contoh. Pertama dibutuhkan suatu lemma sederhana berikut.

Lemma 4.3.1 Misalkan G adalah suatu grup, H dan K adalah subgrup dari G yang memenuhi

(1) $H \lhd G$ dan $K \lhd G$.

(2) $H \cap K = \{e\}$.

Maka untuk semua $h \in H$ dan $k \in K$ didapat $hk = kh$.

Bukti Akan ditunjukkan $hk = kh$, untuk semua $h \in H$ dan $k \in K$, untuk itu tinjau elemen $y = hkh^{-1}k^{-1}$. Karena $H \lhd G$, maka $kh^{-1}k^{-1} \in H$. Jadi $y = h(kh^{-1}k^{-1}) \in H$. Karena $K \lhd G$, maka $hkh^{-1} \in K$. Jadi $y = (hkh^{-1})k^{-1} \in K$. Dengan demikian

$$hkh^{-1}k^{-1} = y \in H \cap K = \{e\},$$

akibatnya $hkh^{-1}k^{-1} = e$ atau $hk = kh$.

Teorema 4.3.1 *G adalah suatu grup berhingga, H dan K adalah subgrup dari G yang memenuhi*

(1) $H \lhd G$ dan $K \lhd G$.

(2) $H \cap K = \{e\}$.

(3) $|HK| = |G|$.

Maka $G \cong H \times K$.

Bukti definisikan suatu pemetaan $\phi : H \times K \to G$ oleh $\phi((h,k)) = hk$, $\forall (h,k) \in H \times K$. Pemetaan ϕ adalah homomorpisma, sebab dari Lemma 4.3.1 didapat

$$\phi((h_1,k_1)(h_2,k_2)) = \phi((h_1h_2,k_1k_2)) = h_1h_2k_1k_2 = (h_1k_1)(h_2k_2) = \phi((h_1,k_1))\phi((h_2,k_2)).$$

Pemetaan ϕ adalah satu-satu, sebab bila $\phi((h_1,k_1)) = \phi((h_2,k_2))$, maka $h_1k_1 = h_2k_2$. Hal ini berakibat bahwa $h_1^{-1}h_2 = k_2k_1^{-1} \in H \cap K = \{e\}$ atau $h_1 = h_2$ dan $k_1 = k_2$. Juga, pemetaan ϕ adalah pada sebab dari teorema isomorpisma pertama didapat

$$|\phi(H \times K)|/|\ker(\phi)| = |H|\,|K|/1 = |HK| = |G|.$$

Pada akhir bagian ini kosentrasi pembahasan pada grup komutatif dimana kondisi (1) dalam Teorema 4.3.1 selalu dipenuhi. Misalkan H_1 dan H_2 adalah subgrup dari suatu grup komutatif G, maka H_1 dan H_2 adalah subgrup normal dari G; dan $H_1 + H_2$ adalah suatu subgrup dari G. Tambahan pula, bila $H_1 \cap H_2 = \{e\}$, maka setiap elemen x di $H_1 + H_2$ dapat ditulis secara tunggal sebagai $x = h_1 + h_2$, dimana $h_1 \in H_1$ dan $h_2 \in H_2$. Dalam hal ini $H_1 + H_2$ dinamakan jumlahan langsung dari H_1 dan H_2 dan ditulis $H_1 \oplus H_2$. Berikut ini secara formal dinyatakan definisi jumlahan langsung dari sebanyak berhingga subgrup.

Definisi 4.3.1 Misalkan $H_1, H_2, \ldots, H_n$ adalah subgrup dari suatu grup komutatif G. Maka

$$H_1 + H_2 + \cdots + H_n$$

dinamakan suatu **jumlahan langsung** dan ditulis sebagai

$$H_1 \oplus H_2 \oplus \cdots \oplus H_n,$$

bila untuk sebarang $x \in H_1 + H_2 + \cdots + H_n$ didapat

$$x = h_1 + h_1 + \cdots + h_n = h_1' + h_2' + \cdots + h_n',$$

dimana $h_i, h_i' \in H_i$ bila dan hanya bila $h_i = h_i'$ untuk semua i, $1 \le i \le n$.

Jadi dalam suatu jumlahan langsung $H \oplus K$, sebarang elemen x secara tunggal disajikan sebagai $x = h + k$, dimana $h \in H$ dan $k \in K$. Dalam Contoh 4.3.1, $\mathbb{Z}_{12} = H \oplus K$, tetapi $\mathbb{Z}_{12} = H + L$ bukan jumlahan langsung.

Diberikan beberapa definisi yang ekivalen dari jumlahan langsung yang akan membuat pengertian lebih jelas.

Teorema 4.3.2 Misalkan G adalah suatu grup komutatif dan $H_1, H_2, \ldots, H_n$ adalah subgrup dari G. Maka pernyataan berikut adalah ekivalen.

(1) $H_1 + H_2 + \cdots + H_n$ adalah suatu jumlahan langsung.

(2) $(H_1 + H_2 + \cdots + H_{i-1} + H_{i+1} + \cdots + H_n) \cap H_i = \{0\}$, untuk semua i, $2 \leq i < n$.

(3) $(H_1 + H_2 + \cdots + H_{i-1}) \cap H_i = \{0\}$, untuk semua i, $2 \leq i \leq n$.

(4) bila $h_1 + h_2 + \cdots + h_n = e$, dimana $h_i \in H_i$ untuk semua i, $1 \leq i \leq n$, maka $h_i = 0$ untuk semua i, $1 \leq i \leq n$.

Bukti $(1 \Rightarrow 2)$ Misalkan $x \in (H_1 + H_2 + \cdots + H_{i-1} + H_{i+1} + \cdots + H_n) \cap H_i$. Maka

$$x = h_1 + h_2 + \cdots + h_{i-1} + h_{i+i} + \cdots + h_n,$$

untuk beberapa $h_j \in H_j$, $j \neq i$. Karena $x \in H_i$, didapat dua penyajian dari $0 \in H_1 + H_2 + \cdots + H_n$, yaitu

$$0 = h_1 + h_2 + \cdots + h_{i-1} + (-x) + h_{i+1} + \cdots + h_n = 0 + 0 + \cdots + \cdots + 0.$$

Dengan definisi jumlahan langsung, maka masing-masing $h_j = 0$ juga, khususnya $x = 0$. $(2 \Rightarrow 3)$ Hal ini langsung dari fakta

$$(H_1 + H_2 + \cdots + H_{i-1}) \cap H_i \subseteq (H_1 + H_2 + \cdots + H_{i-1} + H_{i+1} + \cdots + H_n) \cap H_i.$$

$(3 \Rightarrow 4)$ Bila $h_1 + h_2 + \cdots + h_n = 0$, dimana $h_i \in H_i$ akan ditunjukkan $h_i = 0$ untuk semua i. Asumsikan sebaliknya yaitu beberapa h_i tidak nol dan tinjau bilangan bulat terbesar $k, 1 \leq k \leq n$ yang memenuhi $h_k \neq 0$. Jadi $h_{k+1} = \cdots = h_n = 0$ dan $0 = h_1 + \cdots + h_k$,. Didapat

$$h_k = -h_1 - h_2 - \cdots - h_{k-1} \in (H_1 + H_2 + \cdots H_{k-1}) \cap H_k = \{0\}.$$

Jadi $h_k = 0$, kontradiksi dengan asumsi $h_k = 0$. Jadi suatu k yang ditentukan tidak ada dengan demikian $h_i = 0$ untuk semua $i, 1 \leq i \leq n$. $(4 \Rightarrow 1)$ Ingin ditunjukkan bahwa sebarang x di $H_1 + H_2 + \cdots + H_n$ dapat disajikan secara tunggal sebagai suatu jumlah dari elemen-elemen subgrup. Jadi, misalkan

$$x = h_1 + h_2 + \cdots + h_n = h_1' + h_2' + \cdots + h_n',$$

dimana $h_i, h_i' \in H_i$. Didapat

$$(h_1 - h_1') + (h_2 - h_2') + \cdots + (h_n - h_n') = 0,$$

dimana $(h_i - h_i') \in H_i$. Jadi $(h_i - h_i') = 0$ untuk semua $i, 1 \leq i \leq n$. Dengan demikian $h_i = h_i'$ untuk semua $i, 1 \leq i \leq n$. ✓

Akibat 4.3.1 Misalkan G adalah grup komutatif berhingga, H dan K subgrup dari G yang memenuhi

(1) $H \cap K = \{0\}$.

(2) $|H + K| = |G|$.

Maka $G = H \oplus K \cong H \times K$.

Bukti Karena G komutatif, maka $H \lhd G$ dan $K \lhd G$. Dengan menggunakan Teorema 4.3.1 didapat $G \cong H \times K$ dan menggunakan Teorema 4.3.2 didapat $H + K$ adalah suatu jumlahan langsung $H \oplus K$. Juga $H \oplus K$ adalah suatu subgrup dari G dengan $|H \oplus K| = |H + K| = |G|$. Jadi $H \oplus K = G$. ✓

Teorema 4.3.3 Misalkan G grup komutatif yang memenuhi $G = H_1 \oplus H_2 \oplus \cdots \oplus H_n$. Maka $G \cong H_1 \times H_2 \times \cdots \times H_n$.

Bukti Didefinisikan suatu pemetaan $\phi : H_1 \oplus H_2 \oplus \cdots \oplus H_n \to H_1 \times H_2 \times \cdots \times H_n$ oleh

$$\phi(h_1 + h_2 + \cdots + h_n) = (h_1, h_2, \ldots, h_n),\ \forall h_1 + h_2 + \cdots + h_n \in H_1 \oplus H_2 \oplus \cdots \oplus H_n.$$

Pemetaan ϕ terdefinisi secara baik, sebab bila

$$h_1 + h_2 + \cdots + h_n = h_1' + h_2' + \cdots + h_n',$$

maka $h_i = h_i'$ untuk semua i dan $(h_1, h_2, \ldots, h_n) = (h_1', h_2', \ldots, h_n')$. Pemetaan ϕ adalah suatu homomorpisma, sebab

$$\begin{aligned}
\phi((h_1 + h_2 + \cdots + h_n) + (h_1' + h_2' + \cdots + h_n')) &= \phi((h_1 + h_1') + (h_1 + h_2') + \cdots + (h_n + h_n')) \\
&= (h_1 + h_1', h_2 + h_2', \ldots, h_n + h_n') \\
&= (h_1, h_2, \ldots, h_n) + (h_1', h_2', \ldots, h_n') \\
&= \phi(h_1 + h_2 + \cdots + h_n) + \phi(h_1' + h_2' + \cdots + h_n').
\end{aligned}$$

Pemetaan ϕ, jelas dari definisi adalah satu-satu pada. ✓

Akibat 4.3.2 Misalkan G suatu grup komutatif berhingga yang memenuhi

$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_n.$$

Maka $|G| = |H_1|\,|H_2| \cdots |H_n|$.

Bukti Hal ini didapat langsung dari Teorema 4.3.3, yaitu $G \cong H_1 \times H_2 \times \cdots \times H_n$. Akibatnya $|G| = |H_1|\,|H_2| \cdots |H_n|$. ✓

Kesimpulan berikut suatu akibat penting dari penyajian $x = h_1 + h_2 + \cdots + h_n$ untuk $x \in H_1 \oplus H_2 \oplus \cdots \oplus H_n$.

Akibat 4.3.3 Bila G suatu grup komutatif berhingga sedemikian hingga $G = H_1 \oplus H_2 \oplus \cdots \oplus H_n$ dan $x = h_1 + h_2 + \cdots + h_n$ suatu elemen di G dimana $h_i \in H_i$ untuk i, $1 \le i \le n$. Maka

$$|x| = \text{kpk}(|h_1|, |h_2|, \ldots, |h_n|).$$

Bukti Dari Teorema 4.3.3 didapat

$$G \cong H_1 \times H_2 \times \cdots \times H_n$$

dengan demikian elemen $x = x = h_1 + h_2 + \cdots + h_n$ di G berkaitan dengan elemen $(h_1, h_2, \ldots, h_n)$ di $H_1 \times H_2 \times \cdots \times H_n$. Gunakan Akibat 4.2.1 didapat

$$|(h_1, h_2, \ldots, h_n)| = \text{kpk}(|h_1|, |h_2|, \ldots, |h_n|).$$

Jadi

$$|x| = |h_1 + h_2 + \cdots + h_n| = \text{kpk}(|h_1|, |h_2|, \ldots, |h_n|). \quad \checkmark$$

Akibat 4.3.4 Bila $G = G_1 \oplus G_2$ dimana G_1 siklik berorder n dan G_2 siklik berorder m, maka $G \cong \mathbb{Z}_{nm}$ bila dan hanya bila $\text{kpk}(n, m) = 1$.

Bukti Dari Teorema 4.3.3 didapat

$$G_1 \oplus G_2 \cong \mathbb{Z}_n \times \mathbb{Z}_m$$

dan menggunakan Kesimpula 4.2.2 didapat

$$G_1 \oplus G_2 \cong \mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

bila dan hanya bila $\text{kpk}(n, m) = 1$. $\checkmark$

Lemma 4.3.2 Misalkan G suatu grup komutatif sedemikian hingga

$$G = H_1 \oplus H_2 \oplus \cdots \oplus H_n,$$

K_i adalah subgrup dari H_i untuk semua $i,\ 1 \leq i \leq n$ dan

$$K = K_1 + K_2 + \cdots + K_n.$$

Maka

$$K = K_1 \oplus K_2 \oplus \cdots \oplus K_n.$$

Bukti Tinjau sebarang elemen $x \in K$. Bila

$$x = k_1 + k_2 + \cdots + k_n = k_1' + k_2' + \cdots + k_n',$$

dimana $k_i, k_i' \in K_i$ untuk semua $i,\ 1 \leq i \leq n$ dan karena K_i subgrup dari H_i, maka $k_i, k_i' \in H_i$. Juga karena $G = H_1 \oplus H_2 \oplus \cdots \oplus H_n$, maka haruslah $k_i = k_i'$ untuk semua $i,\ 1 \leq i \leq n$. Jadi

$$K = K_1 \oplus K_2 \oplus \cdots \oplus K_n. \quad \checkmark$$

Proposisi 4.3.1 Misalkan G suatu grup komutatif sedemikian hingga

$$G = H_1 \oplus \cdots \oplus H_n,$$

K_i adalah subgrup dari H_i untuk semua $i,\ 1 \leq i \leq n$ dan

$$K = K_1 + \cdots + K_n.$$

Maka

$$G/K = G/(K_1 \oplus \cdots \oplus K_n) \cong H_1/K_1 \times \cdots \times H_n/K_n.$$

Bukti Dari Lemma 4.3.2 didapat

$$K = K_1 \oplus \cdots \oplus K_n.$$

definisikan pemetaan $\phi : G \to H_1/K_1 \times \cdots \times H_n/K_n$ oleh

$$\phi(x) = \phi(h_1 + \cdots + h_n) = (h_1 + K_1, \ldots, h_n + K_n), \ \forall x \in G,$$

dimana $x = h_1 + \cdots + h_n$ dengan $h_i \in H_i$ untuk semua i, $1 \leq i \leq n$. Karena representasi sebarang x di G adalah tunggal, maka pemetaan ϕ terdefinisi secara baik. Pemetaan ϕ adalah suatu homomorpisma, sebab untuk sebarang $x = h_1 + \cdots + h_n$ dan $x' = h'_1 + \cdots + h'_n$ di G didapat

$$\begin{aligned}
\phi((h_1 + \cdots + h_n) + (h'_1 + \cdots + h'_n)) &= \phi((h_1 + h'_1) + \cdots + (h_n + h'_n) \\
&= ((h_1 + h'_1) + K_1, \ldots, (h_n + h'_n) + K_n) \\
&= (h_1 + K_1, \ldots, h_n + K_n) + (h'_1 + K_1, \ldots, h'_n + K_n) \\
&= \phi((h_1 + \cdots + h_n)) + \phi((h'_1 + \cdots + h'_n)).
\end{aligned}$$

Elemen netral $H_1/K_1 \times \cdots \times H_n/K_n$ adalah $(K_1, \ldots, K_n)$. Dengan demikian bila $x = h_1 + \cdots + h_n$, maka $x \in \ker(\phi)$ bila dan hanya bila $h_i + K_i = K_i$ hal ini berarti bahwa $h_i \in K_i$ untuk semua i, $1 \leq i \leq n$. Tetapi kondisi ini ekivalen dengan $x \in K_1 \oplus \cdots \oplus K_n$. Jadi $\ker(\phi) = K_1 \oplus \cdots \oplus K_n = K$. Pemetaan ϕ adalah pada, sebab diberikan sebarang $y = (h_1 + K_1, \ldots, h_n + K_n)$ di $H_1/K_1 \times \cdots \times H_n/K_n$, dapat dipilih $x = h_1 + \cdots + h_n$ di G yang memenuhi

$$\phi(x) = \phi(h_1 + \cdots + h_n) = (h_1 + K_1, \ldots, h_n + K_n) = y.$$

Dengan menggunakan teorema isomorpisma pertama didapat

$$G/\ker(\phi) \cong H_1/K_1 \times \cdots \times H_n/K_n$$

atau

$$G/K = G/(K_1 \oplus \cdots \oplus K_n) \cong H_1/K_1 \times \cdots \times H_n/K_n.$$

Pengkonstruksian jumlahan langsung yang telah dibahas pada bagian ini adalah suatu yang esensial untuk pengkajian grup komutatif berhingga dan dibahas pada bagian berikutnya.

Latihan

Latihan 4.3.1 Dapatkan subgrup sejati tak-trivial H dan K dari grup G berikut yang memenuhi $G \cong H \oplus K$.
1. $\mathbb{Z}_{10}$. 2. $\mathbb{Z}_{15}$. 3. $\mathbb{Z}_{18}$. 4. $\mathbb{Z}_{20}$. 5. $\mathbb{Z}_{36}$.

Latihan 4.3.2 Jelaskan mengapa tidak ada subgrup sejati tak-trivial H dan K dalam $\mathbb{Z}_9$ yang memenuhi $\mathbb{Z}_9 = H \oplus K$.

Latihan 4.3.3 Jelaskan mengapa tidak ada subgrup sejati tak-trivial H dan K dalam $\mathbb{Z}_8$ yang memenuhi $\mathbb{Z}_8 = H \oplus K$.

Latihan 4.3.4 Bila mungkin dapatkan subgrup sejati tak-trivial H_1, H_2, H_3 dalam $\mathbb{Z}_{60}$ yang memenuhi $\mathbb{Z}_{60} = H_1 \oplus H_2 \oplus H_3$.

Latihan 4.3.5 Jelaskan mengapa tidak ada subgrup sejati tak-trivial H_1, H_2 dan H_3 dalam $\mathbb{Z}_{36}$ yang memenuhi $\mathbb{Z}_{36} = H_1 \oplus H_2 \oplus H_3$.

Latihan 4.3.6 Dapatkan subgrup sejati tak-trivial H dan K dalam $\mathbb{U}(12)$ yang memenuhi $HK = \mathbb{U}(12)$.

Latihan 4.3.7 Dapatkan subgrup sejati tak-trivial H dan K dalam $\mathbb{U}(15)$ yang memenuhi $HK = \mathbb{U}(15)$.

Latihan 4.3.8 Tunjukkan bahwa tidak ada subgrup sejati tak-trivial H dan K dalam $\mathbb{U}(10)$ yang memenuhi $HK = \mathbb{U}(10)$.

Latihan 4.3.9 Misalkan H dan K adalah subgrup dari grup G yang memenuhi $G = H \oplus K$, dimana H siklik berorder 4 dan K siklik berorder 35. Tunjukkan bahwa $G \cong \mathbb{Z}_{140}$.

Latihan 4.3.10 Misalkan H dan K adalah subgrup dari grup G yang memenuhi $G = H \oplus K$, dimana H siklik berorder 6 dan K siklik berorder 15. Tunjukkan bahwa G suatu grup komutatif tidak siklik berorder 90.

Latihan 4.3.11 Misalkan G suatu grup berhingga dan H_i, untuk $i,\ 1 \leq i \leq n$ adalah subgrup dari G yang memenuhi

(1) $H_i \lhd G$ untuk semua $i,\ 1 \leq i \leq n$.

(2) $(H_1 H_2 \cdots H_{i-1}) \cap H_i = \{e\}$ untuk semua $i,\ 2 \leq i \leq n$.

(3) $|G| = |H_1|\,|H_2| \cdots |H_n|$.

Tunjukkan bahwa $G = H_1 \oplus H_2 \oplus \cdots \oplus H_n$.

Latihan 4.3.12 Misalkan $G = H_1 \oplus H_2 \oplus \cdots \oplus H_n$ dan $x = h_1 + h_2 + \cdots + h_n \in G$. Tunjukkan bahwa $|x| = \text{kpk}(|h_1|, |h_2|, \ldots, |h_n|)$.

Latihan 4.3.13 Misalkan $G = H \oplus K$ dimana H siklik berorder n dan K berorder m. Tunjukkan bahwa $G \cong \mathbb{Z}_{nm}$ bila dan hanya bila $\text{kpk}(n, m) = 1$.

Latihan 4.3.14 Misalkan $G = \mathbb{Z}_6 \times \mathbb{Z}_8$ dan didefinisikan suatu pemetaan $\phi : G \to \mathbb{Z}_3 \times \mathbb{Z}_4$ oleh $\phi((h_1, h_2)) = ([h_1]_3, [h_2]_4)$ untuk sebarang $h_1 \in \mathbb{Z}_6$ dan $h_2 \in \mathbb{Z}_8$.

(a) Tunjukkan bahwa ϕ suatu homomorpisma.

(b) Dapatkan $\ker(\phi)$

(c) Dapatkan $\text{Im}(\phi) = \phi(G)$.

Latihan 4.3.15 Misalkan H dan K adalah subgrup dari suatu grup komutatif G dan $\phi : G \to H$ adalah suatu homomorpisma yang memenuhi

(1) $\phi(h) = h$ untuk semua $h \in H$.

(2) $\ker(\phi) = K$.

Tunjukkan bahwa $G = H \oplus K$.

Latihan 4.3.16 Misalkan H dan K adalah subgrup dari suatu grup komutatif G dan $\phi : G \to H$ adalah suatu homomorpisma yang memenuhi

(1) $\phi(h) = h$ untuk semua $h \in H$.

(2) $\ker(\phi) = K$.

Tunjukkan bahwa ada suatu homomorpisma $\psi : G \to K$ yang memenuhi

(1) $\psi(k) = k$ untuk semua $k \in K$.

(2) $\ker(\psi) = H$.

Latihan 4.3.17 Misalkan H dan K adalah subgrup dari suatu grup komutatif G. Tunjukkan bahwa $G = H \oplus K$ bila dan hanya bila ada suatu homomorpisma $\phi : G \to H$ yang memenuhi

(1) $\phi(h) = h$ untuksemua $h \in H$.

(2) $\ker(\phi) = K$.

Latihan 4.3.18 Misalkan H dan K adalah subgrup normal dari suatu grup G dan $\phi : G \to H$ adalah suatu homomorpisma yang memenuhi

(1) $\phi(h) = h$ untuk semua $h \in H$.

(2) $\ker(\phi) = K$.

Tunjukkan bahwa $G \cong H \times K$.

Latihan 4.3.19 Misalkan G adalah suatu grup komutatif dan $\phi : G \to G$ adalah suatu homomorpisma yang memenuhi $\phi(\phi(g)) = g$ untuk semua $g \in G$ (homomorpisma ini dinamkan suatu **proyeksi**). Tunujkkan bahwa $G \cong \phi(G) \times \ker(\phi)$.

Latihan 4.3.20 Misalkan G adalah suatu grupdengan $|G| = nm$ dimana kpk$(n, m) = 1$. Asumsikan bahwa G mempunyai tepat satu subrup H berorder n dan mempunyai tepat satu subgrup K berorder m. Tunjukkan bahwa $G \cong H \times K$.

Latihan 4.3.21 Tunjukkan bahwa setiap grup berorder 9 adalah komutatif.

Latihan 4.3.22 Tunjukkan bahwa setiap grup berorder p^2 adalah komutatif untuk bilangan prima p.

4.4 Teorema Fundamental dari Grup Abelian Berhingga

Pada bagian ini ditunjukkan grup komutatif berhingga secara lengkap dapat diuraikan dalam istilah produk langsung dari beberapa grup siklik. Dimulai dengan mendaftar semua grup komutatif dari suatu grup berhingga yang diberikan. Karena telah diketahui bagaimana mengkonstruksi subgrup dari grup siklik dan bagaimana menghitung order elemen dalam grup siklik hal ini akan bisa dilakukan yang sama untuk sebarang grup komutatif berhingga.

Telah diketahui bahwa grup siklik G dengan $|G| = n$ isomorpik dengan $\mathbb{Z}_n$ dan produk langsung dari grup $\mathbb{Z}_n \times \mathbb{Z}_m$ adalah suatu grup komutatif. Teorema yang akan dibuktikan membahas bahwa sebarang grup komutatif somorpik dengan suatu produk langsung dari grup siklik.

Contoh 4.4.1 Misalkan G adalah suatu grup komutatif dengan $|G| = 24$, $H = \{x \in G \,|\, |x| = 1, 2, 4 \text{ atau } 8\}$ dan $K = \{x \in G \,|\, |x| = 1 \text{ atau } 3\}$. Karena G komutatif digunakan penjumlahan sebagai operasi. Perlu diperhatikan bahwa H dan K keduanya subgrup dari G. Hal ini bisa terlihat sebagai berikut, $x \in H$ bila hanya $8x = 0$, jadi bila $x, y \in H$, maka $8(x - y) = 8x - 8y = 0 - 0 = 0$. Dengan demikian $x - y \in H$, jadi H subgrup dari G. Sejalan dengan hal ini, untuk $x \in K$ bila hanya $3x = 0$, jadi bila $x, y \in K$, maka $3(x - y) = 3x - 3y = 0 - 0 = 0$. Dengan demikian $x - y \in K$, jadi K subgrup dari G. Selanjutnya untuk sebarang $g \in G$, karena $1 = 2(8) - 5(3)$ didapat $g = (2(8) - 5(3))g = 2(8g) - 5(3g)$. Karena $|G| = 24$, maka dengan Teorema Lagrange didapat $3(16g) = 0$ dan $16g \in K$ begitu juga $8(15g) = 0$ dan $15g \in H$. Jadi $g \in H + K$ dan $H + K = G$. Karena $H \cap K = \{0\}$, maka $G = H \oplus K$ dan $24 = |G| = |H||K|$. Juga dari Teorema 3.4.4, 3 tidak membagi $|H|$, sebab bila tidak maka H mempunyai elemen yang berorder 3. Hal yang sama, juga 2 tidak membagi $|K|$. Jadi $|H| = 8$ dan $|K| = 3$. ●

Proposisi 4.4.1 Misalkan G suatu grup berhingga berorder $p^r\, m$ dimana p prima tidak membagi m. Misalkan $H = \{x \in G \,|\, |x| = p^s, 0 \leq s \leq r\}$ dan $K = \{x \in G \,|\, |x| \text{ mebagi } m\}$. Maka

(1) $G = H \oplus K$.

(2) $|H| = p^r$ dan $|K| = m$.

Bukti

(1) Pertama ditunjukkan bahwa H dan K keduanya subgrup dari G. Untuk $x \in H$ bila dan hanya bila $p^r x =$. Jadi bila $x, y \in H$, maka $p^r(x - y) = p^r x - p^r y = 0 - 0 = 0$ dan $x - y \in H$. Dengan demikian H adalah subgrup dari G. Untuk $x \in K$ bila dan hanya bila $mx =$. Jadi bila $x, y \in H$, maka $m(x - y) = mx - my = 0 - 0 = 0$ dan $x - y \in K$. Dengan demikian K adalah subgrup dari G. Karena p^r dan m prima relatif, maka dengan menggunakan Teorema 1.3.6 didapat $1 = up^r + vm$ untuk beberapa bilangan bulat u dan v. Dengan demikian untuk sebarang $g \in G$ didapat

$$g = 1(g) = (up^r + vm)g = (up^r)g + (vm)g.$$

Karena $|G| = p^r m$, didapat $p^r(vm)g = 0$ hal ini berakibat $(vm)g \in H$ dan $m(up^r)g = 0$ hal ini berakibat $(up^r)g \in K$. Jadi $G = H + K$. Selanjutnya bila $x \in H \cap K$, maka order dari x harus membagi p^r dan m dengan demikian juga membagi kpk$(p^r, m) = 1$. Jadi $|x| = 1$ dengan demikian $x = 0$, didapat $H \cap K = \{0\}$. Krena $G = H + K$ dan $H \cap K = \{0\}$, maka $G = H \oplus K$.

(2) Grup G adalah komutatif, maka subgrup K adalah komutatif. Dengan menggunakan Teorema 3.4.4 (Teorema Cauchy) didapat bila p membagi $|K|$, maka K memuat suatu elemen berorder p, hal ini tidak mungkin terjadi. Jadi p tidak membagi $|K|$. Sejalan dengan hal ini didapat $|H|$ tidak dapat dibagi oleh bilangan prima selain p. Karena $|G| = p^r\, m$ dan $|G| = |H||K|$, maka yang mungkin adalah $|H| = p^r$ dan $|K| = m$. ✓

Contoh 4.4.2 Misalkan G adalah suatu grup komutatif berorder $900 = 4(9)(25) = 2^2\, 3^2\, 5^2$, $H = \{x \in G \,|\, |x| = 1, 2, \text{ atau } 4\}$ dan $K = \{x \in G \,|\, |x| \text{ membagi } 3^2 5^2 = 225\}$. Maka dengan menggunakan Proposisi 4.4.1 didapat $G = H \oplus K$. Selanjutnya, misalkan $L = \{x \in G \,|\, |x| = 1, 3, \text{ atau } 9\}$ dan $M = \{x \in G \,|\, |x| = 1, 5, \text{ atau } 25\}$. Lagi dengan menggunakan Proposisi 4.4.1 didapat $K = L \oplus M$. Jadi $G = H \oplus L \oplus M$. ●

Diberikan G suatu grup komutatif dengan $|G| = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, dimana p_i adalah bilangan prima yang berbeda untuk i, $1 \le i \le k$. Misalkan $G(p_i^{a_i}) = \{x \in G \,|\, |x| = p_i^s, 0 \le s \le a_i\}$. Suatu akibat langsung dari Proposisi 4.4.1 didapat kesimpulan berikut.

Akibat 4.4.1 Misalkan G adalah suatu grup komutatif dengan $|G| = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, dimana p_i adalah bilangan prima yang berbeda untuk semua i, $1 \le i \le k$. Maka

(1) $G = G(p_1^{a_1}) \oplus G(p_2^{a_2}) \oplus \cdots \oplus G(p_k^{a_k})$.

(2) $|G(p_i^{a_i})| = p_i^{a_i}$, untuk semua i, $1 \le i \le k$.

Bukti Hal ini langsung dari Proposisi 4.4.1.

Definisi 4.4.1 Diberikan G suatu grup komutatif berhingga dan p bilangan prima. Maka G dinamakan suatu p**-grup** bila $|G| = p^r$ untuk beberapa bilangan bulat r.

Akibat 4.4.1 menyatakan bahwa sebarang grup komutatif berhingga dapat didekomposisi sebagai jumlahan langsung dari p-grup. Dalam pembahasan berikutnya ditunjukkan bahwa setiap grup komutatif berhingga adalah suatu jumlahan langsung grup siklik melalui p-grup dan ditunjukkan bahwa setiap p-grup adalah jumlahan langsung dari grup siklik.

Pembuktian proposisi berikut merupakan kerja keras, untuk itu sebelumnya diberikan suatu contoh yang menguraikan ide yang tercakup didalam suatu kasus ringkas dan sederhana.

Contoh 4.4.3 Diberikan G grup komutatif berorder 8, $a \in G$ suatu elemen yang berorder maksimal, yaitu suatu elemen yang memenuhi $|x| \le |a|$ untuk semua $x \in G$. Didapat $|a| = 8, 4$ atau 2.

Kasus 1 Untuk $|a| = 8$, maka $G = \langle a \rangle \cong \mathbb{Z}_8$.

Kasus 2 Untuk $|a| = 4$. Maka $H = \langle a \rangle$ adalah suatu subgrup sejati dari G. Pilih $b \in G, b \notin \langle a \rangle$ adalah suatu elemen di G yang berorder minimal yaitu $|y| \ge |b|$ untuk setiap $y \in G$ dan $y \notin \langle a \rangle$. Bila $|b| = 4$, maka H dan $K = \langle b \rangle$ akan mempunyai elemen yang berorder 2. Sehingga didapat $2a = 2b$ hal ini berakibat $|a + b| = 2$. Karena $a + b \notin \langle a \rangle$, maka suatu hal yang tidak mungkin $|a + b| = 2$ sebab b telah diplih dengan order minimal. Jadi haruslah $|b| = 2$ dan $H \cap K = \{0\}$. Dalam kasus ini maka $G = H \oplus K \cong \mathbb{Z}_4 \oplus \mathbb{Z}_2$.

Kasus 3 Untuk $|a| = 2$. Maka, pilih $b \in G$ dengan $b \notin \langle a \rangle$ didapat $|b| = 2$. Misalkan $H = \langle a \rangle$ dan $K = \langle b \rangle$. Maka $H \cap K = \{0\}$ dan $|H \oplus K| = 4$. Selanjutnya pilih elemen $c \in G$ dengan $c \notin H \oplus K$. Didapat $|c| = 2$ dan bila $L = \langle c \rangle$, maka $(H \oplus K) \cap L = \{0\}$ dan $G = H \oplus K \oplus L \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Dalam Contoh 4.4.3 telah ditunjukkan bagaimana mendapatkan semua grup komutatif berorder 8 dan didapat ada tepat tiga macam grup yang berbeda sesuai dengan pengertian isomorpisma. Pada saat yang sama dalam Contoh 4.4.3 dijelaskan dua ide utama yang akan diberikan dalam proposisi berikut, yaitu mengenai pilihan suatu elemen a dengan order maksimal dan suatu elemen $b \notin \langle a \rangle$ dengan order terkecil.

Proposisi 4.4.2 Diberikan p adalah bilangan bulat prima dan G adalah suatu p-grup komutatif berhingga. Misalkan a suatu elemen di G dengan order maksimal. Maka $G = \langle a \rangle \oplus H$ untuk beberapa H subgrup dari G.

Bukti Misalkan $G = p^n$. Digunakan induksi pada n. Bila $n = 1$, maka G siklik dan $G = \langle a\rangle \oplus \langle 0\rangle$. Jadi asumsikan proposisi benar untuk semua grup komutatif berorder p^k dimana $k < n$. Misalkan $a \in G$ elemen berorder maksimal, jadi $|a| = p^r$ dimana $r \leq n$ dan $|x| \leq p^r$ untuk semua $x \in G$. Catatan bila $r = n$, maka $G = \langle a\rangle$ dan bukti selesai. Jadi misalkan $r < n$ dan pilih $b \in G$ adalah elemen dengan order minimal dan $b \notin \langle a\rangle$. Hal ini berarti bila $x \in G$ dan $|x| < |b|$, maka $x \in \langle a\rangle$. Selanjutnya ditunjukkan bahwa $\langle a\rangle \cap \langle b\rangle = \{0\}$. Tinjau elemen $pb \in G$, maka $|pb| = |b|/\text{fpb}(|b|, p) = |b|/p < |b|$, jadi $pb \in \langle a\rangle$ akibatnya $pb = ma$ untuk beberapa bilangan bulat m. Karena $|a| = p^r$ dan a dipilih dengan order maksimal, maka $0 = p^r b = p^{r-1}(pb) = p^{r-1}(ma)$. Jadi $|ma| \leq p^{r-1}$ dan ma bukan generator dari $\langle a\rangle$. Dengan menggunakan Akibat 2.3.4 didapat $\text{fpb}(p^r, m) \neq 1$, jadi p membagi m. Misalkan $m = ps$, didapat $pb = ma = psa$. Tinjau elemen $-sa + b \in G$, jelas bahwa $p(-sa + b) = 0$. Karena $b \notin \langle a\rangle$, maka $-sa + b \notin \langle a\rangle$. Jadi $|-sa + b| = p$. Karena dipilih $b \in G$ dan $b \notin \langle a\rangle$ dengan order minimal, maka haruslah $|b| = p$. Dengan demikian $\langle a\rangle \cap \langle b\rangle = \{0\}$. Tinjau grup kuasi $G' = G/\langle b\rangle$. Karena $|G'| = p^{n-1}$, dengan menggunakan hipotesis induksi, proposisi dipenuhi untuk G'. Misalkan $a' = a + \langle b\rangle \in G'$. Order elemen a' adalah bilangan bulat positip k yang memenuhi $ka \in \langle b\rangle$. Karena $\langle a\rangle \cap \langle b\rangle = \{0\}$,maka $|a'| = |a|$. Misalkan homomorpisma $\phi : G \to G/\langle b\rangle = G'$, dimana $\phi(a) = a'$, $\forall a \in G$. Dengan menggunakan Proposisi 3.2.2 bagian (4) didapat a' adalah pembangun dari G'. Akibatnya a' adalah elemen di G' dengan order maksimal. Jadi dengan hipotesis induksi didapat $G' = \langle a'\rangle \oplus H'$ untuk beberapa H' subgrup dari G'. Selanjutnya, misalkan $H = \phi^{-1}(H')$, maka dengan Proposisi 3.2.2 bagian (6) didapat H adalah subgrup dari G dengan $H/\langle b\rangle = H'$. Jadi $|H| = |H'|p$ dan

$$|G| = |G'|\,|\langle b\rangle| = |G'|p = |\langle a'\rangle|\,|H'|\,p = p^r|H'|p = p^r|H| = |\langle a\rangle|\,|H|.$$

Akhirnya untuk menunjukkan $G = \langle a\rangle \oplus H$, dengan menggunakan Akibat 4.3.1 cukup ditunjukkan $\langle a\rangle \cap H = \{0\}$. Untuk itu, misalkan $x \in \langle a\rangle \cap H$. Karena$G' = \langle a'\rangle \oplus H'$, maka $x + \langle b\rangle \in \langle a'\rangle \cap H' = \{\langle b\rangle\}$. Jadi $x \in \langle b\rangle$, akibatnya $x \in \langle a\rangle \cap \langle b\rangle$. Karena $\langle a\rangle \cap \langle b\rangle = \{0\}$, maka $x = 0$. Jadi $\langle a\rangle \cap H = \{0\}$, dengan demikian $G = \langle a\rangle \oplus H$. ✓

Bukti Proposisi 4.4.2 cukup panjang, tetapi akan terlihat dalam contoh berikut betapa berdaya gunanya proposisi ini yang berkaitan dengan langkah-langkah yang telah dibahas.

Contoh 4.4.4 Diberikan G suatu grup komutatif dengan $|G| = 27 = 3^3$ dan misalkan $a \in G$ suatu elemen dengan order maksimal. Maka $|a| = 3, 3^2$ atau 3^3.

Kasus 1 $|a| = 3^3$, maka $G \cong \mathbb{Z}_{27}$.

Kasus 2 $|a| = 3^2$, maka $G = \langle a\rangle \oplus H$, dimana H adalah subgrup dari G. Dalam kasus ini didapat $G \cong \mathbb{Z}_9 \times \mathbb{Z}_3$.

Kasus 3 $|a| = 3$, maka $G \cong \langle a\rangle \oplus H$, dimana H suatu subgrup berorder 9. Karena $a \in G$ berordre maksimal, maka H tidak akan mempunyai elemen yang berorder lebih besar dari 3. Gunakan Proposisi 4.4.2 pada H, didapat $H \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Jadi $G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.

Catatan, $\mathbb{Z}_{27}$ tidak isomorpik dengan $\mathbb{Z}_9 \times \mathbb{Z}_3$ dan $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. ●

Proposisi 4.4.3 Misalkan p bilangan bulat prima dan G suatu p-grup berhingga. Maka

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_s,$$

dimana masing-masing G_i adalah siklik dan $|G_1| \geq |G_2| \geq \cdots \geq |G_2|$.

Bukti Digunakan induksi pada $|G|$. Bila $|G| = 1, 2$ atau 3, maka tidak ada yang peluh dibuktikan. Jadi diasumsikan proposisi benar untuk semua grup komutatif berhingga berorder lebih kecil dari $|G|$. Dengan menggunakan Proposisi 4.4.2 didapat $G = \langle a_1 \rangle \oplus H$, dimana $a_1 \in G$ berorder maksimal. Jadi bila $a_2 \in H$ berorder maksimal, maka $|a_1| \geq |a_2|$. Misalkan $G_1 = \langle a_1 \rangle$, dan gunakan hipotisisi induksi pada H didapat $H = G_2 \oplus \cdots \oplus G_s$, dimana masing-masing G_i adalah siklik dan $|G_2| \geq \cdots \geq |G_s|$. Dengan demikian didapat

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_s,$$

dimana masing-masing G_i adalah siklik dan $|G_1| \geq |G_2| \geq \cdots \geq |G_2|$. ✓

Contoh 4.4.5 Misalkan G dan H grup komutatif berorder 2^4. Misalkan, $G = G_1 \oplus G_2$, dimana G_1 dan G_2 siklik berorder 4, jadi $G \cong \mathbb{Z}_4 \times \mathbb{Z}_4$. Misalkan, $H = H_1 \oplus H_2 \oplus H_3$ dimana H_1 adalah siklik berorder 4, H_2 dan H_3 siklik berorder 2, jadi $H \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Selanjutnya, dihitung banyaknya elemen-elemen berorder 1 atau 2 di G dan di H. Misalkan $G^{(2)} = \{x \in G \,|\, |x| = 1 \text{ atau } 2\}$. Bila $x, y \in G^{(2)}$, maka $2(x - y) = 2x - 2y = 0 - 0 = 0$, jadi $(x - y) \in G^{(2)}$. Dengan demikian $G^{(2)}$ adalah subgrup dari G. Bila $x = g_1 + g_2$, dimana $g_1 \in G_1$ dan $g_2 \in G_2$, maka dengan menggunakan Akibat 4.3.3 didapat $|x|$ membagi 2 bila dan hanya bila $|g_1|$ dan $|g_2|$ keduanya membagi 2. Hal ini berarti $G^{(2)} = G_1^{(2)} + G_2^{(2)}$, dimana $G_i^{(2)} = G^{(2)} \cap G_i = \{x \in G_i \,|\, |x| = 1 \text{ atau } 2\}$. Dengan menggunakan Lemma 4.3.2, maka jumlahan $G^{(2)} = G_1^{(2)} + G_2^{(2)}$ adalah jumlahan langsung dengan menggunakan Akibat 4.3.2 didapat $\left|G^{(2)}\right| = \left|G_1^{(2)}\right| \left|G_2^{(2)}\right|$. Tetapi himpunan elemen-elemen berorder 1 atau 2 dalam suatu grup siklik dengan order membagi 2 adalah suatu grup siklik tunggal berorder 2. Jadi $\left|G_1^{(2)}\right| = \left|G_2^{(2)}\right| = 2$ dan $\left|G^{(2)}\right| = 2^2$. Dengan cara perhitungan yang sama, didapat bila $H^{(2)} = \{x \in G \,|\, |x| = 1 \text{ atau } 2\}$, maka $\left|H^{(2)}\right| = \left|H_1^{(2)}\right| \left|H_2^{(2)}\right| \left|H_3^{(2)}\right| = 2^3$.Karena banyaknya himpunan dalam $G^{(2)}$ dan $H^{(2)}$ yang elemen-elemennya berorder 2 tidak sama, maka G dan H tidak akan isomorpik. Jadi $\mathbb{Z}_4 \times \mathbb{Z}_4$ tidak isomorpik dengan $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. ●

Contoh 4.4.6 Misalkan $G = G_1 \oplus G_2 \oplus G_3$ dengan $G_1 \cong \mathbb{Z}_8, G_2 \cong \mathbb{Z}_4$ dan $G_3 \cong \mathbb{Z}_4$. Juga, misalkan $H = H_1 \oplus H_2 \oplus H_3$ dengan $H_1 \cong \mathbb{Z}_8, H_2 \cong \mathbb{Z}_8$ dan $H_3 \cong \mathbb{Z}_2$. Selanjutnya, misalkan $G^{(2)} = \{x \in G \,|\, |x| = 1 \text{ atau } 2\}$ dan $H^{(2)} = \{x \in H \,|\, |x| = 1 \text{ atau } 2\}$. Maka, suatu perhitungan seperti dilakukan dalam contoh sebelumnya menunjukkan bahwa $\left|G^{(2)}\right| = 2^3$ dan $\left|H^{(2)}\right| = 2^3$. Dengan demikian tidak bisa dibedakan elemen-elemen berorder 2 dalam G dan H. Apapun hal ini, tinjau grup kuasi $G/G^{(2)}$ dan gunakan Proposisi 4.3.1 didapat

$$G/G^{(2)} = G_1/G_1^{(2)} \oplus G_2/G_2^{(2)} \oplus G_3/G_3^{(2)},$$

dimana sebagaimana dalam contoh sebelumnya

$$G_i^{(2)} = G^{(2)} \cap G_i = \{x \in G_i \,|\, |x| = 1 \text{ atau } 2\}$$

adalah subgrup siklik dari G_i berorder 2 dan $\left|G_i/G_i^{(2)}\right| = |G_i|/2$. Jadi $G/G^{(2)} \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Dengan argumen yang sama didapat $H/H^{(2)} \cong \mathbb{Z}_4 \times \mathbb{Z}_4 \times \{0\} \cong \mathbb{Z}_4 \times \mathbb{Z}_4$. Sebagaimana dalam contoh sebelumnya, maka $G/G^{(2)}$ dan $H/H^{(2)}$ tidak akan isomorpik. Dengan demikian G dan H tidak isomorpik. Jadi $\mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_4 \ncong \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_2$. ●

Proposisi 4.4.4 Misalkan p bilangan bulat prima dan G adalah p-grup komutatif berhingga. Bila

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_r \text{ dan } G = H_1 \oplus H_2 \oplus \cdots \oplus H_s,$$

dimana G_i dan H_i adalah siklik dengan

$$|G_1| \geq |G_2| \geq \cdots \geq |G_r| \text{ dan } |H_1| \geq |H_2| \geq \cdots \geq |H_s|.$$

Maka

(1) $r = s$.

(2) $G_i \cong H_i$.

Bukti

(1) Misalkan $G^{(p)} = \{x \in G \,|\, |x| = 1 \text{ atau } p\}$ dan untuk sebarang K subgrup dari G $K \cap G^{(p)} = \{x \in K \,|\, |x| = 1 \text{ atau } p\}$. Bila $x, y \in G^{(p)}$, maka $p(x-y) = px - py = 0 - 0 = 0$. Jadi $(x-y) \in G^{(p)}$, dengan demikian $G^{(p)}$ suatu subgrup dari G. Bila $x = g_1 + g_2 + \cdots + g_r$, dimana $g_i \in G_i$ untuk semua i, $1 \leq i \leq r$, maka dengan Akibat 4.3.3 $|x|$ membagi p bila dan hanya bila $|g_i|$ membagi p untuk semua i. Hal ini berarti $G^{(p)} = G_1^{(p)} + G_2^{(p)} + \cdots + G_r^{(p)}$ dengan menggunakan Lemma 4.3.2, maka jumlahan tersebut adalah jumlahan langsung. Dengan menggunakan Akibat 4.3.2 didapat $\left|G^{(p)}\right| = \left|G_1^{(2)}\right| \left|G_2^{(p)}\right| \left|G_r^{(p)}\right|$. Tetapi himpunan elemen-elemen berorder 1 atau p dalam suatu grup siklik dengan order membagi p adalah suatu subgrup siklik tunggal berorder p. Jadi $\left|G_i^{(p)}\right| = p$ untuk semua i dan $\left|G^{(p)}\right| = p^r$. Sejalan dengan perhitungan ini untuk G_i diganti H_i didapat $\left|G^{(p)}\right| = p^s$. Akibatnya $p^r = p^s$, jadi $r = s$.

(2) Untuk menunjukkan $G_i \cong H_i$ untuk semua i, $1 \leq i \leq r$ digunakan induksi pada n, dimana $|G| = p^n$. Bila $n = 1$, maka G adalah siklik dengan demikian tidak ada yang dibuktikan. Misalkan proposisi benar untuk semua p-grup komutatif berorder p^r dengan $r < n$. Tinjau grup kuasi $G/G^{(p)}$, dengan menggunakan Proposisi 4.3.1 didapat

$$G/G^{(p)} \cong G_1/G_1^{(p)} \oplus G_2/G_2^{(p)} \oplus \cdots \oplus G_r/G_r^{(p)}$$

dan

$$G/G^{(p)} \cong H_1/H_1^{(p)} \oplus H_2/H_2^{(p)} \oplus \cdots \oplus H_r/H_r^{(p)}.$$

Terlihat ada dua dekomposisi dari p-grup komutatif $G/G^{(p)}$ dimana ordernya lebih kecil dari p^n. Dengan hipotesis induksi $G_i/G_i^{(p)} \cong H_i/H_i^{(p)}$ untuk semua i. Sebagaimana telah dibuktikan pada bagian (1) bahwa $\left|G_i^{(p)}\right| = \left|H_i^{(p)}\right| = p$ untuk semua i, jadi $|G_i| = |H_i|$ dan karena G_i dan H_i siklik, maka $G_i \cong H_i$ untuk semua i. ✓

Sebagai ringkasan dari apa yang telah dibahas baik dari beberapa contoh, proposisi dan kesimpulan diberikan teorema berikut sehingga bukti dengan mudah didapat.

Teorema 4.4.1 (**Fundamental Grup Komutatif Berhingga**) Misalkan G adalah suatu grup komutatif berhingga. Maka

(1) $G \cong \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_s^{a_s}}$, dimana p_i adalah prima tidak perlu berbeda.

(2) Produk langsung adalah tunggal, kecuali urutan dari faktor.

Bukti Misalkan G grup komutatif berhingga dimana

$$|G| = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Maka dengan menggunakan Akibat 4.4.1 didapat

$$G \cong G(p_1^{a_1}) \oplus G(p_2^{a_2}) \oplus \cdots \oplus G(p_k^{a_k}),$$

dimana $\left|G(p_i^{a_i})\right| = p_i^{a_i}$. Dengan menggunakan Proposisi 4.4.3 didapat

$$G(p_i^{a_i}) \cong \mathbb{Z}_{p_i^{t_1}} \times \mathbb{Z}_{p_i^{t_2}} \times \cdots \times \mathbb{Z}_{p_i^{t_s}},$$

dimana $a_i = t_1 + t - 2 + \cdots + t_2$. Dengan demikian telah terbukti bagian (1). Bukti bagian (2) didapat dari Proposisi 4.4.4. ✓

Contoh 4.4.7 Akan ditentukan semua grup komutatif berorder 180 yang berbeda dengan makna isomorpik. Untuk grup G yang demikian didapat $G \cong \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$, dimana $|G| = 180 = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ dan p_i adalah bilangan bulat prima yang tidak harus berbeda. Dalam hal ini $180 = 2^2\, 3^2\, 5$. Jadi G adalah grup yang isomorpik dengan grup-grup berikut

$$\begin{aligned}
G &\cong \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_{180} \\
G &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{90} \\
G &\cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_{60} \\
G &\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_6 \times \mathbb{Z}_{30}.
\end{aligned}$$

Catatan bahwa hasil dari semua grup-grup yang tidak saling isomorpik, digunakan teorema fundamental grup komutatif dan Teorema 4.2.2 yaitu $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$ bila dan hanya bila fpb$(n, m) = 1$. ●

Diakhir bagian ini, diberikan akibat langsung dari teorema fundamental grup komutatif berhingga.

Definisi 4.4.2 Suatu grup G dikatakan **terdekomposisi** bila G adalah jumlahan langsung dari dua subgrup sejati tak-trivial. Bila tidak dikatakan **tak-terdekomposisi**. ✓

Teorema 4.4.2 Diberikan G suatu grup komutatif berhingga. Maka G tak-terdekomposisi bila dan hanya bila G isomorpik dengan $\mathbb{Z}_{p^r}$ untuk bebarapa bilangan prima p dan bilangan bulat positip r.

Bukti Bila G tak-terdekomposisi, langsung dari Teorema 4.4.1, maka $G \cong \mathbb{Z}_p^r$. Sebaliknya, bila $G \cong \mathbb{Z}_p^r$, maka dengan menggunakan Akibat 4.3.4 G tak-terdekomposisi. ✓

Dalam kasus G suatu grup siklik berhingga, diketahui bahwa bila m membagi $|G|$, maka G mempunyai suatu subgrup tunggal berorder m. Selanjutnya dapat dibuktikan sebagai pembanding untuk grup komutatif berhingga.

Teorema 4.4.3 Bila m membagi order dari suatu grup komutatif berhingga G, maka G mempunyai suatu subgrup berorder m.

Bukti Dari Akibat 4.4.1 didapat didapat $G = G_1 \oplus G_2 \oplus \cdots \oplus G_k$, dimana G_i suatu subgrup siklik yang berorder $p_i^{a_i}$ untuk semua i, $1 \leq i \leq k$ dan $|G| = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Karena m membagi $|G|$, maka m dapat ditulis sebagai $m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ dimana $b_i \leq a_i$ untuk semua i. Untuk masing-masing i subgrup siklik G_i berorder $p_i^{a_i}$ mempunyai suatu subgrup H_i berorder $p_i^{b_i}$. Tinjau jumlahan $H = H_1 + H_2 + \cdots + H_k$, dengan menggunakan Lemma 4.3.2, maka jumlahan tersebut adalah jumlahan langsung, sehingga dengan menggunakan Akibat 4.3.2 didapat $|H| = |H_1||H_2| \cdots |H_k| = m$.

Teorema 4.4.4 Diberikan bilangan bulat $m = p_1 p_2 \cdots p_k$ dimana p_i adalah bilangan prima yang berbeda untuk semua i, $1 \leq i \leq k$. Maka sebarang grup komutatif berorder m adalah siklik.

Bukti Karena $m = p_1 p_2 \cdots p_k$ dimana p_i adalah bilangan prima yang berbeda untuk semua i, $1 \leq i \leq k$, maka dengan menggunakan Teorema 4.4.1 didapat

$$G \cong \mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k},$$

dengan menggunakan Akibat 4.3.4 didapat

$$\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k} \cong \mathbb{Z}_{p_1 p_2 \cdots p_k} = \mathbb{Z}_m.$$

Jadi $G \cong \mathbb{Z}_m$, dengan demikian G adalah siklik.

Latihan

Latihan 4.4.1 Dapatkan semua grup komutatif yang berorder n.

1. $n = 6$
2. $n = 9$
3. $n = 10$
4. $n = 12$
5. $n = 16$
6. $n = 20$
7. $n = 60$
8. $n = 80$
9. $n = 72$
10. $n = 108$.

Latihan 4.4.2 Dapatkan semua grup komutatif yang berorder 32 dan tepat mempunyai dua subgrup berorder 4.

Latihan 4.4.3 Dapatkan semua grup komutatif berorder 32 dan tidak mempunyai elemen berorder 4.

Latihan 4.4.4 Tunjukkan bahwa setiap grup komutatif berorder 6 memuat suatu elemen yang berorder 6.

Latihan 4.4.5 Misalkan p adalah suatu bilangan prima. Tentukan berapa banyak grup komutatif yang berorder p^5.

Latihan 4.4.6 Misalkan p dan q adalah bilangan prima yang berbeda. Tentukan berapa banyak grup komutatif yang mempunyai order berikut.

(a) pq

(b) pq^2

(c) p^2q^2.

Latihan 4.4.7 Misalkan p adalah bilangan prima. Tentukan semua grup komutatif berorder p^n dan memuat suatu elemen berorder p^{n-2}.

Latihan 4.4.8 tentukan apakah pasngan grup berikut isomorpik atau tidak.

(a) $\mathbb{Z}_{180} \times \mathbb{Z}_{42} \times \mathbb{Z}_{35}$ dan $\mathbb{Z}_{315} \times \mathbb{Z}_{140} \times \mathbb{Z}_6$.

(b) $\mathbb{Z}_{20} \times \mathbb{Z}_{70} \times \mathbb{Z}_{14}$ dan $\mathbb{Z}_{28} \times \mathbb{Z}_{28} \times \mathbb{Z}_{25}$.

Latihan 4.4.9 Misalkan p dan q adalah bilangan prima yang berbeda, G grup komutatif berorder n dimana p dan q keduanya membagi n. Tunjukkan bahwa G memuat suatu subgrup siklik berorder pq.

Latihan 4.4.10 Diberikan G adalah suatu grup komutatif berhingga dan p suatu bilangan prima yang memenuhi untuk semua $x \in G, x \neq e$, $|x| = p^r$ untuk beberapa bilangan bulat positip r. Tunjukkan bahwa G adalah suatu p-grup.

Latihan 4.4.11 Misalkan G adalah suatu p-grup komutatif berhingga untuk beberapa bilangan prima p. Tinjau

$$G^{(p)} = \{x \in G \,|\, |x| = 1 \text{ atau } p\},$$

dan misalkan H suatu subgrup siklik tak-trivial dari G. Tunjukkan bahwa

$$\left|G^{(p)} \cap H\right| = p.$$

Latihan 4.4.12 Tentukan semua grup komutatif berorder 625. Untuk masing-masing grup komutatif tersebut, maka

(a) hitung $\left|G^{(5)}\right|$ dimana $G^{(5)} = \{x \in G \,|\, |x| = 1 \text{ atau } 5\}$.

(b) Dapatkan $G/G^{(5)}$.

Latihan 4.4.13 Misalkan G adalah p-grup komutatif berhingga untuk beberapa bilangan prima p. Misalkan $G^{(p)}$ sebagaimana dalam Latihan 4.4.11 dan $pG = \{pg \,|\, g \in G\}$. Tunjukkan bahwa

(a) pG adalah suatu subgrup dari G.

(b) $pG \cong G/G^{(p)}$.

Latihan 4.4.14 Misalkan G_1 dan G_2 grup komutatif berhingga. Tunjukkan bahwa G_1 dan G_2 mepunyai elemen-elemen berorder n dengan jumlah yang sama untuk semua n bila dan hanya bila $G_1 \cong G_2$.

Latihan 4.4.15 Misalkan H dan K adalah p-grup komutatif berhingga. Tunjukkan bahwa $H \times H \cong K \times K$ bila dan hanya bila $H \cong K$.

Bab 5

Tindakan Grup

Dalam bab ini dibahas konsep dari suatu tindakan grup pada suatu himpunan. Hal yang penting dari pengertian ini akan tampak sepanjang bab ini melalui berbagai aplikasi. Hal ini meliputi masalah enumerasi (aplikasi toerema Burnside) dan analisisi struktur grup berorder pq atau p^2q dimana p dan q adalah bilangan prima (aplikasi teorema sylow). Kajian topik ini menggunakan konsep dari tidakan suatu grup.

5.1 Tindakan Grup dan Teorema cayley

Konsep yang dikenalkan dalam bagian ini meliputi dua obyek yaitu suatu grup G dan suatu himpunan $X \neq \emptyset$. Masing-masing elemen dari grup G akan menentukan suatu permutasi dari elemen-elemen himpunan X. Operasi pada X akan sesuai dengan komposisi dari permutasi yang terkait dari X. Contoh berikut secara visual membantu untuk memahami konsep baru ini.

Contoh 5.1.1 Diberikan sebarang $\theta \in \mathbb{R}$, tinjau matriks

$$A(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}.$$

Misalkan $G = \{A(\theta) \mid \theta \in \mathbb{R}\} \subseteq \mathrm{SL}(2, \mathbb{R})$. Dengan operasi perkalian matriks dapat ditunjukkan G adalah subgrup dari $\mathrm{SL}(2, \mathbb{R})$. Misalkan X adalah bidang $\mathbb{R}^2$. Dinyatakan representasi dari suatu titik sebagai suatu vektor kolom dan digunakan koordinat polar:

$$P(r, \phi) = \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} r\cos\theta \\ r\sin\theta \end{bmatrix}.$$

Jadi $X = \{P(r, \phi) \mid r, \phi \in \mathbb{R}, r \geq 0\}$. Untuk sebarang $A(\theta) \in G$ dan sebarang $P(r, \phi) \in X$ didapat

$$\begin{aligned} A(\theta)P(r,\phi) &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} r\cos\theta \\ r\sin\theta \end{bmatrix} \\ &= \begin{bmatrix} r\cos\phi\cos\theta - r\sin\phi\sin\theta \\ r\cos\phi\sin\theta + r\sin\phi\cos\theta \end{bmatrix} \\ &= \begin{bmatrix} r\cos(\phi+\theta) \\ r\sin(\phi+\theta) \end{bmatrix} = P(r, \phi+\theta). \end{aligned}$$

Perlu diperhatikan bahwa, titik $P(r, \phi + \theta)$ diperoleh dari titik $P(r, \phi)$ melalui rotasi bidang pada titik asal dengan sudutsebesar θ. Juga matriks berikut:

(1) Matriks

$$A(0) = \begin{bmatrix} \cos 0 & -\sin 0 \\ \sin 0 & \cos 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

adalah matriks identitas dalam G. Dengan demikian didapat untuk sebarang titik $P(r, \phi) \in X$,

$$A(0)P(r, \phi) = P(r, \phi + 0) = P(r, \phi).$$

(2) Untuk perkalian matriksdidapat

$$\begin{aligned} A(\theta)A(\psi) &= \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} \cos\psi & -\sin\psi \\ \sin\psi & \cos\psi \end{bmatrix} \\ &= \begin{bmatrix} \cos\theta\cos\psi - \sin\theta\sin\psi & -\cos\theta\sin\psi - \sin\theta\cos\psi \\ \cos\theta\sin\psi + \sin\theta\cos\psi & \cos\theta\cos\psi - \sin\theta\sin\psi \end{bmatrix} \\ &= \begin{bmatrix} \cos(\theta+\psi) & -\sin(\theta+\psi) \\ \sin(\theta+\psi) & \cos(\theta+\psi) = A(\theta+\psi). \end{bmatrix} \end{aligned}$$

Jadi

$$(A(\theta)A(\psi))P(r, \phi) = P(r, \phi + \theta + \psi) = A(\theta)(A(\psi)P(r, \phi)).$$

Hal ini berarti bahwa bila terlebih dahulu dilakukan perkalian dua matriks kemudian merotasi titik melalui hasil perkalian matriks tersebut atau bila dilakukan lebih dulu merotasi titik melalui satu matriks dan kemudian hasilnya dirotasi lagi dengan matriks yang lainnya didapat hasil yang sama.

(3) Diberikan dua titik $P(r, \phi)$ dan $P(s, \psi)$ di X, maka dapat dipilih matriks $A(\theta)$ di G yang memenuhi $A(\theta)P(r, \phi) = P(s, \psi)$ bila dan hanya bila $s = r$. Yaitu bila dan hanya bila dua titik tersebut terletak pada lingkaran $x^2 + y^2 = r^2$. ●

Untuk sebarang himpunan tak-kosong X dan grup G tinjau pemetaan dari $G \times X$ ke X yang ditulis sebagai $(g, x) \to g.x$, dimana $g \in G$ dan $x \in X$. Apapun hal ini G ditinjau sebagai suatu grup dan bukan sekedar himpunan. Berkaitan dengan pemetaan tersebut dalam hal makna tertentu dapat disesuaikan dengan struktur grup G.

Definisi 5.1.1 Suatu **tindakan grup** G pada suatu himpunan tak-kosong X adalah suatu pemetaan $G \times X$ ke X dengan sifat berikut:

(1) $e.x = x$ untuk semua $x \in X$ dan e adalah elemen netral di G.

(2) $g_1.(g_2.x) = (g_1g_2).x$ untuk semua $g_1, g_2 \in G$ dan semua $x \in X$. Bila tindakan tersebut ada, maka dikatakan grup G **bertindak** pada X dan X adalah $G-$ **set**. ✓

Dalam Contoh 5.1.1 menjelaskan suatu tindakan grup. Difinisi 5.1.1 dapat diilustrasikan oleh berbagai contoh nyata berikut.

Contoh 5.1.2 Grup *additive* $\mathbb{R}$ bertindak pada bidang $\mathbb{R}^2$ melalui tranlasi horizontal

$$(a, (x, y)) \to (x + a, y)$$

dan suatu tindakan yang lain translasi vertikal

$$(b, (x, y)) \to (x, (y + b)).$$ ●

Contoh 5.1.3 Misalkan $G = \{e, g\}$ adalah grup siklik berorder 2 dan himpunan $X = \mathbb{C}$. Maka G bertindak pada himpunan bilangan kompleks $\mathbb{C}$ melalui tindakan $(e, x + iy) \to x + iy$ dan $(g, x + iy) \to x - iy$.

Contoh 5.1.4 Setiap subgrup H dari suatu grup G (termasuk G sendiri) bertindak pada G melalui **perkalian kiri**. Tindakan ini adalah $H \times G \to G$, dimana $(h, g) \to hg$ untuk semua $h \in H$ dan semua $g \in G$.

Contoh 5.1.5 Setiap subgrup H dari suatu grup G (termasuk G sendiri) bertindak pada G melalui **konjugasi**. Tindakan ini adalah $H \times G \to G$, dimana $(h, g) \to hgh^{-1}$ untuk semua $h \in H$ dan semua $g \in G$. Sifat (1) jelas, sedangkan sifat (2) dari persamaan $(h_1h_2)g(h_1h_2)^{-1} = h_1(h_2gh_2^{-1})h_1^{-1}$.

Konjugasi adalah suatu tindakan yang sangat penting yang akan dibahas lebih dekat dalam suatu bagian kemudian. Contoh berikut juga merupakan suatu contoh fundamental.

Contoh 5.1.6 Misalkan $X = \{1, 2, \ldots, n\}$ dan S_n adalah grup permutasi dari n elemen. Maka S_n bertindak pada X sebagai berikut: $(\tau, i) \to \tau(i)$, dimana τ suatu permutasi di S_n dan $i \in X$. Sifat (1) mengikuti definisi permutasi identitas dan sifat (2) dari definisi perkalian permutasi sebagai komposisi dari fungsi.

Contoh 5.1.6 adalah fundamental sebab tindakan dari sebarang grup G pada himpunan tak-kosong X terkait dekat dengan tindakan grup simetri dari X yaitu S_X pada X sebagaimana telah dibahas dalam contoh. Keterkaitan ini dibahas pada proposisi berikut.

Proposisi 5.1.1 Misalkan G adalah suatu grup bertindak pada suatu himpunan tak-kosong X. Maka

(1) untuk masing-masing $g \in G$ pemetaan $\tau_g : X \to X$ didefinisikan oleh $\tau_g(x) = g.x$ adalah suatu permutasi dari X.

(2) Pemetaan $\chi : G \to S_X$ didefinisikan oleh $\chi(g) = \tau_g$ adalah suatu homomorpisma.

Bukti

(1) Ditunjukkan bahwa $\tau_g : X \to X$ adalah suatu permutasi dari X atau τ_g adalah bijektif. Pemetaan τ_g adalah satu-satu sebab bila $\tau_g(x) = \tau_g(y)$, maka $g.x = g.y$. Didapat $g^{-1}.(g.x) = g^{-1}.(g.y)$. Jadi

$$x = e.x = (g^{-1}g).x = g^{-1}.(g.x) = g^{-1}.(g.y) = (g^{-1}g).y = e.y = y.$$

Pemeteaan τ_g pada, sebab bila $w \in X$ dapat dipilih $g^{-1}.w \in X$ yang memenuhi

$$\tau_g(g^{-1}.w) = g.(g^{-1}.w) = (gg^{-1}).w = e.w = w.$$

(2) Diberikan sebarang $g_1, g_2 \in G$ dan sebarang $x \in X$ didapat

$$\begin{aligned} \chi(g_1g_2)(x) &= (g_1g_2).x \\ &= g_1.(g_2.x) \\ &= \tau_{g_1}(\tau_{g_1}(x)) \\ &= (\tau_{g_1} \circ \tau_{g_2})(x) \\ &= \chi(g_1) \circ \chi(g_2)(x) \end{aligned}$$

Jadi $\chi(g_1g_2) = \chi(g_1) \circ \chi(g_2)$.

Kebalikan dari Proposisi 5.1.1 juga benar sebagaimana ditunjukkan oleh proposisi berikut.

Proposisi 5.1.2 Diberikan suatu homomorpisma grup $\psi : G \to S_X$, maka pemetaan $G \times X \to X$ didefinisikan oleh $(g, x) \to g.x = \psi(g)(x)$ adalah suatu tindakan dari G pada X.

Bukti Ditunjukkan berdasarkan Definisi 5.1.1 memenuhi sifat:

(1) $e.x = \psi(e)(x) = \mathrm{id}(x) = x$, dimana $\mathrm{id} \in S_X$ adalah permutasi identitas.

(2) $g_1.(g_2.x) = \psi(g_1)((\psi(g_2)(x)) = (\psi(g_1) \circ \psi(g_2))(x) = \psi(g_1 g_2)(x) = (g_1 g_2).x.$

Akan menjadi jelas kemudian ketika diinginkan mengkonstruksi suatu contoh dari suatu grup bahwa bukan grup komutatif. Sering dicari subgrup dari beberapa S_n yang memenuhi kondisi yang diinginkan. Grup S_n tampaknya memberikan suatu sumber persediaan yang tak-habis-habisnya untuk membuat contoh. Alasan ini menjadi jelas sebagaimana ditunjukkan dalam hasil berikut.

Teorema 5.1.1 (**Teorema Cayley**) Setiap grup isomorpik dengan suatu subgrup dari grup permutasi.

Bukti Misalkan G sebarang grup dan bertindak pada dirinya sendiri melalui perkalian kiri. Dengan demikian didapat $G \times G \to G$, dimana $(g, x) \to gx$. Dengan Proposisi 5.1.1 ada suatu homomorpisma grup $\chi : G \to S_G$ didefinisikan oleh $\chi(g) = \tau_g \in S_G$, dimana $\tau_g(x) = gx$ untuk semua $x \in G$. Kernel dari χ adalah himpunan semua $g \in G$ yang memenuhi $\tau_g = \mathrm{id}$. Jadi $\ker(\chi) = \{g \in G \mid gx = x \text{ untuk semua } x \in G\} = \{e\}$. Jadi χ adalah satu-satu, dengan demikian G isomorpik dengan $\mathrm{im}(\chi)$. Tetapi $\mathrm{im}(\chi)$ adalah subgrup dari S_G. Jadi G isomorpik dengan suatu subgrup dari suatu grup permutasi.

Definisi 5.1.2 Homomorpisma $\chi : G \to S_X$ dikaitkan dengan suatu tindakan dari suatu grup G pada suatu himpunan tak-kosong X disebut **representasi permutasi** dari tindakan.

Contoh 5.1.7 Sudah diberikan suatu representasi permutasi dari grup D_4 dalam Contoh 2.4.11. Secara lebih umum, tindakan dari grup dihedral D_n pada segi-n beraturan memberikan suatu representasi dari grup dihedral D_n sebagai suatu subgrup dari grup simetri S_n.

Definisi 5.1.3 Grup G dikatakan **secara tepat** bertindak pada himpunan tak-kosong X bila $\ker(\chi) = \{e\}$ dengan kata lain elemen di G yang menjadikan setiap elemen dari X tetap hanya elemen netral e. Jadi G secara tepat bertindak pada X bila dan hanya bila χ adalah satu-satu, dalam hal yang demikian grup G isomorpik dengan subgrup $\mathrm{im}(\chi)$ dari S_X.

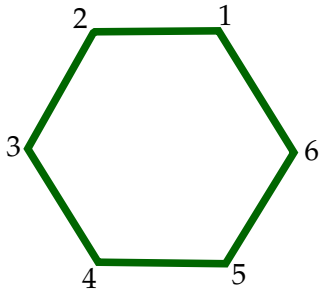
Contoh 5.1.8 Tindakan dari dihedral grup

$$D_n = \{e, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \rho\tau, \rho^2\tau, \ldots, \rho^{n-1}\tau\}$$

pada segi-n beraturan adalah setia. Misalkan $G = \{e, g, g^2\}$ siklik berorder 3 dan $X = \{1, 2, 3, 4, 5, 6\}$ adalah himpunan enam titik sudut dari segi-6 beraturan, sebagaimana diberikan oleh Gambar 5.1. Misalkan G bertindak pada X melalui rotasi g sebesar 120° berlawanan arah jarum jam pada segi-6 beraturan. Jadi $G = \{e, \rho^2, \rho^4\}$ adalah subgrup dari D_6 dimana ρ adalah rotasi sebesar 60° berlawanan arah jarum jam. Dengan demikian G secara tepat bertindak pada X dan dapat direpresentasikan oleh subgrup

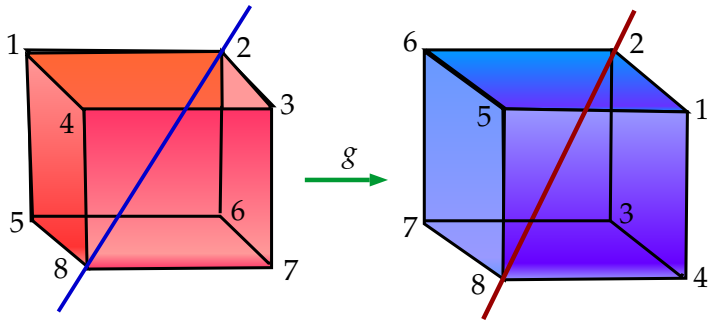
$$\{e, (1\ 3\ 5)(2\ 4\ 6), (1\ 5\ 3)(2\ 6\ 4)\}$$

dari grup simetri S_6, dimana generator g adalah permutasi $g = (1\ 3\ 5)(2\ 4\ 6)$.



Gambar 5.1: Segi-6 beraturan

Contoh 5.1.9 Misalkan $G = \{e, g, g^2\}$ grup siklik berorder 3 dan $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ adalah himpunan titik sudut dari suatu kubus. Misalkan G bertindak pada X melalui rotasi g yaitu rotasi pada garis melalui titik sudut 2 dan 8. Jadi $g.1 = 3, g.2 = 2, g.3 = 6, g.4 = 7, g.5 = 4, g.6 = 1, g.7 = 5$ dan $g.8 = 8$ sebagai mana diberikan oleh Gambar 5.2. Tindakan G pada X

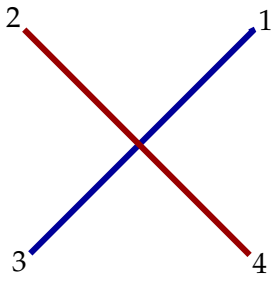


Gambar 5.2: Tindakan G pada Kubus

adalah tepat, sebab G dapat direpresentasikan oleh subgrup

$$\{e, (1\ 3\ 6)(4\ 7\ 5), (1\ 6\ 3)(4\ 5\ 7)\}$$

dari grup simetri S_8. Dalam kasus ini generator dari G direpresentasikan oleh elemen $g = (1\ 3\ 6)(4\ 7\ 5)$. ●



Gambar Diagonal Persegi

Contoh 5.1.10 Sebagaimana telah diketahui tindakan dari dihedral grup D_4 pada himpunan titik sudut $\{1, 2, 3, 4\}$ dari persegi adalah tindakan tepat. Tetapi sebagai pengganti, bila D_4 bertindak pada himpunan $\{d_1, d_2\}$ dari diagonal persegi, dimana d_1 adalah diagonal $1-3$ dan d_2 diagonal $2-4$ (lihat gambar sebelah). Dalam hal ini, tindakan tidak tepat, sebab $\rho^2.d_1 = d_1$ dan $\rho^2.d_2 = d_2$, dimana $\rho = (1\ 2\ 3\ 4) \in D_4$. ●

Latihan

Latihan 5.1.1 Tunjukkan bahwa G sebagaimana didefinisikan dalam Contoh 5.1.1 adalah

suatu subgrup dari SL(2, $\mathbb{R}$). ✓

Latihan 5.1.2 Lagi, dengan G sebagaimana didefinisikan dalam Contoh 5.1.1, tunjukkan bahwa untuk sebarang titik P dan Q dalam bidang $\mathbb{R}^2$ ada suatu matriks $A \in G$ dengan $A.P = Q$ bila dan hanya bila P dan Q keduanya adalah titik yang terletak pada lingkaran $x^2 + y^2 = r^2$ untuk beberapa $r > 0$. ✓

Latihan 5.1.3 Untuk latihan berikut (a) Tunjukkan bahwa X dapat dianggap sebagai suatu $G-$ set dalam suatu cara yang wajar, yaitu uraikan suatu tindakan grup G pada X dengan cara yang wajar. (b) Tunjukkan bahwa tindakan memenuhi sifat dua sifat definisi dari suatu tindakan. (c) Berikan suatu representasi permutasi dari tindakan.

(1) $G = \{e, g\}$ grup siklik berorder 2 dan X himpunan titik dari suatu segitiga sama sisi.

(2) $G = \{e, g, g^2\}$ grup siklik berorder 3 dan X himpunan titik dari suatu segitiga sama sisi.

(3) $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ grup tak-siklik berorder 4 dan X himpunan titik sudut dari suatu persegi.

(4) $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ grup tak-siklik berorder 6 dan X himpunan titik sudut dari suatu segi-6 beraturan.

(5) $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ dan X himpunan titik sudut dari suatu persegi. ✓

Latihan 5.1.4 Misalkan $G = \mathbb{Z}$ dan X adalah himpunan koset dari $5\mathbb{Z}$ dalam $\mathbb{Z}$. Berikan suatu contoh dari suatu tindakan G pada X didefinisikan dengan cara yang wajar tetapi bukan tindakan tepat. ✓

Latihan 5.1.5 Tunjukkan bahwa $\mathbb{R}^2$ adalah suatu $G-$set dengan tindakan translasi horizontal sebagaimana diberikan dalam Contoh 5.1.2. ✓

Latihan 5.1.6 Misalkan G suatu grup dan X adalah himpunan dari semua subgrup dari G. Tunjukkan bahwa X adalah suatu $G-$ set terhadap konjugasi : $(g, H) \to gHg^{-1}$. ✓

Latihan 5.1.7 Misalkan $G = S_3$ dan X himpunan semua subgrup dari S_3. Tulis tabel untuk menunjukkan tindakan dari G pada X melalui konjugasi seperti Latihan 5.1.6. Apakah tindakan ini suatu tindakan tepat? ✓

Latihan 5.1.8 Misalkan G dan X seperti dalam Latihan 5.1.6 dengan G bertindak pada X melalui konjugasi. Uraikan kernel dari χ sebagaimana dalam Proposisi 5.1.1 dimana G adalah suatu grup komutatif. ✓

Latihan 5.1.9 Misalkan H adalah suatu subgrup dari suatu grup G dan X himpunan semua koset kiri dari H dalam G. Tunjukkan bagaimana X dapat dibuat sebagai suatu $G-$ set dengan cara yang wajar. ✓

Latihan 5.1.10 Misalkan X_1 dan X_2 adalah $G-$set untuk grup G dan $X_1 \cap X_2 = \varnothing$. Tunjukkan bagaimana himpunan $X_1 \cup X_2$ dapat menjadi suatu $G-$ set dalam suatu cara yang wajar. ✓

Latihan 5.1.11 Untuk latihan berikut, misalkan H adalah suatu subgrup dari suatu grup G dan himpunan $X = \{xH \mid x \in G\}$. Misalkan G bertindak pada X melalui perkalian kiri $(g, xH) \to gxH \in X$.

(1) Tunjukkan bahwa tindakan tersebut adalah suatu tindakan grup.

(2) Bila $\chi : G \to S_X$ adalah suatu representasi permutasi dari tindakan G. Maka

- **(a)** Tentukan $K = \ker(\chi)$.
- **(b)** Tunjukkan bahwa $K \subset H$.
- **(c)** Tunjukkan bahwa bila N adalah suatu subgrup normal dari G dan $N \subset H$, maka $N \subset K$. Dengan kata lain, tunjukkan bahwa K adalah subgrup normal terbesar dari G yang termuat dalam H.

(3) Tunjukkan bagaimana teorema Cayley dalam latihan yang baru dibahas tersebut.

(4) Misalkan $i = [G : H]$ adalah ideks dari H dalam G. Maka

- **(a)** Tunjukkan bahwa bila χ satu-satu, maka $|G|$ membagi $i!$
- **(b)** Tunjukkan bahwa bila $|G|$ tidak membagi $i!$, maka K adalah tak-trivial.
- **(c)** Tunjukkan bahwa bila $|G|$ tidak membagi $i!$, maka G mempunyai suatu subgrup normal sejati tak-trivial.

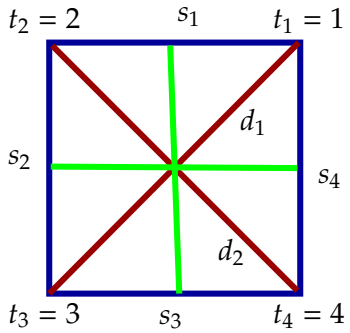
5.2 Stabiliser dan Orbit dalam suatu Tindakan Grup

Dalam bagian ini ditunjukkan bahwa suatu tindakan grup menentukan suatu relasi ekivalen pada X sebagai $G-$set. Dalam hal ini X dipartisi menjadi klas-klas ekivalen yang dinamakan orbit. Selanjutnya dibuktikan teorema utama yang menentukan banyaknya elemen dari masing-masing orbit. Teorema ini akan digunakan berkali-kali pada bab ini untuk berbagai tindakan grup. Contoh berikut diharapkan memberikan kemudahan untuk memahami beberapa pengertian beberapa definisi dan sifat-sifat terkait yang dibahas dalam bagian ini.

Contoh 5.2.1 Tinjau Dihedral grup D_4 bertindak dengan cara yang wajar pada himpunan

$$X = \{t_1, t_2, t_3, t_4, s_1, s_2, s_3, s_4, d_1, d_2\},$$

dimana $t_i = i$, $i = 1, 2, 3, 4$ adalah titik sudut dari persegi, $s_1 = 1-2, s_2 = 2-3, s_3 = 3-4, s_4 = 4-1$ adalah sisi-sisi persegi dan $d_1 = 1-3, d_2 = 2-4$ adalah diagonal persegi (lihat gambar sebelah). Tabel 5.1 menguraikan tindakan D_4 pada X akan membantu untuk mempermudah memahami beberapa definisi baru yang diberikan dalam bagian ini.



Gambar Persegi dari grup D_4.

Proposisi 5.2.1 Misalkan X adalah $G-$set dan untuk sebarang $x \in X$ didefinisikan himpunan

$$G_x = \{g \in G \mid g.x = x\}.$$

Tabel 5.1: Tindakan D_4 pada X

	1	2	3	4	t_1	t_2	t_3	t_4	d_1	d_2
ρ_0	1	2	3	4	t_1	t_2	t_3	t_4	d_1	d_2
ρ	2	3	4	1	t_2	t_3	t_4	t_1	d_2	d_1
ρ^2	3	4	1	2	t_3	t_4	t_1	t_2	d_1	d_2
ρ^3	4	1	2	3	t_4	t_1	t_2	t_3	d_2	d_1
τ	2	1	4	3	t_1	t_4	t_3	t_2	d_2	d_1
$\rho\tau$	3	2	1	4	t_2	t_1	t_4	t_3	d_1	d_2
$\rho^2\tau$	4	3	2	1	t_3	t_2	t_1	t_4	d_2	d_1
$\rho^3\tau$	1	4	3	2	t_4	t_3	t_2	t_1	d_1	d_2

Maka G_x adalah subgrup dari G.

Bukti Cukup ditunjukkan bahwa bila $g \in G_x$, maka $g^{-1} \in G_x$ dan bila $g_1, g_2 \in G_x$, maka $g_1 g_2 \in G_x$. Bila $g \in G_x$, maka $g.x = x$. Jadi

$$g^{-1}.x = g^{-1}.(g.x) = (g^{-1}g).x = e.x = x.$$

Hal ini menunjukkan bahwa $g^{-1} \in G_x$. Selanjutnya, bila $g_1, g_2 \in G_x$, maka

$$(g_1 g_2).x = g_1.(g_2.x) = g_1.x = x.$$

Jadi $g_1 g_2 \in G_x$.

Definisi 5.2.1 Grup G_x dinamakan **stabilizer** dari x dalam G. Subgrup G_x juga dinamakan subgrup **isotropy** dari G untuk elemen $x \in X$.

Contoh 5.2.2 Dalam Contoh 5.2.1 tidakan dari D_4 pada X dan dari Tabel 5.1 didapat untuk $g.2 = 2$ maka $g = \rho_0$ atau $g = \rho\tau$. Jadi $G_2 = \{\rho_0, \rho\tau\}$. untuk $g.d_1 = d_1$ maka $g = \rho_0, \rho^2, \rho\tau$ atau $g = \rho^3\tau$. Jadi $G_{d_1} = \{\rho_0, \rho^2, \rho\tau, \rho^3\tau\}$. Untuk $g.t_4 = t_4$ maka $g = \rho_0$ atau $g = \rho^2\tau$. Jadi $G_2 = \{\rho_0, \rho^2\tau\}$.

Berikut ini ditunjukkan bagaimana cara dari tindakan suatu grup G pada himpunan tak-kosong X yang mempartisi X menjadi klas-klas yang ekivalen.

Proposisi 5.2.2 Misalkan G adalah suatu grup bertindak pada suatu himpunan tak-kosong X. Relasi pada X didefinisikan oleh

$$a \sim b \text{ bila dan hanya bila } a = g.b \text{ untuk beberapa } g \in G \text{ dan } a, b \in X.$$

Maka relasi $\sim$ adalah relasi ekivalen.

Bukti Sifat refleksif, untuk sebarang $a \in X$, didapat $a = e.a$. Jadi $a \sim a$. Sifat simetri, untuk sebarang $a, b \in X$. Bila $a \sim b$ maka dapat dipilih $g \in G$ yang memenuhi $a = g.b$. Jadi

$$g^{-1}.a = g^{-1}.(g.b) = (g^{-}g).b = e.b = b.$$

Hal ini menunjukkan bahwa $b \sim a$. Sifat transitif, untuk sebarang $a, b, c \in X$. Bila $a \sim b$ dan $b \sim c$, maka dapat dipilih $g, h \in G$ yang memenuhi $a = g.b$ dan $b = h.c$. Didapat

$$a = g.b = g.(h.c) = (gh).c.$$

Jadi $a \sim c$.

Definisi 5.2.2 Diberikan grup G bertindak pada himpunan tak-kosong X. Maka himpunan klas ekivalen

$$O_a = \{b \in X \mid a \sim b\}$$

dinamakan **orbit** dari a dalam X.

Contoh 5.2.3 Tinjau lagi Contoh 5.2.1 tindakan dari D_4 pada X. Dari Tabel 5.1 dapat dilihat bahwa ada tiga himpunan orbit, yaitu himpunan titik sudut, himpunan sisi dan himpunan diagonal. Jadi

$$O_2 = \{1, 2, 3, 4\}, O_{d_1} = \{d_1, d_2\} \text{ dan } O_{t_4} = \{t_1, t_2, t_3, t_4\}.$$

Sudah ditunjukkan bahwa G_2 subgrup berorder 2, sedangkan O_2 mempunyai 4 elemen. Begitu juga G_{d_1} subgrup berorder 4, sedangkan O_{d_1} mempunyai 2 elemen. Serta, G_{t_4} subgrup berorder 2, sedangkan O_{t_4} mempunyai 4 elemen.

Dalam Contoh 5.2.3, didapat $|G_a||O_a| = |G|$ untuk setiap kasus. Hal ini dibuktikan oleh teorema berikut untuk sebarang tindakan grup.

Teorema 5.2.1 (**Hubungan Orbit-Stabilizer**) Diberikan grup G bertindak pada suatu himpunan tak-kosong X dan a adalah sebarang elemen di X. Bila G adalah berhingga, maka $|O_a| = |G|/|G_a|$.

Bukti Indeks $[G : G_a]$ adalah banyaknya koset dari G_a dalam G. Sebagaimana telah diketahui bahwa bila $|G|$ berhingga, maka $[G : G_a] = |G|/|G_a|$. Diberikan sebarang $b \in O_a$, dapat dipilih suatu $g \in G$ yang memenuhi $b = g.a$. Dengan demikian didefinisikan pemetaan $\tau : O_a \to H$ dimana $H = \{gG_a \mid g \in G\}$ oleh $b = g.a \to gG_a$, $\forall b \in O_a$. Pemetaan τ terdefinisi secara baik, sebab bila $b = g_1.a$ dan $b = g_2.a$, maka

$$(g_1^{-1}g_2).a = g_1^{-1}.(g_2.a) = g_1^{-1}.b = g_1^{-1}.(g_1.a) = (g_1^{-1}g_1).a = e.a = a.$$

Jadi $g_1^{-1}g_2 \in G_a$ akibatnya $g_1G_a = g_2G_a$. Pemetaan τ adalah satu-satu, sebab $\tau(b_1) = \tau(b_2)$ bila dan hanya bila $g_1G_a = g_2G_a$ dimana $b_1 = g_1.a$ dan $b_2 = g_2.a$. Tetapi $g_1G_a = g_2G_a$ bila dan hanya bila $g_1 = g_2h$ untuk beberapa $h \in G_a$, dalam hal ini didapat

$$b_1 = g_1.a = (g_2h).a = g_2.(h.a) = g_2.a = b_2.$$

Pemetaan τ adalah pada, sebab diberikan sebarang koset kiri $g'G_a \in H$ dapat dipilih $g'.a \in O_a$ yang memenuhi $\tau(g'.a) = g'G_a$. Karena τ satu-satu dan pada, maka $|O_a| = |H| = [G : G_a]$. Jadi $|O_a| = |G|/|G_a|$.

Contoh 5.2.4 Misalkan $X = \{1, 2, \ldots, n\}$ dan $G = S_n$. Diberikan sebarang $i, j \in X$ dapat dipilih suatu permutasi $\tau \in S_n$ yang memenuhi $\tau(i) = j$. Jadi melalui tindakan S_n didapat hanya satu orbit. Bila dipilih $x = 3 \in X$, maka O_3 adalah X dan stabilizer G_3 isomorpik dengan S_{n-1}. Sehingga didapat $|S_n| = |O_3||G_3| = n|S_{n-1}|$.

Definisi 5.2.3 Diberikan grup G bertindak pada suatu himpunan tak-kosong X. Tindakan dari G pada X dinamakan **transitif** bila hanya ada satu orbit dalam tindakan G pada X, yaitu untuk sebarang dua elemen $a, b \in X$ ada beberapa $g \in G$ yang memenuhi $g.a = b$.

Contoh 5.2.5 Dalam Contoh 5.1.2 tindakan grup *additive* $\mathbb{R}$ pada bidang $\mathbb{R}^2$ melalui translasi horizontal bukan tindakan transitif. Sebab orbit dari sebarang titik (a, b) adalah garis horizontal $y = b$ yang tidak sama dengan bidang $\mathbb{R}^2$.

Contoh 5.2.6 Misalkan $X = \{1, 2, 3, \ldots, n\}$ adalah himpunan dari n titik sudut dari segi-n beraturan dengan $n \geq 3$. Tindakan grup dihedral D_n (dalam Contoh 2.1.16) pada X adalah transitif. Jadi untuk sebarang $a \in X$, orbit O_a mempunyai elemen sebanyak n. Bila dipilih $a = 1$ dan sebarang $\sigma \in G_1$, maka $\sigma(2) = 2$ dalam hal ini σ adalah identitas atau $\sigma(2) = n$, dimana n adalah titik sudut yang terletak pada sisi $1 - n$ dalam kasus ini σ adalah suatu pencerminan pada sumbu melalui titik pusat segi-n beraturan dan titik sudut 1. Sehingga didapat $\sigma(1) = 1$ dan $\sigma(i) = n - i + 2$ untuk semua $i \in X$ dengan $i \neq 1$. Jadi $|G_1| = 2$ dan $|D_n| = |O_1||G_1| = n \cdot 2 = 2n$.

Contoh 5.2.7 Misalkan G adalah grup rotasi pada suatu kubus. Tindakan G pada delapan titik sudut dari kubus adalah transitif. Bila dipilih titik sudut 3 dan sebarang $\tau \in G_2$, maka $\tau(3) = 3$ dalam kasus ini τ adalah identitas. Bila $\tau(3) = 6$, maka dalam kasus ini $\tau(6) = 1, \tau(1) = 3$. Bila $\tau(3) = 1$, maka dalam kasus ini $\tau(1) = 6, \tau(6) = 3$. (Lihat gambaran ini dalam Contoh 5.1.9.) Jadi $|G_2| = 3$ dan $|G| = |O_2||G_2| = 8(3) = 24$.

Pada akhir pembahasan ini diberikan suatu akibat langsung dari Proposisi 5.2.2 dan Teorema 5.2.1 yang berperanan sebagai suatu aturan dasar pada bab ini.

Teorema 5.2.2 Misalkan X adalah suatu $G-$ set dan N adalah banyaknya orbit dalam tindakan. Bila $a_1, a_2, \ldots, A_N$ adalah representasi yang berbeda dari himpunan orbit yaitu setiap elemen dari X berada secara tepat dalam satu orbit O_{a_i}. Maka

$$|X| = \sum_{i=1}^{N} [G : G_{a_i}],$$

dimana G_{a_i} adalah stabilizer dari a_i.

Bukti Dari Proposisi 5.2.2 didapat bahwa tindakan G pada X mempartisi X menjadi orbit-orbit O_{a_i}, $i = 1, 2, \ldots, N$ yang berbeda dengan menggunakan Teorema 1.2.2 didapat

$$|X| = \sum_{i=1}^{N} |O_{a_i}|.$$

Tetapi dari Teorema 5.2.1 didapat $|O_{a_i}| = [G : G_{a_i}]$. Jadi

$$|X| = \sum_{i=1}^{N} [G : G_{a_i}].$$

Latihan

Latihan 5.2.1 Untuk latihan berikut : (a) dapatkan stabilizer G_a untukmasing-masing a, dapatkan orbit O_a, (c) selidiki bahwa $|O_a| = [G : G_a]$, (d) tentukan apakah tindakan transitif dan (e) tentukan apakah G bertindak pada X secara tepat. Dimana X, G dan a diberikan sebagai berikut.

1. $X = \{1, 2, 3\}$; $G = S_3$; $a = 1, 2, 3$.
2. $X = \{1, 2, 3, 4\}$; $G = A_3 \subset S_3$; $a = 1, 2, 3$.
3. $X = \{1, 2, 3, 4\}$; $G = S_4$; $a = 1, 3, 4$.
4. $X = \{1, 2, 3, 4\}$; $G = A_4 \subset S_4$; $a = 1, 3, 4$.
5. $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$; $G = \{\rho_0, (1\ 2\ 3\ 4)(5\ 7), (1\ 3)(2\ 4), (1\ 4\ 3\ 3)(5\ 7)\} \subset S_7$, dimana ρ_0 adalah permutasi identitas; $a = 1, 3, 6, 7$.
6. $X = \{1, 2, 3, 4\}$ himpunan titik sudut dari persegi; $G = D_4$; $a = 1, 2, 3$.
7. $X = \{1, 2, 3, 4\}$ himpunan titik sudut dari persegi; $G = \langle \rho \rangle \subset D_4$, ρ adalah rotasi 90°; $a = 1, 3$.
8. $X = \{1, 2, 3, 4\}$ himpunan titik sudut dari persegi; $G = \left\langle \rho^2, \tau \right\rangle \subset D_4$; $a = 1, 3$.

Latihan 5.2.2 Misalkan $X = \mathbb{C} - \{0, -1\}$. Untuk $z \in X$, misalkan

$$T_0(z) = z, T_1(z) = -1/(1 + z), T_2 = (1 - z)/ - z$$

dan $G = \{T_0, T_1, T_2\}$.

(a) Tunjukkan bahwa G adalah grup terhadap komposisi fungsi.

(b) Tunjukkan bahwa G bertindak pada X secara wajar.

(c) Dapatkan semua $a \in X$ yang memenuhi $G_a = G$.

Latihan 5.2.3 Untuk $a, b \in \mathbb{R}$, misalkan $g(a, b) \in M(2, \mathbb{R})$ adalah matriks

$$g(a, b) = \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix}.$$

Misalkan $G = \{g(a, b) \mid a, b \in \mathbb{R}, a \neq 0\}$ dengan operasi perkalian matriks dan $X = \mathbb{R}$. Untuk $g = g(a, b) \in G$ dan $x =\in X$ didefinisikan $g.x = ax + b$.

(a) Tunjukkan bahwa G adalah subgrup dari $\mathrm{GL}(2, \mathbb{R})$.

(b) Tunjukkan $g.x = ax + b$ mendefinisikan suatu tindakan G pada X.

(c) Dapatkan G_0 dan O_0.

(d) Apakah G brtindak secara tepat pada X?

(e) Apakah tindakan transitif?

Latihan 5.2.4 Misalkan H suatu subgrup dari suatu grup G dan $X = \{xH \mid x \in G\}$. Misalkan G bertindak pada X melalui perkalian kiri, yaitu $g.xH = gxH$ untuk $g \in G$ dan $xH \in X$.

(a) Tunjukkan bahwa G_{xH} stabilizer dari $xH \in X$ adalah subgrup xHx^{-1} dari G.

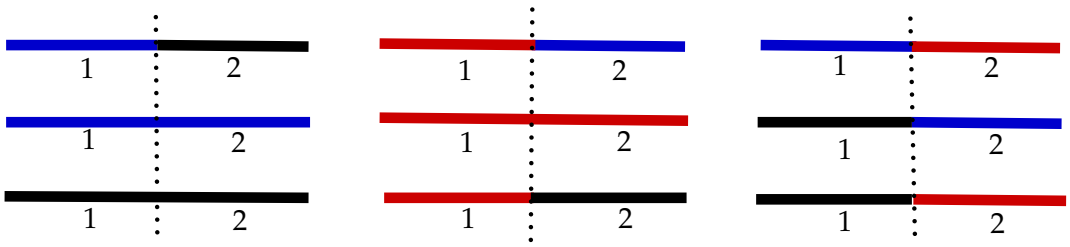
(b) Tunjukkan bahwa untuk sebarang $xH \in X$, $|O_{xH}| = [G : H]$.

Latihan 5.2.5 Diberikan G adalah suatu grup berhingga dengan $|G| = n$ dan misalkan p adalah bilangan prima terkecil membagi n. Tunjukkan bahwa bila H adalah suatu subgrup dari G dengan $[G : H] = p$, maka $H \lhd G$.

5.3 Teorema Burside dan Aplikasi

Pada bagian ini diaplikasikan hubungan orbit-stabilizer (Teorema 5.2.1) yang telah dibahas pada bagian sebelumnya untuk membuktikan teorema Burnside. Teorema ini memberikan metode konting banyaknya orbit dari suatu himpunan melalui tindakan suatu grup simetri. Juga diilustrasikan bagaimana teorema Burnside dapat diaplikasikan untuk berbagai masalah *counting*, yaitu untuk menentukan banyaknya disain "yang secara esensial berbeda".

Contoh 5.3.1 Suatu tongkat teridiri dari dua bagian, yaitu bagian 1 dan bagian 2. Bila pada masing-masing bagian akan diwarnai dengan tiga warna berbeda, yaitu merah, hitam dan biru sebagaimana diberikan oleh Gamabr 5.3. Maka berapakah banyaknya cara yang



Gambar 5.3: Pewarnaan Tongkat

berbeda dari dari pewarnaan tongkat tersebut bila aturan perwarnaan adalah satu bagian dari tongkat hanya diwarnai oleh satu warna? Persoalan ini bisa dijawab sebagai berikut. Ada sebanyak $3^2 = 9$ cara perwarnaan, yaitu

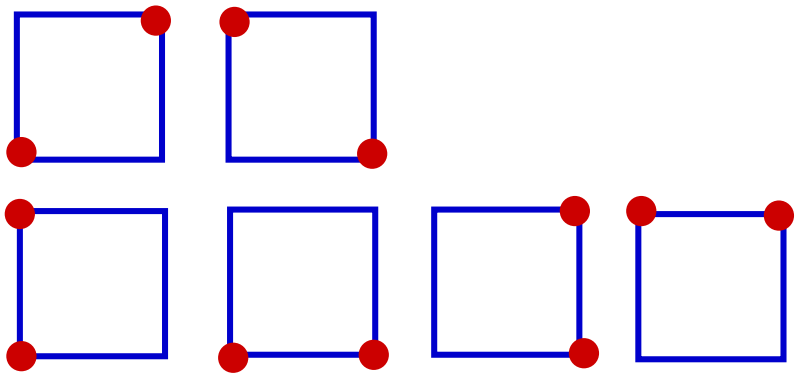
$$x_1 = bh, x_2 = mb, x_3 = bm, x_4 = bb, x_5 = mm, x_6 = hb, x_7 = hh, x_8 = mh, x_9 = hm,$$

dimana $m =$ merah, $b =$ biru dan $h =$ hitam. Jadi $x_1 = bh$ artinya bagian tonkat 1 berwarna biru bagian 2 tongkat berwarna hitam. Juga $x_6 = hb$, artinya bagian tonkat 1 berwarna hitam bagian 2 tongkat berwarna biru. Tetapi secara esensial tongkat yang berwarna x_1 dan x_6 adalah sama. Begitu juga tongkat yang berwarna $x_2 = mb$ dan yang berwarna $x_3 = bm$ secara esensial adalah sama. Jadi ada sebanyak enam perwarnaan yang berbeda pada tongkat yaitu: biru-biru, merah-merah, hitam-hitam, biru-merah, biru-hitam dan merah-hitam. Masalah ini bisa dianalisa dengan menggunakan pengertian tindakan grup. Misalkan

$$X = \{x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9\}$$

dan $G = \langle \tau \rangle$ adalah subgrup dari S_2 dimana τ adalah pencerminan tongkat pada garis yang melewati pusat tongkat. Jadi $G = \{e, \tau\}$. Dengan demikian bila G bertindak secara wajar pada X, maka X memuat enam orbit yang berbeda yaitu $O_{x_1} = \{x_1, x_6\}$ sebab $x_1 = \tau.x_6$, $O_{x_2} = \{x_2, x_3\}$ sebab $x_2 = \tau.x_3$, $O_{x_4} = \{x_4\}$ sebab $x_4 = \tau.x_4$, $O_{x_5} = \{x_5\}$ sebab $x_5 = \tau.x_5$, $O_{x_7} = \{x_7\}$ sebab $x_7 = \tau.x_7$ dan $O_{x_8} = \{x_8, x_9\}$ sebab $x_8 = \tau.x_9$. ●

Contoh 5.3.2 Tinjau semua cara yang mungkin untuk mewarnai titik sudut persegi dengan dua warna merah, maka banyaknya cara perwarnaan yang mungkin diberikan oleh koefisien binomial $4!/2!(4-2)! = 6$. Hasil ini bisa dilihat pada Gambar 5.4. Dari semua pewarnaan ini terdapat hanya dua pewarnaan yang berbeda. Pada Gambar 5.4 terlihat bahwa hasil



Gambar 5.4: Pewarnaan Titik Sudut Persegi

pewarnaan titik sudut persegi dengan dua warna merah, dikelompokkan pada dua baris. Baris pertama secara esensial menghasilkan pewarnaan benda yang sama. Begitu juga baris kedua secara esensial menghasilkan pewarnaan benda yang sama. Hasil ini bisa dilakukan menggunakan pengertian tindakan suatu grup. Misalkan $G = \langle \rho \rangle$ adalah subgrup dari D_4, dimana ρ adalah rotasi pada pusat persegi sebesar 90° berlawanan arah dengan arah jarum jam. Jadi $G = \{\rho_0, \rho, \rho_2, \rho_3\}$. Misalkan X adalah himpunan dari hasil pewarnaan yang diberikan oleh Gambar 5.4. Bila G bertindak pada X secara wajar, maka X memuat dua orbit yang berbeda yaitu baris pertama pada Gambar 5.4 dan baris kedua pada Gambar 5.4. Dua hasil pewarnaan pada baris pertama Gambar 5.4 ekivalen pewarnaan yang satu bisa diperoleh dari pewarnaan yang lain dengan melakukan tindakan dari ρ pada masing-masing pewarnaan. Empat hasil pewarnaan pada baris kedua Gambar 5.4 adalah ekivalen satu dengan yang lainnya. Sebab hasil pewarnaan kedua, ketiga dan keempat dapat diperoleh dari tindakan ρ, ρ^2 dan ρ^3 pada hasil pewarnaan yang pertama pada baris kedua Gambar 5.4. ●

Masalah-masalah yang dibahas dalam bagian ini, himpunan X memuat hasil disain berbeda dan dua disain A dan B dalam A dikatakan secara esensial sama bila A dan B adalah ekivalen melalui tindakan suatu grup permutasi yang sesuai G pada X. Dengan kata lain A dan B terletak pada satu orbit yang sama. Jadi bila diinginkan untuk menghitung banyaknya disain yang secara esensial berbeda, maka hal ini sama saja menentukan banyaknya orbit pada X. Teorema berikut memberikan suatu cara untuk menentukan banyaknya orbit yang berbeda pada X. Namum sebelumnya diberikan suatu definisi sebagai berikut.

Definisi 5.3.1 Misalkan G bertindak pada suatu himpunan tak-kosong X dan $a \in X$, telah dikenalkan notasi G_a yang menyatakan stabilizer dari a dan merupakan subgrup dari G. Juga

notasi O_a adalah orbit dari a yang mana merupakan himpunan bagian dari X. Selanjutnya untuk $g \in G$ dikenalkan suatu notasi $\text{Fix}(g) = X_g$ dengan

$$X_g = \{x \in X \,|\, g.x = x\}$$

yaitu himpunan elemen-elemen di X yang dijadikan **tetap** oleh g.

Teorema 5.3.1 (**Burnside**) Misalkan G adalah suatu grup berhingga bertindak pada suatu himpunan tak-kosong berhingga X. Bila N adalah banyaknya orbit dalam X oleh tindakkan dari G, maka

$$N = \frac{1}{|G|}\sum_{g\in G}|X_g| = \frac{1}{|G|}\sum_{g\in G}|\text{Fix}(g)|.$$

Bukti Definisikan suatu fungsi

$$T : G \times X \to \{0,1\} \text{ oleh } T(g,a) \stackrel{\text{def}}{=} \begin{cases} 1, & \text{bila } g.a = a \\ 0, & \text{bila } g.a \neq a. \end{cases}$$

Ada dua hal penting bagi T, pertama untuk sebarang g tetap di G didapat

$$|X_g| = \sum_{a\in X} T(g,a).$$

Kedua, untuk sebarang $a \in X$ dimana a tetap, didapat

$$|G_a| = \sum_{g\in G} T(g,a).$$

Selanjutnya, misalkan $a_1, a_2, \ldots, a_N$ adalah representasi dari N orbit dari G dalam X. Didapat

$$\begin{aligned}
\sum_{g\in G}|X_g| &= \sum_{g\in G}\left(\sum_{a\in X} T(g,a)\right) \\
&= \sum_{a\in X}\left(\sum_{g\in G} T(g,a)\right) \\
&= \sum_{a\in X}|G_a| = \sum_{a\in X}\frac{|G|}{|O_a|} \\
&= \sum_{i=1}^{N}\left(\sum_{a\in O_{a_i}}\frac{|G|}{|O_a|}\right) \\
&= \sum_{i=1}^{N}\left(\sum_{a\in O_{a_i}}\frac{|G|}{|O_{a_i}|}\right) \\
&= \sum_{i=1}^{N}\cancel{|O_{a_i}|}\frac{|G|}{\cancel{|O_{a_i}|}} \\
&= \sum_{i=1}^{N}|G| = N\,|G|.
\end{aligned}$$

Jadi

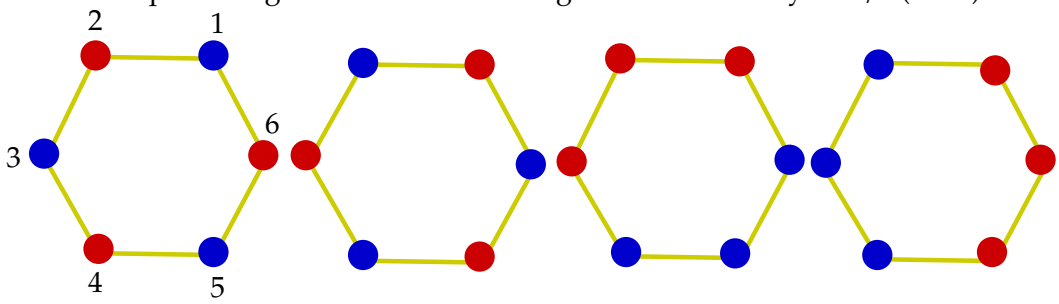
$$\boxed{\mathbf{N = \frac{1}{|G|}\sum_{g\in G}|X_g| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|.}}$$

Aplikasi

Diberikan ilustrasi bagaimana menerapkan teorema Burnside untuk masalah konting tertentu. Pada semua masalah konting ini, dihitung banyak orbit dari beberapa tindakan grup. Pertama diperlukan himpunan tertentu X dan grup G bertindak pada X, kemudian ditentukan $|X_g|$ untuk semua $g \in G$.

Menentukan struktur molekul adalah satu dari berbagai contoh penggunaan teorema Burnside. Struktur Elektronik dari suatu molekul dapat ditentukan melalui struktur geometrinya. Untuk hal ini ditinjau simetri dari suatu molekul karena dapat mengungkapkan tentang sifat-sifatnya yaitu: strukur, spektra, polaritas dan lain sebagainya.

Contoh 5.3.3 (**Masalah Kalung**) Tiga untai manik merah dan biru dirangkai untuk membentuk sebuah kalung, yang dapat diputar dan dibalik. Dengan asumsi bahwa manik-manik dengan warna yang sama bisa dibedakan. Berapa banyak jenis kalung dapat dibuat?
Untuk menjawab masalah ini 3 untai manik biru dan merah dilekatkan pada enam titik sudut segi enam beraturan contoh hasil disain perangkain kalung diberikan oleh Gambar 5.5. Banyaknya cara dari pemasangan untai manik kalung ini adalah sebanyak $6!/3!(6-3)! = 20$



Gambar 5.5: Penempatan Untai Kalung

cara. Jadi Himpunan X terdiri dari 20 disain. Karena kalung dapat diputar dan dibalik, grup G yang bertindak pada X adalah grup dihedral

$$D_6 = \{\rho_0, \rho, \rho^2, \ldots, \rho^5, \tau, \rho\tau, \rho^2\tau, \ldots, \rho^5\tau\},$$

dimana $\rho = (1\,2\,3\,4\,5\,6)$ adalah rotasi sebesar 60° berlawanan arah jarum jam dan $\tau = (2\,6)(3\,5)$ adalah pencerminan pada garis melaui titik 1 dan 4. Bila dihitung $|X_g|$ untuk setiap $g \in G$ hasilnya diberikan dalam Tabel 5.2. Selanjutnya dengan menggunakan teorema Burnside didapat

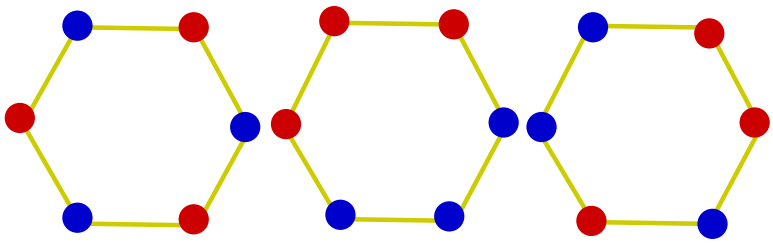
$$N = 1/12(20 + 2(2) + 3(4)) = 4.$$

Jadi banyaknya hasil disain kalung yang berbeda adalah tiga sebagaimana diberikan oleh Gambar 5.6

Berikut ini diberikan suatu contoh aplikasi dari teorema Burnside pada pada Enumerasi Pola Molekul Karbon [16].

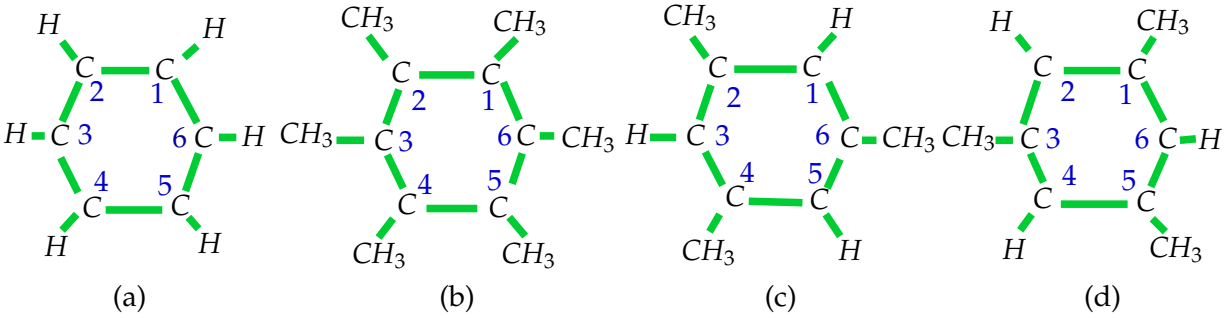
Tabel 5.2: Tindakan dari D_6 pada X

g	X_g	g	X_g
ρ_0 = identitas	20	$\tau = (2\,6)(3\,5)$	4
$\rho = (1\,2\,3\,4\,5\,6)$	0	$\rho\tau = (1\,2)(3\,6)(4\,5)$	0
$\rho^2 = (1\,3\,5)(2\,4\,6)$	2	$\rho^2\tau = (1\,3)(4\,6)$	4
$\rho^3 = (1\,4)(2\,5)(3\,6)$	0	$\rho^3\tau = (1\,4)(2\,3)(5\,6)$	0
$\rho^4 = (1\,5\,3)(2\,6\,4)$	2	$\rho^4\tau = (1\,5)(2\,4)$	4
$\rho^5 = (1\,6\,5\,4\,3\,2)$	0	$\rho^5\tau = (1\,6)(2\,5)(3\,4)$	0



Gambar 5.6: Hasil Untain Manik yang berbeda

Contoh 5.3.4 Menentukan ada berapa banyak senyawa organik yang terjadi dari suatu proses kimia yang mungkin. Dari satu rantai karbon terdiri dari enam atom karbon C dikaitkan dengan satu atom hidrogen H dan satu molekul CH_3. Ada sebanyak $2^6 = 64$ pola senyawa molekul yang mungkin. Beberapa diantaranya membentuk senyawa yang



Gambar 5.7: Pola senyawa rantai karbon C

sama. Sebagai contoh, dalam Gambar 5.7 bagian (c) dan (d) adalah pola molekul yang sama sebab yang satu dapat diperoleh dari yang lainnya melalui putaran berlawanan arah jarum jam sebesar 60°. Sedangkan pada bagian (a), (b) dan (c) adalah tiga pola molekul yang berbeda, sebab yang satu tidak bisa didapat dari yang lainnya dengan melakukan putaran atau pencerminan pada sumbu yang ditentukan. Jadi dalam hal ini himpunan X adalah himpunan semua pola senyawa yang terjadi dengan $|X| = 64$, sedangkan grup G adalah grup dihedral

$$D_6 = \{\rho_0, \rho, \rho^2, \ldots, \rho^5, \tau, \rho\tau, \rho^2\tau, \ldots, \rho^5\tau\},$$

dimana $\rho = (1\,2\,3\,4\,5\,6)$ adalah rotasi sebesar 60° berlawanan arah jarum jam dan $\tau = (2\,6)(3\,5)$

Tabel 5.3: Pola senyawa rantai karbon C

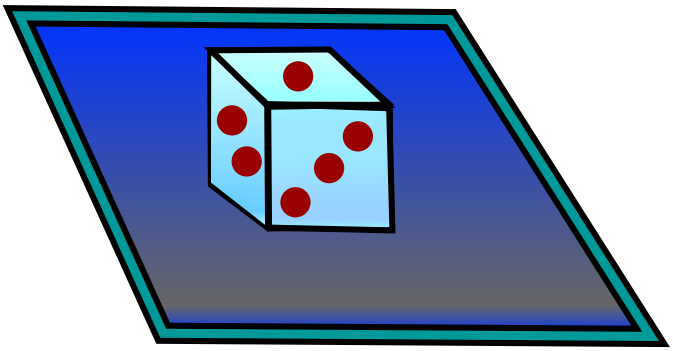
g	$\lvert X_g \rvert$	g	$\lvert X_g \rvert$
ρ_0 = identitas	64	τ = (2 6)(3 5)	16
ρ = (1 2 3 4 5 6)	2	$\rho\tau$ = (1 2)(3 6)(4 5)	8
ρ^2 = (1 3 5)(2 4 6)	4	$\rho^2\tau$ = (1 3)(4 6)	16
ρ^3 = (1 4)(2 5)(3 6)	8	$\rho^3\tau$ = (1 4)(2 3)(5 6)	8
ρ^4 = (1 5 3)(2 6 4)	4	$\rho^4\tau$ = (1 5)(2 4)	16
ρ^5 = (1 6 5 4 3 2)	2	$\rho^5\tau$ = (1 6)(2 5)(3 4)	8

adalah pencerminan pada garis diagonal tetap melaui titik 1 dan 4, juga $\rho^2\tau, \rho^4\tau$ adalah pencerminan pada garis diagonal tetap masing-masing melalui titik 2 dan 5; dan 3 dan 6. Sedangkan $\rho\tau, \rho^3\tau$ dan $\rho^5\tau$ adalah pencerminan pada garis bisektor masing-masing sisi segi-6 beraturan. Bila dihitung $\lvert X_g \rvert$ untuk setiap $g \in G$ hasilnya diberikan dalam Tabel 5.3. Selanjutnya dengan menggunakan teorema Burnside didapat

$$N = 1/12(64 + 2 + 4 + 8 + 4 + 2 + 16 + 8 + 16 + 8 + 16 + 8) = 156/12 = 13.$$

Jadi banyaknya pola senyawa yang berbeda adalah 13. ●

Contoh 5.3.5 (**Masalah Dadu**) Suatu kubus diletakan pada suatu meja. Misalkan masing-

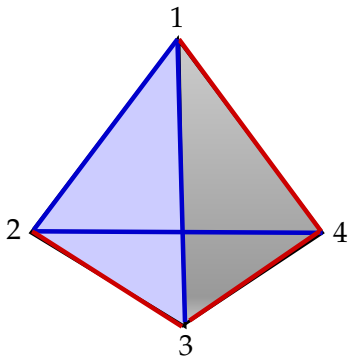


Gambar 5.8: Permukaan Dadu

masing enam sisi permukaan kubus dinamakan sisi bawah, atas, depan, belakang, kiri dan kanan. Selanjutnya dihitung banyaknya cara yang berbeda untuk menandai enam permukaan kubus dengan titik merah untuk memperoleh suatu dadu (lihat Gambar 5.8). Untuk sisi atas kubus dapat ditandai sebarang titik merah sebanyak satu sampai enam titik yang mungkin. Untuk sisi bawah dapat ditandai titik merah dari sisanya sebanyak lima yang mungkin, penandaan ini dilakukan pada semua enam sisi kubus. Dengan demikian ada sebanyak 6! = 720 cara penandaan kubus yang mungkin. Dalam hal ini X adalah himpunan penandaan kubus dengan $|X| = 720$. Untuk menentukan grup G bertindak pada X dalam contoh ini, ditinjau semua cara yang mungkin suatu kubus diletakkan pada suatu meja. Sebarang satu sisi kubus dari enam sisi yang ada dapat diletakkan pada sisi bawah dan kubus dapat diputar sehingga sebarang permukaan yang tegak dapat ditempatkan pada sisi depan. Dalam hal ini ada empat cara yang mungkin, tetapi banyaknya sisi kubus adalah

enam. Jadi $|G| = 4(6) = 24$. Bila $g \in G$ dan $g \neq e$, maka $\left|X_g\right| = 0$ sebab tidak ada dua sisi kubus yang bertanda sama. Jadi banyaknya dadu secara esensi berbeda adalah $N = 1/24\,(720) = 30$. ●

Contoh 5.3.6 Misalkan akan diwarnai rusuk tetrahedron teratur. Rusuk tetrahedron diwarnai merah atau biru. Ada sebanyak 6 rusuk, dengan demikian bila himpunan X adalah semua cara pewarnaan rusuk yang mungkin, maka $|X| = 2^6 = 64$. Sebarang satu sisi tetrahedron dari empat sisi yang ada dapat diletakkan di bagian bawah sedangkan sebarang satu dari tiga sisi sisanya dapat diletakan di bagian belakang dengan melakukan rotasi tetrahedron (lihat Gambar 5.9). Maka dari itu grup G mempunyai sebanyak $4(3) = 12$ elemen. Sebelum



Gambar 5.9: Pewarnaan Rusuk Tetrahedron

menghitung $\left|X_g\right|$ untuk masing-masing $g \in G$, maka ditentukan dulu 12 elemen dari G. Elemen-elemen dari G adalah ρ_0 merupakan elemen identitas, tiga elemen berorder 2 yaitu

$$\rho_1 = (1\ 2)(3\ 4), \qquad \rho_2 = (1\ 3)(2\ 4), \qquad \rho_3 = (1\ 4)(2\ 3)$$

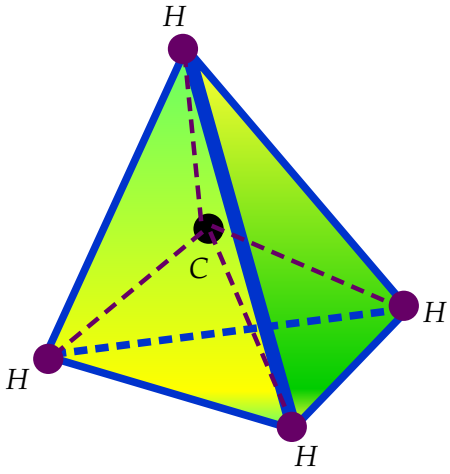
dan 8 elemen berorder 3, yaitu

$$\begin{array}{ll} \tau_1 = (1\ 3\ 4), & \tau_2 = (4)1\ 3 \\ \tau_3 = (1\ 2\ 4), & \tau_4 = (1\ 2\ 3) \\ \tau_1^{-1} = (2\ 4\ 3), & \tau_2^{-1} = (1\ 4\ 3), \\ \tau_3^{-1} = (1\ 4\ 2), & \tau_4^{-1} = (1\ 3\ 2). \end{array}$$

Faktanya, grup G isomorpik dengan grup alternating A_4. Selanjutnya ditentukan $\left|X_g\right|$ untuk masing-masing $g \in G$. Tinjau rotasi $\tau_1 = (2\ 3\ 4)$ dan misalkan suatu pewarnaan khusus di X_{τ_1}. Maka rusuk yang melalui 2-3, 3-4 dan 4-2 semuanya harus berwarna sama dan begitu juga rusuk yang melalui 1-2, 1-3 dan 1-4. Jadi $\left|X_{\tau_1}\right| = 2^2 = 4$. Perlakuan yang sama dapat dilakukan untuk sebarang 8 rotasi berorder 3. Berikutnya tinjau rotasi $\rho_1 = (1\ 2)(3\ 4)$. Karena rusuk 1-2 dan 3-4 tetap didapat $2^2 = 4$ pilihan pewarnaan. Untuk empat rusuk sisanya yaitu 1-3 dan 1-4 berubah, maka harus mempunyai warna yang sama. Hal yang sama untuk rusuk 2-3 dan 2-4. Jadi $\left|X_{\rho_1}\right| = 2^2\,2\,2 = 16$. Lagi dengan argumen yang sama berlaku untuk sebarang 3 rotasi berorder 2. Tentunya untuk identitas ρ_0 didapat $\left|X_{\rho_0}\right| = 64$. Dengan demikian didapat

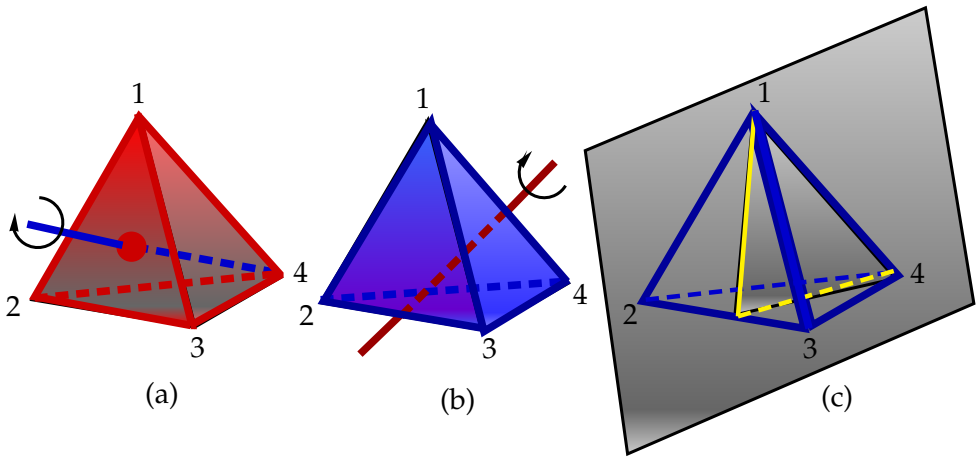
$$N = 1/12(64 + 3(16) + 8(4)) = 12. \qquad ●$$

Contoh 5.3.7 Molekul methane CH_4 terdiri dari suatu atom Carbon pada pusat suatu tetrahedron reguler yang masing-masing titik sudutnya melekat empat atom Hidrogen (lihat Gambar 5.10). Bila pada empat titik sudut tetrahedron dilekatkan H, CH_3, Cl atau C_2H_5, maka banyaknya konfigurasi senyawa kimia yang mungkin terjadi sebanyak $4^4 = 256$ molekul. Jadi himpunan X adalah himpunan semua senyawa kimia yang mungkin terjadi dari dari tetrahedron dengan lengan atom C yang keempat lengannya dapat mengikat H, CH_3, Cl atau C_2H_5 dimana $|X| = 256$. Selanjutnya untuk menentukan grup tetrahedron G yang bertindak



Gambar 5.10: Molekul Methane CH_4

pada X, diperlukan elemen-elemen dari grup G. Untuk mempermudah bagimana memper-



Gambar 5.11: Rotasi dan Refleksi Tetrahedron

oleh elemen-elemen dari G diberikan Gambar 5.11 sehingga didapat elemen-elemen dari G sebagai berikut:

(a) Satu elemen identitas $\rho_0 = ()$.

(b) Delapan rotasi $120°$ dan $240°$ berlawanan arah jarum jam terhadap sumbu yang melalui titik sudut dan titik pusat permukaan (lihat Gambar 5.11 bagian (a)). Karena ada empat

titik sudut, maka banyaknya rotasi 120° adalah 4, salah satu rotasi ini adalah (1 2 3), Dengan cara yang sama ada sebanyak 4 rotasi 240°,salah satu rotasi ini adalah (1 3 2).

(c) Tiga rotasi 180° terhadap sumbu yang melalui titik tengah rusuk yang saling berhdapan (lihat Gambar 5.11 bagian (b)). Salah satu contoh rotasi ini adalah (2 3)(1 4). Karena ada 3 pasang rusuk yang berhadapan, maka banyaknya rotasi ini adalah tiga.

(d) Enam refleksi pada bidang tegak lurus sisi (lihat Gambar 5.11 bagian (c)). Salah satu contoh refleksi ini adalah (2 3).

(e) Enam kombinasi rotasi dan refleksi, salah satu contohnya adalah (1 2 3 4).

Faktanya Grup G isomorpik dengan grup simetri S_4. Dengan demikian didapat banyaknya senyawa yang berbeda adalah

$$N = 1/24(4^4 + 6(4^3) + 11(4^2) + 6(4)) = 1/24(840) = 35. \quad \bullet$$

Contoh 5.3.8 Berapa banyaknya cara essensial berbeda yang dapat terjadi dari pewarnaan 8 titik sudut suatu kubus denganontoh n warna? Dalam hal ini himpunan X adalah memenuhi $|X| = n^8$. Sebagaimana telah dibahas dalam Contoh 5.2.7 bahwa $|G| = 24$. Selanjutnya untuk masing-masing $g \in G$ ditentukan $|X_g|$. Sebagaimana dalam Contoh 5.1.9, bila $g \in G$ adalah suatu rotasi ρ sebesar 90° atau 270° pada sumbu melalui pusat dua sisi yang berlawanan, misalnya (1 2 3 4)(5 6 7 8), maka disain dalam X_ρ semua titik 1,2,3,4 harus berwarna sama begitu juga untuk titik 5,6,7,8. Jadi banyaknya disain yang mungkin dalam X_ρ adalah n^2. Bila $g \in G$ adalah suatu rotasi σ sebesar 180° pada sumbu yang serupa, misalnya (1 3)(2 4)(5 7)(6 8), maka pasangan titik 1,3 dan 2,4 harus berwarna sama begitu juga untuk pasangan titik 5,7 dan 6,8. Maka banyaknya disain dalam X_σ yang mungkin adalah n^4. Bila $g \in G$ adalah rotasi τ sebesar 180° pada suatu sumbu yang melalui titi tengah dua rusuk yang berlawanan misalnya (1 5)(2 8)(3 7)(4 6), maka dengan argumen yang sama didapat sebanyak n^4 yang mungkin untuk disain dalam X_τ. Bila $g \in G$ adalah rotasi ϕ sebesar 120° atau 240° pada suatu sumbu yang melalui dua titi sudut yang berlawanan, misalnya (2 4 5)(3 8 6), maka titik 2,4 dan 5 harus diberi warna yang sama begitu juga untuk titik 3,8 dan 6. Sedangkan titik tetap 1 dan 7 bisa diwarnai dengan pilihan yang sebarang. Untuk hal ini banyaknya disain dalam X_ϕ yang mungkin adalah n^4. Semua hasil penghitungan yang dilakukan diringkas dalam Tabel 5.4

Tabel 5.4: Rotasi Kubus dengan n pewarnaan

Macam Rotasi	e	ρ	σ	τ	ϕ
Banyaknya Rotasi	1	6	3	6	8
$\lvert X_g \rvert$	n^8	n^2	n^4	n^4	n^4

Dengan demikian banyaknya pewarnaan yang berbeda adalah

$$N = 1/24(n^8 + 17n^4 + 6n^2). \quad \bullet$$

Latihan

Latihan 5.3.1 Dapatkan banyaknya cara yang berbeda untuk soal berikut.

1. Dari suatu permukaan sisi regular tetrahedron dibuat dadu dengan menandai satu, dua, tiga atau empat titik pada sisi permukaannya. Masing-masing penandaan titik hanya tepat terlihat satu kali.

2. Pewarnaan pada empat sisi suatu persegi bila diwarnai dengan enam warna dan satu warna hanya boleh digunakan sekali.

3. Pewarnaan dua sisi permukaan suatu tetrahedron reguler dengan warna merah dan dua sisi permukaan yang diwarnai hijau.

4. Pewarnaan dua sisi permukaan kubus dengan warna merah, dua sisi permukaan yang diwarnai biru dan sisa dua sisi permukaan diwarnai hijau.

5. Pewarnaan enam permukaan sisi suatu kubus dengan enam warna berbeda bila tujuh warna digunakan. Aturannya adalah satu warna hanya boleh digunakan satu kali.

6. Perangkaian manik-manik pada suatu kalung tiga diberi warna kuning dan enam merah dengan asumsi kalung dapat dibalik serta diputar. Manik-manik dengan warna yang sama tidak dapat dibedakan.

7. Perangkaian manik-manik pada suatu kalung satu diberi warna kuning, dua merah dan tiga biru dengan asumsi kalung dapat dibalik serta diputar. Manik-manik dengan warna yang sama tidak dapat dibedakan.

Latihan 5.3.2 Misalkan X adalah suatu himpunan dengan empat elemen. Dapatkan banyaknya relasi ekivalen pada X yang tidak ekivalen terhadap sebarang permutasi dalam S_4.

5.4 Indeks Sikel Polinomial suatu Grup

Pada bagian ini dibahas indeks sikel polinomial dari suatu grup secara umum. Setelah itu dibahas indeks sikel polinomial khusus, yaitu grup S_n, D_n, A_n dan $\mathbb{Z}_n$.

5.4.1 Indeks Sikel Polinomial suatu Permutasi

Indeks sikel dapat digunakan untuk memecahkan masalah penghitungan yang berkaitan dengan grup G. Dengan mengetahui indeks sikel polinomial suatu suatu grup dapat dihitung banyaknya orbit dari suatu himpunan tanpa harus mengetahui elemen-elemen yang tetap oleh permutasi dari G atau stabilizer dari elemen-elemen suatu himpunan.

Definisi 5.4.1 Bila $g \in S_n$ adalah komposisi dari sikel-sikel disjoint yang terdiri dari sikel panjang 1 sebanyak a_1, sikel dengan panjang 2 sebanyak a_2,..., sikel panjang n sebanyak a_n dengan $a_i \in \mathbb{Z}$ yang memenuhi

$$1a_1 + 2a_2 + \ldots + na_n = n,$$

maka tipe permutasi dari g adalah $[a_1, a_2, \ldots, a_n]$ dan indeks sikel dari g adalah

$$z(g : x_1, x_2, \ldots, x_n) = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in \mathbb{Q}[x_1, x_2, \ldots, x_n],$$

dengan $x_1, x_2, \ldots, x_n$ adalah *inderteminant*.

Contoh 5.4.1 Misalkan dalam S_3, maka

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)(2)(3) \Rightarrow \text{ terdiri dari 3 sikel dengan panjang tiap sikel 1,}$$

sehingga tipe permutasi dari e adalah $[3, 0, 0]$ dan indeks sikel dari e adalah $x_1^3 x_2^0 x_3^0 = x_1^3$.

$$f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3) \Rightarrow \text{ terdiri dari 1 sikel dengan panjang 3,}$$

sehingga tipe permutasi dari f adalah $[0, 0, 1]$ dan indeks sikel dari f adalah $x_1^0 x_2^0 x_3^1 = x_3$.

$$g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2) \Rightarrow \text{ terdiri dari 1 sikel dengan panjang 3,}$$

sehingga tipe permutasi dari g adalah $[0, 0, 1]$ dan indeks sikel dari g adalah $x_1^0 x_2^0 x_3^1 = x_3$.

$$h = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(2\ 3) \Rightarrow \text{ terdiri dari 2 sikel masing-masing dengan panjang 1 dan 2,}$$

sehingga tipe permutasi dari h adalah $[1, 1, 0]$ dan indeks sikel dari h adalah $x_1^1 x_2^1 x_3^0 = x_1 x_2$.

$$i = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2)(3) \Rightarrow \text{ terdiri dari 2 sikel masing-masing dengan panjang 2 dan 1,}$$

sehingga tipe permutasi dari i adalah $[1, 1, 0]$ dan indeks sikel dari i adalah $x_1^1 x_2^1 x_3^0 = x_1 x_2$.

$$j = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\ 3)(2) \Rightarrow \text{ terdiri dari 2 sikel masing-masing dengan panjang 2 dan 1,}$$

sehingga tipe permutasi dari j adalah $[1, 1, 0]$ dan indeks sikel dari j adalah $x_1^1 x_2^1 x_3^0 = x_1 x_2$. ●

Definisi 5.4.2 Bila $G \leq S_n$, maka indeks sikel polinomial dari grup G adalah

$$Z(G; x_1, x_2, \ldots, x_n) = \frac{1}{|G|} \sum_{g \in G} z(g) = \frac{1}{|G|} \sum_{g \in G} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \in \mathbb{Q}[x_1, x_2, \ldots, x_n],$$

dengan $z(g)$ adalah indeks sikel polinomial dari elemen $g \in G$.

Contoh 5.4.2 Dengan menjumlahkan semua indeks sikel dari semua elemen di S_3 pada Contoh 5.4.1 lalu dibagi oleh $|S_3|$, maka indeks sikel dari $G = S_3$ adalah

$$Z(S_3; x_1, x_2, x_3) = \frac{1}{|S_3|} \sum_{g \in S_3} z(g) = \frac{1}{6}(x_1^3 + 3x_1 x_2 + 2x_3)$$

Tabel 5.5: Indeks Sikel Polinomial Elemen S_4

Elemen	Notasi Sikel	Tipe Permutasi	Indeks Sikel
a	(1)(2)(3)(4)	$[4,0,0,0]$	x_1^4
b	(1 2 3 4)	$[0,0,0,1]$	x_4
c	(1 3)(2 4)	$[0,2,0,0]$	x_2^2
d	(1 4 3 2)	$[0,0,0,1]$	x_4
e	(1)(2 3)(4)	$[2,1,0,0]$	$x_1^2x_2$
f	(1)(2 3 4)	$[1,0,1,0]$	x_1x_3
g	(1)(2 4)(3)	$[2,1,0,0]$	$x_1^2x_2$
h	(1)(2 4 3)	$[1,0,1,0]$	x_1x_3
i	(1)(2)(3 4)	$[2,1,0,0]$	$x_1^2x_2$
j	(1 2)(3 4)	$[0,2,0,0]$	x_2^2
k	(1 2)(3)(4)	$[2,1,0,0]$	$x_1^2x_2$
l	(1 2 3)(4)	$[1,0,1,0]$	x_1x_3
m	(1 2 4)(3)	$[1,0,1,0]$	x_1x_3
n	(1 2 4 3)	$[0,0,0,1]$	x_4
o	(1 3 2)(4)	$[1,0,1,0]$	x_1x_3
p	(1 3 4 2)	$[0,0,0,1]$	x_4
q	(1 3 2 4)	$[0,0,0,1]$	x_4
r	(1 3)(2)(4)	$[2,1,0,0]$	$x_1^2x_2$
s	(1 3 4)(2)	$[1,0,1,0]$	x_1x_3
t	(1 4)(2 3)	$[0,2,0,0]$	x_2^2
u	(1 4 2)(3)	$[1,0,1,0]$	x_1x_3
v	(1 4 3)(2)	$[1,0,1,0]$	x_1x_3
w	(1 4)(2)(3)	$[2,1,0,0]$	$x_1^2x_2$
x	(1 4 2 3)	$[0,0,0,1]$	x_4

Contoh 5.4.3 Misalkan $X = \{1,2,3,4\}$, maka order grup simetri dari himpunan X adalah $|S_4| = 4! = 24$. Elemen-elemen dari S_4 beserta indeks sikelnya diberikan oleh Tabel 5.5.

Dari Tabel 5.5 didapat indeks sikel dari S_4 sebagai berikut

$$\begin{aligned} Z(S_4; x_1, x_2, x_3, x_4) &= \frac{1}{|S_4|}\sum_{g\in S_4} z(g) \\ &= \frac{1}{24}(x_1^4 + 8x_1x_3 + 6x_1^2x_2 + 3x_2^2 + 6x_4). \end{aligned}$$

Contoh 5.4.4 Sebagaimana telah diketahui grup alternating A_n yang merupakan himpunan semua permutasi genap adalah subgrup dari grup permutasi S_n. Dari Tabel 5.5, didapat

$$A_4 = \{a, c, f, h, j, l, m, o, s, t, u, v\},$$

sehingga indeks sikel dari A_4 adalah

$$Z(A_4; x_1, x_2, x_3, x_4) = \frac{1}{12}(x_1^4 + 3x_2^2 + 8x_1x_3).$$

Contoh 5.4.5 Grup permutasi siklik berorder n (C_n) yang merupakan subgrup dari S_n adalah himpunan semua permutasi yang bersesuaian dengan rotasi dari segi-n beraturan. Dalam hal ini, sebagaimana telah diketahui $C_n \cong \mathbb{Z}_n$ dengan demikian indeks sikel dari C_n dan $\mathbb{Z}_n$ adalah sama. Dari Tabel 5.5 didapat $C_4 = \{a, b, c, d\}$, sehingga indeks sikel dari $\mathbb{Z}_4$ adalah

$$Z(\mathbb{Z}_4; x_1, x_2, x_3, x_4) = Z(C_4; x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + x_2^2 + 2x_4).$$

Contoh 5.4.6 Grup permutasi Dihedral beorder $2n$ (D_n) yang merupakan subgrup dari S_n adalah himpunan semua permutasi yang bersesuaian dengan rotasi dan pencerminan dari segi-n beraturan. Dari Tabel 5.5 didapat $D_4 = \{a, b, c, d, g, j, r, t\}$, sehingga indeks sikel dari D_4 adalah

$$Z(D_4; x_1, x_2, x_3, x_4) = \frac{1}{8}(x_1^4 + 2x_1^2x_2 + 3x_2^2 + 2x_4).$$

Indeks sikel polinomial yang diberikan oleh Definisi 5.4.1 adalah indeks sikel dari suatu grup yang merupakan subgrup dari S_n. Secara umum grup tersebut bisa berupa C_n, A_n dan D_n ataupun S_n sendiri. Dalam aplikasinya untuk menghitung indeks sikel dari sembarang grup G dengan menggunakan Definisi 5.4.1, langkah pertama harus dicari subgrup dari S_n yang isomorpik dengan G. Lalu dibahas elemen-elemen dari subgrup S_n. Sehingga bila ordernya cukup besar akan membutuhkan waktu yang cukup lama. Namum ada cara lain untuk menghitung indeks sikel suatu grup yaitu dengan menggunakan rumus indeks sikel khusus untuk grup S_n, D_n, C_n dan A_n. Karena sebarang grup berhingga G isomorpik dengan suatu subgrup dari grup permutasi S_n yaitu salah satu dari S_n, D_n, C_n atau A_n yang sudah dapat dihitung indeks sikelnya. Maka, indeks sikel dari G dapat dihitung melalui subgrup dari S_n yang isomorpik dengan G. Oleh karena itu pada bagian berikutnya dibahas indeks sikel dari grup S_n, A_n, C_n dan D_n.

5.5 Indeks Sikel Polinomial dari S_n

Grup permutasi S_n yang anggotanya semua permutasi dari suatu himpunan X dengan $|X| = n$. Banyaknya permutasi type

$$1^{a_1}2^{a_2}3^{a_3}\cdots n^{a_n}$$

atau dapat ditulis sebagai

$$[a_1, a_2, a_3, \ldots, a_n]$$

dari suatu himpunan X dengan n elemen adalah

$$\frac{n!}{(1^{a_1}a_1!)(2^{a_2}a_2!)(3^{a_3}a_3!)\cdots(n^{a_n}a_n!)} \tag{5.1}$$

dengan $1a_1 + 2a_2 + 3a_3 + \cdots + na_n = n$ dan a_i adalah banyaknya sikel dengan panjang i, $a_i \geq 0$.

Contoh 5.5.1 Misalkan $X = \{1, 2, 3\}$, maka banyaknya permutasi di S_3 yang terdiri dari 1 sikel dengan panjang dua dan 1 sikel dengan panjang satu atau bertipe $1^12^13^0$ atau $[1, 1, 0]$ adalah

$$\frac{3!}{(1^11!)(2^11!)(3^00!)} = \frac{6}{2} = 2.$$

Jadi banyaknya permutasi yang bertipe 1 sikel dengan panjang dua dan 1 sikel dengan panjang satu ada 3. Hal sesuai dalam bahasan pada Contoh 5.4.1 yaitu permutasi (1 2)(3), (1 3)(2) dan (2 3)(1). ●

Berdasarkan Persamaan 5.5, maka didapat rumus indeks sikel polinomial dari S_n yaitu

$$\begin{aligned} Z(G; x_1, x_2, \ldots, x_n) &= \frac{1}{|G|}\sum_{g\in G} z(g) \\ &= \frac{1}{G}\sum_{g\in G} x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \\ Z(S_n; x_1, x_2, \ldots, x_n) &= \frac{1}{n!}\sum_{g\in S_n} x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \\ &= \frac{1}{n!}\sum_{*} \frac{n!}{(1^{a_1}a_1!)(2^{a_2}a_2!)(3^{a_3}a_3!)\cdots(n^{a_n}a_n!)} x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n} \\ &= \sum_{*} \frac{1}{(1^{a_1}a_1!)(2^{a_2}a_2!)(3^{a_3}a_3!)\cdots(n^{a_n}a_n!)} x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}, \end{aligned} \tag{5.2}$$

dengan $*$ adalah penjumlahan berlaku untuk semua $(a_1, a_2, \ldots, a_n)$ yang memenuhi $1a_1 + 2a_2 + 3a_3 + \ldots + na_n = n$.

Contoh 5.5.2 Dihitung indeks sikel polinomial dari S_4 menggunakan Persamaan 5.5. Tipe permutasi yang memenuhi

$$1a_1 + 2a_2 + 3a_3 + 4a_4 = 4$$

ada 5, selengkapnya diberikan oleh Tabel 5.6.

Tabel 5.6: Indeks Sikel Polinomial Elemen S_4

Tipe Permutasi		$\frac{1}{(1^{a_1}a_1!)(2^{a_2}a_2!)(3^{a_3}a_3!)(4^{a_4}a_4!)} x_1^{a_1}x_2^{a_2}x_3^{a_3}x_4^{a_4}$	
$[4,0,0,0]$	$a_1 = 4, a_2 = a_3 = a_4 = 0$	$\frac{1}{(1^4 4!)(2^0 0!)(3^0 0!)(4^0 0!)} x_1^4 x_2^0 x_3^0 x_4^0$	$\frac{1}{24}x_1^4$
$[1,0,1,0]$	$a_1 = a_3 = 1, a_2 = a_4 = 0$	$\frac{1}{(1^1 1!)(2^0 0!)(3^1 1!)(4^0 0!)} x_1^1 x_2^0 x_3^1 x_4^0$	$\frac{1}{3}x_1x_3$
$[2,1,0,0]$	$a_1 = 2, a_2 = 1, a_3 = a_4 = 0$	$\frac{1}{(1^2 2!)(2^1 1!)(3^0 0!)(4^0 0!)} x_1^2 x_2^1 x_3^0 x_4^0$	$\frac{1}{4}x_1^2x_2$
$[0,2,0,0]$	$a_2 = 2, a_1 = a_3 = a_4 = 0$	$\frac{1}{(1^0 0!)(2^2 2!)(3^0 0!)(4^0 0!)} x_1^0 x_2^2 x_3^0 x_4^0$	$\frac{1}{8}x_2^2$
$[0,0,0,1]$	$a_1 = a_2 = a_3 = 0, a_4 = 1$	$\frac{1}{(1^0 0!)(2^0 0!)(3^0 0!)(4^1 1!)} x_1^0 x_2^0 x_3^0 x_4^1$	$\frac{1}{4}x_4$

Sehingga didapat

$$\begin{aligned} Z(S_4; x_1, x_2, x_3, x_4) &= \frac{1}{24}x_1^4 + \frac{1}{3}x_1x_3 + \frac{1}{4}x_1^2x_2 + \frac{1}{8}x_2^2 + \frac{1}{4}x_4 \\ &= \frac{1}{24}(x_1^4 + 8x_1x_3 + 6x_1^2x_2 + 3x_2^2 + 6x_4). \end{aligned}$$

Terlihat hasil yang didapat sama seperti pada pembahasan Contoh 5.4.3. ●

5.6 Indeks Sikel Polinomial dari A_n

Sebagaimana telah diketahui bahwa A_n adalah subrup dari S_n yang anggotanya merupakan semua permutasi genap dalam S_n. Setiap permutasi genap dalam S_n dapat dinyatakan sebagai komposisi dari transposisi yang banyaknya genap dan setiap sikel dengan panjang ganjil dapat dibentuk menjadi transposisi yang banyaknya ganjil. Dengan demikian bila jumlahan

$$a_2 + a_4 + a_6 + \dots$$

menghasilkan genap, maka transposisi yang bisa dibentuk dari tipe tersebut banyaknya genap. Jadi tipe permutasi tersebut adalah genap dan merupakan elemen di A_n. Tetapi bila jumlahan

$$a_2 + a_4 + a_6 + \dots$$

menghasilkan ganjil, maka transposisi yang bisa dibentuk dari tipe tersebut banyaknya ganjil. Jadi tipe permutasi tersebut adalah ganjil dan bukan elemen di A_n. Sehingga untuk membentuk A_n semua permutasi yang ganjil di S_n dihilangkan. Dengan demikian dapat dibentuk $1 + (-1)^{a_2+a_4+a_6+\cdots}$ untuk mempertahankan atau menghilangkan suatu permutasi di S_n. Bila $a_2 + a_4 + a_6 + \dots$ menghasilkan nilai genap ini berarti $1 + (-1)^{a_2+a_4+a_6+\cdots} = 2$ dan tipe permutasi yang terbentuk genap, jadi merupakan elemen di A_n. Sebaliknya bila $a_2+a_4+a_6+\dots$ menghasilkan nilai ganjil atau $1 + (-1)^{a_2+a_4+a_6+\cdots} = 0$, maka tipe permutasi yang terbentuk bukan elemen di A_n sehingga permutasi ini harus dihilangkan dari S_n. Untuk $a_2 + a_4 + a_6 + \dots$ yaitu $1 + (-1)^{a_2+a_4+a_6+\cdots} = 2$ hal ini disebabkan oleh $|A_n| = \frac{n!}{2} = \frac{1}{2}|S_n|$. Dari hasil yang dibahas ini dan berdasarkan Persamaan 5.2, maka indeks sikel dari A_n diberikan oleh persamaan berikut

$$Z(A_n; x_1, x_2, \dots, x_n) = \sum_{*} \frac{1 + (-1)^{a_2+a_4+a_6+\dots}}{(1^{a_1}a_1!)(2^{a_2}a_2!)(3^{a_3}a_3!)\cdots(n^{a_n}a_n!)} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}, \tag{5.3}$$

dengan $*$ adalah penjumlahan berlaku untuk semua $(a_1, a_2, \dots, a_n)$ yang memenuhi $1a_1 + 2a_2 + \cdots + na_n = n$.

Contoh 5.6.1 Pada contoh ini dibahas indeks sikel polinomial dari A_4 dengan menggunakan rumus indeks sikel polinomial dari A_n. Tipe indeks sikel yang memenuhi $1a_1+2a_2+3a_3+4a_4 = 4$ ada 5, secara lengkap diberikan oleh Tabel 5.7.

Tabel 5.7: Indeks Sikel Polinomial Elemen A_4

Tipe Permutasi		$\frac{1+(-1)^{a_2+a_4}}{(1^{a_1}a_1!)(2^{a_2}a_2!)(3^{a_3}a_3!)(4^{a_4}a_4!)} x_1^{a_1}x_2^{a_2}x_3^{a_3}x_4^{a_4}$	
$[4,0,0,0]$	$a_1 = 4, a_2 = a_3 = a_4 = 0$	$\frac{1+(-1)^0}{(1^4 4!)(2^0 0!)(3^0 0!)(4^0 0!)} x_1^4 x_2^0 x_3^0 x_4^0$	$\frac{2}{24}x_1^4$
$[1,0,1,0]$	$a_1 = a_3 = 1, a_2 = a_4 = 0$	$\frac{1+(-1)^0}{(1^1 1!)(2^0 0!)(3^1 1!)(4^0 0!)} x_1^1 x_2^0 x_3^1 x_4^0$	$\frac{2}{3}x_1x_3$
$[2,1,0,0]$	$a_1 = 2, a_2 = 1, a_3 = a_4 = 0$	$\frac{1+(-1)^1}{(1^2 2!)(2^1 1!)(3^0 0!)(4^0 0!)} x_1^2 x_2^1 x_3^0 x_4^0$	0
$[0,2,0,0]$	$a_2 = 2, a_1 = a_3 = a_4 = 0$	$\frac{1+(-1)^2}{(1^0 0!)(2^2 2!)(3^0 0!)(4^0 0!)} x_1^0 x_2^2 x_3^0 x_4^0$	$\frac{2}{8}x_2^2$
$[0,0,0,1]$	$a_1 = a_2 = a_3 = 0, a_4 = 1$	$\frac{1+(-1)^1}{(1^0 0!)(2^0 0!)(3^0 0!)(4^1 1!)} x_1^0 x_2^0 x_3^0 x_4^1$	0

Sehingga didapat

$$\begin{aligned} Z(A_4; x_1, x_2, x_3, x_4) &= \frac{2}{24}x_1^4 + \frac{2}{3}x_1x_3 + \frac{2}{8}x_2^2 \\ &= \frac{1}{12}(x_1^4 + 8x_1x_3 + 3x_2^2). \end{aligned}$$

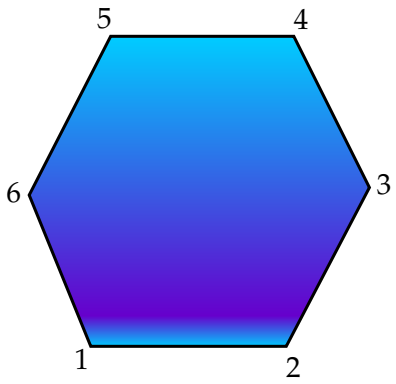
Terlihat hasil yang didapat sama seperti pada pembahasan Contoh 5.4.4. ●

5.7 Indeks Sikel Polinomial C_n

Dari pembahasan sebelumnya telah diketahui bahwa grup siklik permutasi C_n dengan order n adalah subgrup dari S_n yang semua anggotanya merupakan hasil dari semua rotasi segi-n beraturan terhadap titik pusat. Sehingga setiap anggota dari C_n dapat dinyatakan kedalam suatu komposisi sikel-sikel saling asing dengan panjang yang sama dan merupakan faktor dari n.

Contoh 5.7.1

★ Rotasi dari segi-6 beraturan ada 6 yaitu :

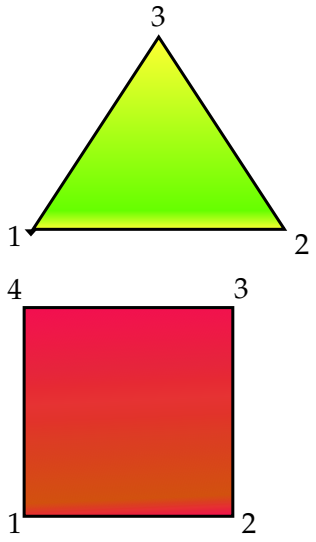


- ♣ (1)(2)(3)(4)(5)(6)
- ♣ (1 2 3 4 5 6)
- ♣ (1 3 5)(2 4 6)
- ♣ (1 4)(2 5)(3 6)
- ♣ (1 5 3)(2 6 4)
- ♣ (1 6 5 4 3 2)

★ Rotasi dari segi-3 beraturan ada tiga yaitu

- ▲ (1)(2)(3)
- ▲ (1 2 3)
- ▲ (1 3 2)

★ Rotasi dari segi-4 beraturan ada 4 yaitu



- (1)(2)(3)(4)
- (1 2 3 4)
- (1 3)(2 4)
- (1 4 3 2)

Dari hasil pembahasan contoh terlihat bahwa suatu rotasi terhadap titik pusat segi-n beraturan banyaknya selalu n dan setiap hasil rotasinya dapat dinyatakan sebagai komposisi sikel-sikel yang saling asing dengan panjang sama dan merupakan faktor dari n. Dari apa yang dibahas ini, maka dengan cepat dapat dihtung indeks sikel polinomial dari C_n dengan cara mencari bilangan bulat d dengan $1 \leq d \leq n$ yang merupakan faktor dari n. Dalam hal ini elemen di C_n yang berorder d sebanyak $\varphi(d)$ dengan φ adalah fungsi-phi Euler. Juga, panjang sikel-sikel dari suatu permutasi yang bersesuaian dengan rotasi segi-n beraturan senuanya sama, sehingga banyaknya sikel dengan panjang d adalah $\frac{n}{d}$. Dengan demikian didapat

$$\begin{aligned} Z(C_n; x_1, x_2, \ldots, x_n) &= \frac{1}{|C_n|} \sum_{g \in C_n} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \\ &= \frac{1}{n} \sum_{g \in C_n} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \\ &= \frac{1}{n} \sum_{d|n} \varphi(d) x_d^{\frac{n}{d}} \end{aligned} \tag{5.4}$$

Contoh 5.7.2 Dalam contoh ini dihitung indeks polinomial dari C_4 dengan menggunakan rumus indeks sikel polinomial untuk C_n yaitu Persamaan (5.4). Langkah pertama dicari d yang merupakan faktor dari n dengan $1 \leq d \leq n$, kemudia dihitung $\varphi(d)$. Hasil selengkapnya diberikan oleh Tabel 5.8.
Dari Tabel 5.8 didapat indeks sikel polinomial dari C_4 sebagai berikut

$$Z(C_4; x_1, x_2, x_3, x_4) = \frac{1}{|C_4|} \sum_{d|n} \varphi(d) x_d^{\frac{n}{d}} = \frac{1}{4}(x_1^4 + x_2^2 + 2x_4),$$

Tabel 5.8: Indeks Sikel Polinomial Elemen C_4

d	$\varphi(d)$	$x_d^{\frac{n}{d}}$
1	1	x_1^4
2	1	x_2^2
4	2	x_4

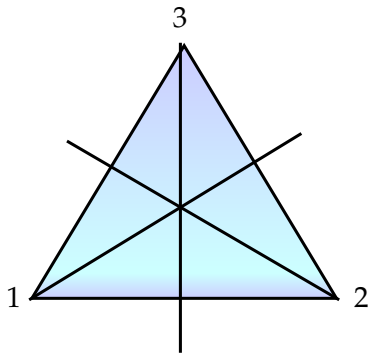
terlihat hasilnya sama seperti pada pembahasan dalam Contoh 5.7.2. ●

5.8 Indeks Sikel Polinomial dari D_n

Grup permutasi Dihedral D_n berorder $2n$ yang merupakan subgrup dari S_n adalah himpunan semua permutasi yang bersesuaian dengan rotasi dan pencerminan dari segi-n beraturan.

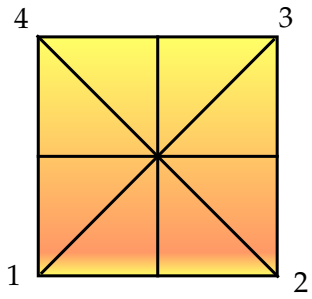
Contoh 5.8.1

- Banyaknya refleksi pada segi-3 beraturan ada 3 yaitu



  - ☑ (1)(2 3)
  - ☑ (2)(1 3)
  - ☑ (3)(1 2)

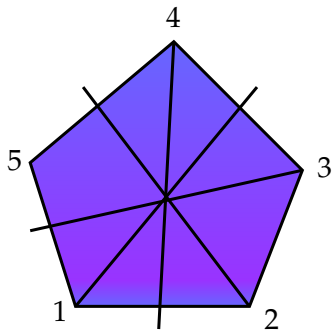
- Banyaknya refleksi pada segi-4 beraturan adalah



  - ☑ (1 2)(3 4)

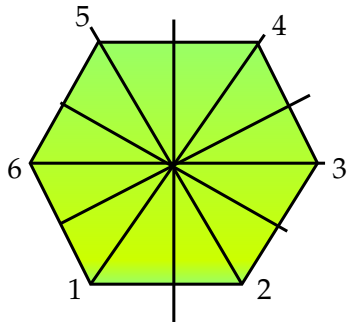
- (1 4)(2 3)
- (1)(3)(2 4)
- (2)(4)(1 3)

♦ Banyaknya refleksi pada segi-5 beraturan adalah



- (1)(2 5)(3 4)
- (2)(1 3)(4 5)
- (3)(1 5)(2 4)
- (4)(1 2)(3 5)
- (5)(1 4)(2 3)

♦ Banyaknya refleksi pada segi-6 beraturan adalah



- (1 6)(2 5)(3 4)
- (1 4)(2 3)(5 6)
- (1 2)(3 6)(4 5)
- (2)(5)(1 3)(4 6)
- (3)(6)(1 5)(2 4)
- (1)(4)(2 6)(3 5)

Dari apa yang dibahas dalam Contoh 5.8.1 terlihat bahwa refleksi dari segi-n beraturan ada n, dan bila n ganjil maka setiap permutasi yang bersesuaian dapat ditulis sebagai $(a)(b\ c)(d\ e)\cdots(m\ n)$ dengan banyaknya transposisi adalah $\frac{n-1}{2}$. Karena tipe permutasi tersebut ada sebanyak n, maka indeks sikel dari semua anggota yang bersesuaian dengan refleksi

dari segi-n beraturan adalah $nx_1x_2^{\frac{n-1}{2}}$. Sedangkan bila n genap refleksi yang terbentuk ada 2 yaitu

1. $(a\,b)(c\,d)\cdots(m\,n)$ komposisi dari transposisi sebanyak $\frac{n}{2}$. Tipe semacam ini ada sebanyak $\frac{n}{2}$, sehingga indeks sikelnya $\frac{n}{2}x_2^{\frac{n}{2}}$.
2. $(a)(b)(c\,d)(e\,f)\cdots(m\,n)$ komposisi dua sikel dengan panjang dengan panjang satu sebagai dua titik yang terletak pada sumbu simetri dan transposisi sebanyak $\frac{n-2}{2}$. Tipe semacam ini ada $\frac{n}{2}$, sehingga indeks sikel dari tipe tersebut adalah $\frac{n}{2}x_1^2x_2^{\frac{n-2}{2}}$.

Jadi indeks sikel dari anggota yang bersesuaian dengan refleksi pada segi-n beraturan adalah

$$nx_1x_2^{\frac{n-1}{2}},$$

untuk n ganjil,

$$\frac{n}{2}x_2^{\frac{n}{2}}+\frac{n}{2}x_1^2x_2^{\frac{n-2}{2}},$$

untuk n genap.

Karena semua anggota D_n bersesuaian dengan hasil dari rotasi dan refleksi pada segi-n beraturan dan $|D_n|=2n$, maka indeks sikel polinomial dari D_n adalah

$$\begin{aligned}
Z(D_n;x_1,x_2,\ldots,x_n) &= \frac{1}{2n}\sum_{g\in D_n}x_1^{a_1}x_2^{a_2}\cdots x_n^{a_n}\\
&= \begin{cases}\frac{1}{2n}\left(\sum_{d|n}\varphi(d)x_d^{\frac{n}{d}}+nx_1x_2^{\frac{n-1}{2}}\right), & \text{untuk } n \text{ ganjil}\\ \frac{1}{2n}\left(\sum_{d|n}\varphi(d)x_d^{\frac{n}{d}}+\frac{n}{2}x_2^{\frac{n}{2}}+\frac{n}{2}x_1^2x_2^{\frac{n-2}{2}}\right), & \text{untuk } n \text{ genap}\end{cases}\\
&= \begin{cases}\frac{1}{2}Z(C_n;x_1,\ldots,x_n)+\frac{1}{2}x_1x_2^{\frac{n-1}{2}}, & \text{untuk } n \text{ ganjil}\\ \frac{1}{2}Z(C_n;x_1,\ldots,x_n)+\frac{1}{4}\left(x_2^{\frac{n}{2}}+x_1^2x_2^{\frac{n-2}{2}}\right), & \text{untuk } n \text{ genap.}\end{cases}
\end{aligned} \tag{5.5}$$

Contoh 5.8.2 Pada contoh dihitung indeks sikel polinomial dari D_4 dengan menggunakan rumus pada Persamaan 5.5. Dengan menggunakan $Z(C_4;x_1,x_2,x_3,x_4)$ pada Contoh 5.7.2 dan karena 4 adalah genap, maka indeks sikel polinomial dari D_4 adalah

$$\begin{aligned}
Z(D_4;x_1,x_2,x_3,x_4) &= \frac{1}{2}Z(C_4;x_1,x_2,x_3,x_4)+\frac{1}{4}(x_2^{\frac{4}{2}}+x_1^2x_2^{\frac{4-2}{2}})\\
&= \frac{1}{2}\left(\frac{1}{4}(x_1^4+x_2^2+2x_4)\right)+\frac{1}{4}(x_2^2+x_1^2x_2^1)\\
&= \frac{1}{8}(x_1^4+2x_1^2x_2+3x_2^2+2x_4),
\end{aligned}$$

terlihat hasilnya sama seperti hasil yang dibahas dalam Contoh 5.4.6. ●

Beberapa hasil yang telah dibahas diringkas dalam Tabel 5.9 yang mana akan beerguna dalam pembahasan berikutnya tentang Teorema Polya.

Tabel 5.9: Indeks Sikel Polinomial Suatu Grup

Group	Indeks Sikel Polinomial
$G \leq S_n$	$\frac{1}{\lvert G\rvert}\sum_{g\in G} z(g) = \frac{1}{\lvert G\rvert}\sum_{g\in G} x_1^{a_1}x_2^{a_2}x_3^{a_3}\cdots x_n^{a_n}$
S_n	$\sum_{*} \frac{1}{(1^{a_1}a_1!)(2^{a_2}a_2!)(3^{a_3}a_3!)\cdots(n^{a_n}a_n!)} x_1^{a_1}x_2^{a_2}x_3^{a_3}\cdots x_n^{a_n}$
A_n	$\sum_{*} \frac{1+(-1)^{a_2+a_4+a_6+\ldots}}{(1^{a_1}a_1!)(2^{a_2}a_2!)(3^{a_3}a_3!)\cdots(n^{a_n}a_n!)} x_1^{a_1}x_2^{a_2}x_3^{a_3}\cdots x_n^{a_n}$
C_n	$\frac{1}{n}\sum_{d\mid n}\varphi(d)x_d^{\frac{n}{d}}$
D_n	$\begin{cases} \frac{1}{2}Z(C_n;x_1,x_2,x_3\ldots,x_n) + \frac{1}{2}x_1x_2^{\frac{n-1}{2}}, & \text{untuk } n \text{ ganjil} \\ \frac{1}{2}Z(C_n;x_1,x_2,x_3\ldots,x_n) + \frac{1}{4}\left(x_2^{\frac{n}{2}} + x_1^2x_2^{\frac{n-2}{2}}\right), & \text{untuk } n \text{ genap.} \end{cases}$

5.9 Teorema Polya

Pada bagian ini dibahas tentang Teorema Polya. Ada dua Teorema Polya, yaitu Teorema Polya I dan Teorema Polya II atau dikenal dengan nama Teorema Redfield-Polya. Teorema Polya I dapat digunakan untuk menghitung banyaknya orbit yang berbeda sebagaimana pada Teorema 5.3.1 (Teorema Burnside), terutama untuk mendapatkan banyaknya pola yang berbeda. Sedangkan Teorema Polya II selain dapat digunakan untuk menentukan banyaknya pola yang berbeda juga dapat menentukan karakteristik atau bentuk dari pola atau orbit yang berbeda tersebut [15].

5.9.1 Teorema Polya I

George Polya menemukan suatu cara untuk metode penghitungan orbit dari suatu grup pada suatu konfigurasi. Metode ini sering sering disebut dengan metode PET (Polya Enumeration Theorem). Dengan menggunakan metode ini dapat dicari banyaknya orbit yang berbeda dari suatu himpunan tak-kosong X terhadap suatu grup G yang bertindak pada himpunan tersebut.

Teorema 5.9.1

Diberikan $C = \{f \mid f : X \to Y\}$ dengan $|X| \geq 2$ dan $|Y| = r$. Bila $G \leq S_n$ yang bertindak pada C dengan indeks sikel $Z(G; x_1, x_2, x_3, \ldots, x_n)$, maka banyaknya orbit atau pola berbeda di C terhadap G adalah $Z(G; r, r, r, \ldots, r)$.

Bukti
Bila $g \in G$, maka $\in X_g \Leftrightarrow f$ tetap oleh tindakan setiap sikel dari g. Bila g adalah suatu permutasi dengan tipe $[a_1, a_2, a_3, \ldots, a_n]$, maka $a_1 + a_2 + a_3 + \cdots + a_n$ menyatakan banyaknya sikel yang saling asing di g. Dengan demikian banyaknya permutasi yang tetap oleh g adalah $r^{a_1+a_2+a_3+\cdots+a_n}$. Jadi $|X_g| = r^{a_1+a_2+a_3+\cdots+a_n}$, dengan $[a_1, a_2, a_3, \ldots, a_n]$ adalah tipe dari permutasi g.

Berdasarkan Teorema 5.3.1 (Burside), banyaknya orbit yang berbeda adalah

$$\begin{aligned} N &= \frac{1}{|G|}\sum_{g\in G}|C_g| \\ &= \frac{1}{|G|}\sum_{g\in G} r^{a_1+a_2+a_3+\cdots+a_n} \\ &= \frac{1}{|G|}\sum_{g\in G} r^{a_1}r^{a_2}r^{a_3}\ldots r^{a_n} \\ &= \frac{1}{|G|}\sum_{g\in G} z(g;r,r,r,\ldots,r) \\ &= Z(G;r,r,r,\ldots,r) \end{aligned}$$

Contoh 5.9.1

Dibahas ulang Contoh 5.3.4, menentukan ada berapa banyak senyawa organik yang terjadi dari suatu proses kimia yang mungkin. Dari satu rantai karbon terdiri dari enam atom karbon C dikaitkan dengan satu atom hidrogen H dan satu molekul CH_3 dalam pembahasannya menggunakan Teorema Burnside. Disini dibahas dengan menggunakan Teorema Polya I. Sebagaimana telah dibahas dalam Contoh 5.3.4 grup $G \leq S_n$ adalah $G = D_6$, $X = \{1,2,3,4,5,6\}$ dan $Y = \{H, CH_3\}$. Jadi $|X| = 6$ dan $|Y| = r = 2$. Sehingga indeks sikel polinomial dari D_6 adalah

$$\begin{aligned} Z(D_6,x_1,x_2,x_3,\ldots,x_6) &= \frac{1}{12}\sum_{g\in D_6} z(g;x_1,x_2,x_3,\ldots,x_n) \\ &= \frac{1}{12}\left(\sum_{d|6}\varphi(d)x_d^{\frac{6}{d}} + \frac{6}{2}x_2^{\frac{6}{2}} + \frac{6}{2}x_1^2x_2^{\frac{6-2}{2}}\right) \\ &= \frac{1}{12}\left(\phi(1)x_1^6 + \phi(2)x_2^3 + \phi(3)x_3^2 + \phi(6)x_6 + 3x_2^3 + 3x_1^2x_2^2\right) \\ &= \frac{1}{12}\left(x_1^6 + x_2^3 + 2x_3^2 + 2x_6 + 3x_2^3 + 3x_1^2x_2^2\right) \\ &= \frac{1}{12}\left(x_1^6 + 4x_2^3 + 2x_3^2 + 3x_1^2x_2^2 + 2x_6\right). \end{aligned}$$

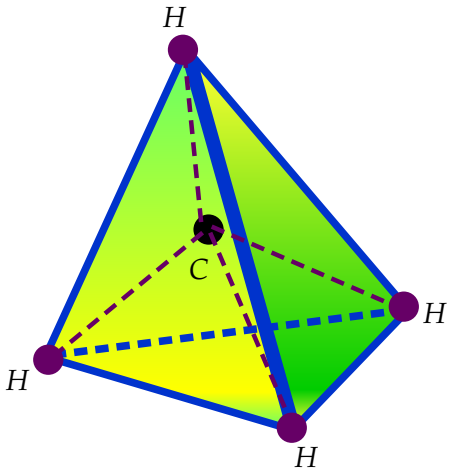
Dengan menggunakan Teorema Polya I didapat banyaknya pola yang berbeda adalah

$$\begin{aligned} N &= \frac{1}{12}\sum_{g\in D_6} z(g;r,r,r,r,r,r) \\ &= \frac{1}{12}\sum_{g\in D_6} z(g;2,2,2,2,2,2) \\ &= \frac{1}{12}\left(2^6 + 4\,(2^3) + 2\,(2^2) + 3\,(2^2 2^2) + 2\,(2)\right) \\ &= \frac{1}{12}(64 + 32 + 8 + 48 + 4) \\ &= \frac{156}{12} = 13. \end{aligned}$$

Jadi banyaknya senyawa yang mungkin terjadi adalah 13, hasilnya ini sama seperti dalam pembahasan Contoh 5.3.4. ●

Contoh 5.9.2

Dibahas ulang Contoh 5.3.7, menentukan ada berapa banyak senyawa yang terjadi dari suatu proses kimia yang mungkin. Yaitu suatu tetrahedron dengan satu atom karbon C sebagai titik pusat. Masing-masing empat titik sudut tetrahedron dikaitkan dengan satu



Gambar 5.12: Molekul Methane CH_4

atom hidrogen H, molekul CH_3, satu atom Cl dan molekul C_2H_5 dalam pembahasannya menggunakan Teorema Burnside. Disini dibahas dengan menggunakan Teorema Polya I. Sebagaimana telah dibahas dalam Contoh 5.3.7 grup $G \leq S_n$ adalah $G \cong S_4$, $X = \{1, 2, 3, 4\}$ dan $Y = \{H, CH_3, Cl, C_2H_5\}$. Jadi $|X| = 4$ dan $|Y| = r = 4$. Misalkan $C = \{f \mid f : X \to Y\}$, disini X adalah titik sudut dari tetrahedron atau lengan dari atom karbon C yang akan mengikat elemen-elemen di Y. Jadi $|C| = |y|^{|X|} = 4^4 = 256$, hal ini menunjukkan bahwa seluruh senyawa kimia yang mungkin terjadi dari tetrahedron dengan lengan atom C yang keempat lengannya dapat mengikat H, CH_3, Cl atau C_2H_5 sebanyak 256. Dari sebanyak 256 senyawa yang mungkin terjadi, banyaknya senyawa yang berbeda dapat dihitung dengan Teorema Polya I. Sebelumnya ditentukan dulu indeks sikel polinomial dari S_4 sebagaimana telah dibahas dalam Contoh 5.4.3 adalah

$$\begin{aligned} Z(S_4; x_1, x_2, x_3, x_4) &= \frac{1}{|S_4|} \sum_{g \in S_4} z(g) \\ &= \frac{1}{24}(x_1^4 + 8x_1x_3 + 6x_1^2x_2 + 3x_2^2 + 6x_4). \end{aligned}$$

Diketahui $|Y| = r = 4$, maka $x_1 = x_2 = x_3 = x_4 = r = 4$ sehingga didapat

$$\begin{aligned} Z(Z_4; r, r, r, r) &= \frac{1}{24}(r^4 + 8r^2 + 6r^3 + 3r^2 + 6r) \\ &= \frac{1}{24}(r^4 + 6r^3 + 11r^2 + 6r) \\ &= \frac{1}{24}(4^4 + 6\,(4^3) + 11\,(4^2) + 6(4)) \\ &= \frac{1}{24}(256 + 384 + 176 + 24) \\ &= \frac{840}{24} \\ &= 35. \end{aligned}$$

Terlihat ada 35 pola molekul yang berbeda dari pengikatan atom karbon C yang membentuk tetrahedron dimana tiap lengannya dapat mengikat salah satu dari H, CH_3, Cl atau C_2H_5. Hasil ini sama seperti dalam pembahasan Contoh 5.3.7.

5.9.2 Teorema Polya II (Redfield-Polya Theorem)

Teorema Polya II berbeda dengan Teorema Polya I yang hanya untuk menghitung banyaknya pola yang berbeda dari suatu konfigurasi. Tetapi Teorema Polya II dapat menentukan bentuk pola yang berbeda dari konfigurasi tersebut. Sehingga Teorema Polya II sekaligus dapat menentukan bentuk pola yang berbeda dan banyaknya dari suatu konfigurasi [15].

Teorema 5.9.2

Misalkan $C = \{f \mid f : X \to Y\}$ sebagaimana dalam Teorema Polya I 5.9.1. Bila disubstitusikan

$$x_i = \sum_{j=1}^{r} y_j^i, \quad i = 1, 2, \ldots, n$$

pada $Z(G; x_1, x_2, \ldots, x_n)$, maka dengan menguraikan indeks sikel polinomial tersebut akan didapat jumlahan dalam bentuk

$$n_{i_1 i_2 \cdots i_r} y_1^{i_1} y_2^{i_2} \cdots y_r^{i_r},$$

dengan $i_1 + i_2 + \cdots + i_r = n$. Yang berarti terdapat tepat $n_{i_1 i_2 \cdots i_r}$ pola $y_1^{i_1} y_2^{i_2} \cdots y_r^{i_r}$ di C, dengan $|C| = r^n$ dibawah G, dimana pola $y_1^{i_1} y_2^{i_2} \cdots y_r^{i_r}$ memuat y_j sebanyak i_j, $j = 1, 2, \ldots, r$. Dengan kata lain fungsi pembangun pola di C adalah

$$F(y_1, y_2, \ldots, y_r) = Z(G; [y_1, y_2, \ldots, y_r]),$$

dengan $[y_1, y_2, \ldots, y_r] = (y_1 + y_2 + \ldots + y_r, y_1^2 + y_2^2 + \ldots + y_r^2, \ldots, y_1^r + y_2^r + \ldots + y_r^r)$.

Bukti

Fungsi pembangun konfigurasi dengan 2 peubah diberikan oleh

$$F(a, w) = \sum a_{mn} b^m w^n,$$

dengan a_{mn} adalah banyaknya pola dari m pola b dan n pola w. Bila $|Y| = r > 2$ dengan $Y = \{y_1, y_2, \ldots, y_r\}$, maka didapat fungsi pembangun

$$F(y_1, y_2, \ldots, y_2) = \sum n_{i_1 i_2 \cdots i_r} y_1^{i_1} y_2^{i_2} \cdots y_r^{i_r},$$

dengan $i_1 + i_2 + \cdots + i_r = r$. Untuk setiap $f \in C$ didefinisikan

$$c(f) = y_1^{i_1} y_2^{i_2} \cdots y_r^{i_r},$$

yang menyatakan bahwa f adalah pola yang memuat y_j sebanyak i_j, $j = 1, 2, \ldots, r$. Bila $h, f \in C$ dalam satu orbit, maka $c(h) = c(f)$. Oleh karena itu, untuk $F \in C/G$, dengan C/G adalah himpunan semua orbit-orbit yang berbeda yang ada di C dibawah G, dapat dituliskan $c(F)$ untuk menyatakan pola dari elemen-elemen yang berada di F. Selanjutnya akan dibuktikan menggunakan cara yang sama seperti pembuktian Teorema Burnside (Teorema 5.3.1). Sehingga didapat

$$\sum_{f \in C} \sum_{g \in G} [gf = f] c(f) = \sum_{g \in G} \sum_{f \in C} [gf = f] c(f). \tag{5.6}$$

Dari bagian sebelah kiri Persamaan 5.6 didapat

$$\sum_{f \in C} \sum_{g \in G} [gf = f] c(f) = \sum_{f \in C} c(f) \sum_{g \in G} [gf = f] = \sum_{f \in C} c(f) |G_f|.$$

Selanjutnya akan dijumlahkan atas orbit yang berbeda, karena $|c(f)|$ dan $|G_f|$ hanya bergantung pada orbit, didapat

$$\sum_{f \in C} c(f)|G_f| = c(f_{1_1}) \left|G_{f_{1_1}}\right| + c(f_{1_2}) \left|G_{f_{1_2}}\right| + \cdots + c(f_{2_1}) \left|G_{f_{2_1}}\right| + c(f_{2_2}) \left|G_{f_{2_2}}\right| + \cdots \tag{5.7}$$

Karena $f_{i_1}, f_{i_2}, \ldots$ terletak dalam satu orbit yang sama, maka $c(f_{i_j}) = c(F_i)$. Sehingga Persamaan 5.7 dapat ditulis sebagai

$$\begin{aligned} c(F_1)\left\{\left|G_{f_{1_1}}\right| + \left|G_{f_{1_2}}\right| + \cdots\right\} \;+\; & c(F_2)\left\{\left|G_{f_{2_1}}\right| + \left|G_{f_{2_2}}\right| + \cdots\right\} + \cdots \\ &= \sum_{F \in C/G} c(F) \sum_{f \in F} |G_f| \\ &= \sum_{F \in C/G} c(F)|G| \\ &= |G| \sum_{F \in C/G} c(F). \end{aligned}$$

Karena $c(F) = y_1^{i_1} y_2^{i_2} \cdots y_r^{i_r}$, maka $\sum_{F \in C/G} c(F)$ merupakan fungsi pembangun konfigurasi di C, adapun koefisien $y_1^{i_1} y_2^{i_2} \cdots y_r^{i_r}$ akan sama deengan banyaknya orbit yang di $c(F) = y_1^{i_1} y_2^{i_2} \cdots y_r^{i_r}$. Sehingga didapat

$$|G| \sum_{F \in C/G} c(F) = |G| F(y_1, y_2, \ldots, y_r). \tag{5.8}$$

Sedangkan berdasarkan ungkapan sebelah kiri Persamaan 5.6 didapat

$$\sum_{g\in G}\sum_{f\in C}[gf = f]c(f) = \sum_{g\in G}\sum_{f\in \text{Fix}(g)} c(f).$$

Karena $|\text{Fix}(g)| = \sum_{f\in\text{Fix}(g)} 1$ dapat dihitung melalui sikel-sikel yang saling asing di g, yaitu

$$|\text{Fix}(g)| = r^{a_1+a_2+\cdots+a_n} = z(r, r, \ldots, r),$$

dengan $[a_1, a_2, \ldots, a_n]$ adalah tipe permutasi dari g. Maka $\sum_{f\in\text{Fix}(g)} c(f)$ juga dapat dituliskan sebagai indeks sikel polinomial. Misal, $g \in G$ dengan $g = (1\ 3\ 5)(2\ 4\ 6)$, maka $|\text{Fix}(g)| = r^{a_1+a_2+\cdots+a_n} = z(r, r, \ldots, r) = r^2$. Untuk $f \in \text{Fix}(g)$, titik $1, 3$ dan 5 berada dalam satu orbit sehingga punya pola yang sama. Jadi terdapat faktor y_i^3 di $c(f)$. Begitu juga untuk titik $2, 4$ dan 6 terdapat faktor y_i^3 di $c(f)$. Jadi jumlahan atas r^2 adalah

$$(y_1^3 + y_2^3 + \cdots + y_r^3)(y_1^3 + y_2^3 + \cdots + y_r^3).$$

Hal berarti bahwa

$$\sum_{f\in\text{Fix}(g)} = (y_1^3 + y_2^3 + \cdots + y_r^3)^2.$$

Begitu juga bila $g = (1\ 4)(2\ 5)(3\ 6)$, maka dengan argumentasi yang sama didapat

$$\sum_{f\in\text{Fix}(g)} = (y_1^2 + y_2^2 + \cdots + y_r^2)^3.$$

Dari apa yang dibahas ini, dapat disimpulkan bahwa untuk setiap sikel dengan panjang k didapat faktor $y_1^k + y_2^k + \cdots + y_r^k$ di $\sum_{f\in\text{Fix}(g)} c(f)$. Sehingga didapat

$$\sum_{f\in\text{Fix}(g)} c(f) = z(g; y_1+y_2+\cdots+y_r, y_1^2+y_2^2+\cdots+y_r^2, \ldots, y_1^k+y_2^k+\cdots+y_r^k, \ldots, y_1^n+y_2^n+\cdots+y_r^n). \quad (5.9)$$

Untuk selanjutnya notasi

$$z(g; y_1 + y_2 + \cdots + y_r, y_1^2 + y_2^2 + \cdots + y_r^2, \ldots, y_1^k + y_2^k + \cdots + y_r^k, \ldots, y_1^n + y_2^n + \cdots + y_r^n)$$

ditulis sebagai

$$z(g; [y_1 + y_2 + \cdots + y_r]).$$

Bila Persamaan 5.8 dan 5.9 disubstitusikan ke Persamaan 5.6 didapat

$$\begin{aligned} |G|F(y_1, y_2, \ldots, y_r) &= \sum_{g\in G}\sum_{f\in\text{Fix}(g)} c(f) \\ &= \sum_{g\in G} z(g; [y_1 + y_2 + \cdots + y_r]). \end{aligned}$$

Sehingga didapat

$$\begin{aligned} F(y_1, y_2, \ldots, y_r) &= \frac{1}{|G|}\sum_{g\in G} z(g; [y_1 + y_2 + \cdots + y_r]) \\ &= Z(G; [y_1 + y_2 + \cdots + y_2]). \end{aligned}$$

Jadi bila disubstitusikan $x_1 = y_1 + y_2 + \cdots + y_r, x_2 = y_1^2 + y_2^2 + \cdots + y_r^2$ dan seterusnya akan didapat jenis dari pola-pola di C.

Contoh 5.9.3

Dibahas ulang Contoh 5.3.4, menentukan ada berapa banyak senyawa organik yang terjadi dari suatu proses kimia yang mungkin. Dari satu rantai karbon terdiri dari enam atom karbon C dikaitkan dengan satu atom hidrogen H dan satu molekul CH_3 dalam pembahasannya menggunakan Teorema Polya I. Disini dibahas dengan menggunakan Teorema Polya II. Sebagaimana telah dibahas dalam Contoh 5.3.4 grup $G \leq S_n$ adalah $G = D_6$, $X = \{1,2,3,4,5,6\}$ dan $Y = \{H, CH_3\}$. Jadi $|X| = 6$ dan $|Y| = r = 2$. Misalkan $H = a$ dan $CH_3 = b$. Maka dengan mensubstitusikan

$$x_1 = a + b, x_2 = a^2 + b^2, x_3 = a^3 + b^3, x_4 = a^4 + b^4, x_5 = a^5 + b^5, x_6 = a^6 + b^6$$

$Z(D_6, x_1, x_2, x_3, x_4, x_5, x_6)$

$$\begin{aligned}
Z(D_6, x_1, x_2, x_3, x_4, x_5, x_6) &= \frac{1}{12}\sum_{g\in D_6} z(g; x_1, x_2, x_3, \ldots, x_n) \\
&= \frac{1}{12}\left(\sum_{d|6} \varphi(d) x_d^{\frac{6}{d}} + \frac{6}{2}x_2^{\frac{6}{2}} + \frac{6}{2}x_1^2 x_2^{\frac{6-2}{2}}\right) \\
&= \frac{1}{12}\left(\phi(1)x_1^6 + \phi(2)x_2^3 + \phi(3)x_3^2 + \phi(6)x_6 + 3x_2^3 + 3x_1^2x_2^2\right) \\
&= \frac{1}{12}\left(x_1^6 + x_2^3 + 2x_3^2 + 2x_6 + 3x_2^3 + 3x_1^2x_2^2\right) \\
&= \frac{1}{12}\left(x_1^6 + 4x_2^3 + 2x_3^2 + 3x_1^2x_2^2 + 2x_6\right).
\end{aligned}$$

Didapat

$$\begin{aligned}
Z(D_6, x_1, x_2, x_3, x_4, x_5, x_6) &= \frac{1}{12}\left(x_1^6 + 4x_2^3 + 2x_3^2 + 3x_1^2x_2^2 + 2x_6\right) \\
&= \frac{1}{12}\Big((a+b)^6 + 4(a^2+b^2)^3 + 2(a^3+b^3)^2 + 3(a+b)^2(a^2+b^2)^2 \\
&\qquad + 2(a^6+b^6)\Big) \\
&= \frac{1}{12}\left(12\,a^6 + 12\,a^5b + 36\,a^4b^2 + 36\,a^3b^3 + 36\,a^2b^4 + 12\,ab^5 + 12\,b^6\right) \\
&= a^6 + a^5b + 3\,a^4b^2 + 3\,a^3b^3 + 3\,a^2b^4 + ab^5 + b^6.
\end{aligned}$$

Dari persamaan yang telah didapat ada sebanyak 13 jumlahan konfigurasi. Nilai 13 ini menyatakan bahwa ada sebanyak 13 pola molekul yang berbeda mengikat atom C. Hal ini menunjukkan hasil yang sama seperti pembahasan Contoh 5.3.4. Sedangkan bentuk pola-pola yang berbeda adalah:

(1) Pola a^6 menyatakan bahwa rantai carbon C diikat oleh H sebanyak 6. Banyaknya pola ikatan ini adalah 1.

(2) Pola a^5b menyatakan bahwa rantai carbon C diikat oleh H sebanyak 5 dan CH_3. Banyaknya pola ikatan ini adalah 1.

(3) Pola $3\,a^4b^2$ menyatakan bahwa rantai carbon C diikat oleh H sebanyak 4 dan CH_3 sebanyak 2. Banyaknya pola ikatan ini adalah 3.

(4) Pola $3a^3b^3$ menyatakan bahwa rantai carbon C diikat oleh H sebanyak 3 dan CH_3 sebanyak 3. Banyaknya pola ikatan ini adalah 3.

(5) Pola $3a^2b^4$ menyatakan bahwa rantai carbon C diikat oleh H sebanyak 2 dan CH_3 sebanyak 4. Banyaknya pola ikatan ini adalah 3.

(6) Pola ab^5 menyatakan bahwa rantai carbon C diikat oleh H dan CH_3 sebanyak 5. Banyaknya pola ikatan ini adalah 1.

(7) Pola b^6 menyatakan bahwa rantai carbon C diikat oleh CH_3 sebanyak 6. Banyaknya pola ikatan ini adalah 1. ●

Contoh 5.9.4

Pada Contoh 5.9.1 digunakan Teorema Polya I. Selanjutnya dengan contoh yang sama ini digunakan Teorema Polya II untuk menentukan bentuk/jenis pola-pola sebagai berikut. Misalkan $H = a, CH_3 = b, Cl = c$ dan $C_2H_5 = d$ [15]. Maka dengan mensubstitusikan

$$x_1 = a + b + c + d, x_2 = a^2 + b^2 + c^2 + d^2, x_3 = a^3 + b^3 + c^3 + d^3, x_4 = a^4 + b^4 + c^4 + d^4$$

pada $Z(S_4; x_1, x_2, x_3, x_4)$ didapat persamaan

$$\begin{aligned} Z(S_4; x_1, x_2, x_3, x_4) &= \frac{1}{24}(x_1^4 + 8x_1x_3 + 6x_1^2x_2 + 3x2^2 + 6x_4) \\ &= \frac{1}{24}\Big((a+b+c+d)^4 + 8(a+b+c+d)(a^3+b^3+c^3+d^3) \\ &\qquad + 6(a+b+c+d)^2(a^2+b^2+c^2+d^2) + 3(a^2+b^2+c^2+d^2)^2 \\ &\qquad + 6(a^4+b^4+c^4+d^4)\Big) \\ &= a^4 + b^4 + c^4 + d^4 + a^3b + a^3c + a^3d + ab^3 + b^3c + b^3d + ac^3 + bc^3 + c^3d \\ &\quad + ad^3 + bd^3 + cd^3 + a^2b^2 + a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 + c^2d^2 + a^2bc \\ &\quad + a^2bd + a^2cd + ab^2c + ab^2d + b^2cd + abc^2 + ac^2d + bc^2d + abd^2 \\ &\quad + acd^2 + bcd^2 + abcd. \end{aligned}$$

Dari persamaan yang telah didapat ada sebanyak 35 jumlahan konfigurasi. Nilai 35 ini menyatakan bahwa ada sebanyak 35 pola molekul yang berbeda mengikat atom C. Hal ini menunjukkan hasil yang sama seperti pembahasan Contoh 5.9.1. Sedangkan bentuk pola-pola yang berbeda adalah:

1. a^4 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H sebanyak 4.
2. b^4 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 sebanyak 4.
3. c^4 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh Cl sebanyak 4.
4. d^4 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh C_2H_5 sebanyak 4.
5. a^3b menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H sebanyak 3 dan CH_3.
6. a^3c menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 sebanyak 3 dan Cl.

7. a^3d menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 sebanyak 3 dan CH_5.
8. ab^3 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H dan CH_3 sebanyak 3.
9. b^3c menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 sebanyak 3 dan Cl.
10. b^3d menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 sebanyak 3 dan C_2H_5.
11. ac^3 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H dan Cl sebanyak 3.
12. bc^3 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 dan Cl sebanyak 3.
13. c^3d menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh Cl sebanyak 3 dan C_2H_5.
14. ad^3 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H dan C_2H_5 sebanyak 3.
15. bd^3 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 dan C_2H_5 sebanyak 3.
16. cd^3 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh Cl dan C_2H_5 sebanyak 3.
17. a^2b^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H sebanyak 2 dan CH_3 sebanyak 2.
18. a^2c^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H sebanyak 2 dan Cl sebanyak 2.
19. a^2d^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H sebanyak 2 dan C_2H_5 sebanyak 2.
20. b^2c^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 sebanyak 2 dan Cl sebanyak 2.
21. b^2d^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 sebanyak 2 dan C_2H_5 sebanyak 2.
22. c^2d^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh Cl sebanyak 2 dan C_2H_5 sebanyak 2.
23. a^2bc menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H sebanyak 2, CH_3 dan Cl.
24. a^2bd menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H sebanyak 2, CH_3 dan C_2H_5.

25. a^2cd menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H sebanyak 2, Cl dan C_2H_5.

26. ab^2c menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H, CH_3 sebanyak 2 dan Cl.

27. ab^2d menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H, CH_3 sebanyak 2 dan C_2H_5.

28. b^2cd menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3 sebanyak 2, Cl dan C_2H_5.

29. abc^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H, CH_3 dan Cl sebanyak 2.

30. ac^2d menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H, Cl sebanyak 2 dan C_2H_5.

31. bc^2d menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3, Cl sebanyak 2 dan C_2H_5.

32. abd^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H, CH_3 dan C_2H_5 sebanyak 2.

33. acd^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H, Cl dan C_2H_5 sebanyak 2.

34. bcd^2 menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh CH_3, Cl dan C_2H_5 sebanyak 2.

35. $abcd$ menyatakan bahwa tetra hedron dengan pusat atom C diikat oleh H, CH_3, Cl dan C_2H_5. ●

5.10 Klas Konjugasi dan Persamaan Klas

Dalam bagian ini dibahas satu tindakan grup khusus yaitu tindakan grup G pada dirinya sendiri melalui konjugasi atau dengan kata lain tindakan $G \times G \to G$ melalui $(g, a) = gag^{-1}$. Dalam bagian sebelumnya telah dibahas formula **counting** Burnside yang berkaitan dengan orbit dalam suatu himpunan berhingga X yang dikenakan tindakan oleh grup berhingga G dan digunakan formula ini pada berbagai masalah. Dalam bagian ini dibahas formula **counting** lain yang penting berkenaan dengan orbit dalam tindakan suatu grup pada dirinya sendiri. Formula ini sangat penting dalam memahami struktur dari suatu grup berhingga dan digunakan formula ini untuk mengkaji grup dengan order pangkat dari suatu bilangan prima p.

Konjugasi

Contoh 5.10.1 Diberikan grup $G = S_3 = \{\rho_0, \rho, \rho^2, \mu_1, \mu_2, \mu_3\}$ bertindak pada dirinya sendiri melalui konjugasi yaitu tindakan $G \times G \to G$ didefinisikan oleh $(g, a) \to gag^{-1}$ (lihat Con-

toh 5.1.5). Melalui tindakan ini, orbit tindakan adalah

$$\begin{aligned} O_{\rho_0} &= \{\rho_0\} \\ O_{\rho} &= O_{\rho^2} = \{\rho, \rho^2\} \\ O_{\mu_1} &= O_{\mu_2} = O_{\mu_3} = \{\mu_1, \mu_2, \mu_3\}. \end{aligned}$$

Stabiliser terkait adalah

$$G_{\rho_0} = G, \quad G_{\rho} = G_{\rho^2} = \{\rho_0, \rho, \rho^2\} \quad \text{dan} \quad G_{\mu_i} = \{\rho_0, \mu_i\}, \text{ untuk } i = 1, 2, 3.$$

Perlu diperhatikan bahwa

(1) $|G| = 6 = \left|O_{\rho_0}\right| + \left|O_{\rho}\right| + \left|O_{\mu_1}\right|$.

(2) $|G| = 6 = |O_a|\,|G_a|$ untuk semua $a \in G$.

Hasil yang diperoleh bukan suatu kejutan sebab sudah dibuktikan dalam Proposisi 5.2.2 dan Teorema 5.2.1.

Berikut ini didefinisikan istilah yang digunakan.

Definisi 5.10.1 Bila G adalah suatu grup dan $a, b \in G$, maka a dan b **berkonjuget** dalam G bila ada suatu $g \in G$ yang memenuhi $b = gag^{-1}$ atau dengan kata lain bila a dan b adalah dalam orbit yang sama oleh tindakan G pada dirinya sendiri melalui konjugasi. **Klas konjugasi** dari suatu $a \in G$ yaitu $K_G(a) = \{gag^{-1} \mid g \in G\}$ adalah himpunan semua konjuget dari a atau dengan kata lain orbit dari a dalam tindakan tersebut. Ingat bahwa, sentralisir dari $a \in G$

$$C_G(a) = \{g \in G \mid ga = ag\} = \left\{g \in G \mid gag^{-1}a\right\}$$

adalah himpunan dari semua elemen yang komutatif dengan a atau secara ekivalen stabiliser dari a dalam tindakan tersebut. Bila konteks grup G jelas yang dimaksud, maka indeks dihapus dan hanya ditulis $K(a)$ dan $C(a)$.

Proposisi 5.10.1 Misalkan G adalah suatu grup bertindak pada dirinya sendiri melalui konjugasi dan $a \in G$. Maka banyaknya klas konjugasi dari a sama dengan indeks dari sentralisir dari a yaitu $|K(a)| = [G : C(a)]$. Bila G berhingga maka $|K(a)| = |G|/|C(a)|$.

Bukti Pernyataan dalam proposisi adalah berkaitan dengan Teorema 5.2.1 yang istilih-istilahnya diberikan dalam definisi sebelumnya.

Berikut ini diberikan teorema utama dalam bagian ini.

Teorema 5.10.1 (**Persamaan Klas**) Diberikan grup berhingga G, $Z(G)$ adalah senter dari G dan misalkan $a_1, a_2, \ldots, a_r$ adalah elemen-elemen tidakdi $Z(G)$ membentuk suatu himpunan dari representasidari klas konjugasi yang tak-termuat di $Z(G)$. Hal berarti bahwa tidak ada dua dari a_i berkonjuget satu dengan yang lainnya, tetapi setiap elemen tidak di senter dari satu diantara keduanya. Maka

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C(a_i)]\,.$$

Bukti Bila $b_1, b_2, \ldots, b_s$ adalah elemen-elemen di $Z(G)$, karena masing-masing b_j berkonjuget dengan dirinya sendiri, maka b_j dan a_i bersama-sama adalah suatu himpunan lengkap dari representasi semua klas konjugasi. Berdasarkan Teorema 5.2.2 didapat

$$|G| = \sum_{i=1}^{s} [G : C(b_i)] + \sum_{i=1}^{r} [G : C(a_i)] ,$$

dimana untuk menyesuaikan dengan Proposisi 5.10.1 $\left[G : G_g\right]$ diganti dengan $[G : C(g)]$. Tetapi untuk masing-masing b_i dalam senter, $C(b_i)$ adalah G sendiri. Jadi $[G : C(b_i)] = 1$, dengan didapat persamaan klas

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C(a_i)] .$$

Contoh 5.10.2 Diberikan grup dihedral D_4. Untuk menentukan klas konjugasi dilakukan hal berikut:

$$\begin{aligned} \tau\rho\tau^{-1} &= (\tau\rho)\tau = (\rho^3\tau)\tau = \rho^3\tau^2 = \rho^3 \\ \rho\tau\rho^{-1} &= \rho(\tau\rho^3) = \rho(\rho\tau) = \rho^2\tau \\ \rho(\rho\tau)\rho^{-1} &= \rho(\rho\tau)\rho^3 = \rho^2(\tau\rho^3) = \rho^2(\rho\tau) = \rho^3\tau. \end{aligned}$$

Dari fakta penghitungan yang dilakukan didapat Tabel 5.10.

Tabel 5.10: Klas Konjugasi dalam D_4

Sentralisir	Klas Konjugasi	Indeks
$Z(D_4) = \{\rho_0, \rho^2\}$	$K(e) = \{e\}, K(\rho^2) = \{\rho^2\}$	
$C(\rho) = C(\rho^3) = \{\rho_0, \rho, \rho^2, \rho^3\}$	$K(\rho) = \{\rho, \rho^3\}$	$[G : C(\rho)] = 2$
$C(\tau) = C(\rho^2\tau) = \{\rho_0, \tau, \rho^2, \rho^2\tau\}$	$K(\tau) = \{\tau, \rho^2\tau\}$	$[G : C(\tau)] = 2$
$C(\rho\tau) = C(\rho^3\tau) = \{\rho_0, \rho\tau, \rho^2, \rho^3\tau\}$	$K(\rho\tau) = \{\rho\tau, \rho^3\tau\}$	$[G : C(\rho\tau)] = 2$

Dalam hal ini persamaan klas adalah $8 = 2 + 2 + 2 + 2$.

Contoh 5.10.3 Diberikan grup kuoternion $Q_8 = \{\pm 1, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\}$. Sebarang elemen dari sebarang grup komutatif dengan elemen pangkat-pangkatnya, jadi sentralisir $C(\boldsymbol{i})$ memuat $\boldsymbol{i}, \boldsymbol{i}^2 = -1, \boldsymbol{i}^3 = -\boldsymbol{i}$ dan $\boldsymbol{i}^4 = 1$. Karena $C(\boldsymbol{i})$ adalah suatu subgrup dari Q_8, maka $|C(\boldsymbol{i})|$ membagi $|Q_8|$. Karena $\boldsymbol{ij} = \boldsymbol{k} \neq -\boldsymbol{k} = \boldsymbol{ji}$, maka $C(\boldsymbol{i}) = \{1, \boldsymbol{i}, -1, -\boldsymbol{i}\}$. Jadi indeks $[Q_8 : C(\boldsymbol{i})] = 2$. Elemen dari klas konjugasi adalah $\boldsymbol{i}$ sendiri dan $\boldsymbol{jij}^{-1} = -\boldsymbol{i}$. Mengikuti alur yang sama untuk $\boldsymbol{j}$ dan $\boldsymbol{k}$ didapat klas konjugasi $\{\pm \boldsymbol{j}\}$ dan $\{\pm \boldsymbol{k}\}$ dengan demikian $Z(Q_8) = \{\pm 1\}$. Jadi persamaan klasnya adalah $8 = 2 + 2 + 2 + 2$.

Berikut ini diberikan akibat penting dari persamaan klas.

Teorema 5.10.2 Bila G adalah suatu grup berorder p^n, dimana p adalah prima dan $n \geq 1$, maka senter dari G adalah tak-trivial, yaitu $|Z(G)| > 1$ dan $|Z(G)| = p^k$ untuk beberapa k dimana $1 \leq k \leq n$.

Bukti Persamaan klas adalah

$$|G| = |Z(G) + \sum_{i=1}^{r} [G : C(a_i)],$$

dimana $a_1, a_2, \ldots, a_r$ adalah merepresentasikan secara lengkap himpunan klas konjugasi yang tidak termuat dalam $Z(G)$. Karena $C(a_i) \neq G$, maka indeks $[G : C(a_i)] \neq 1$, jadi p membagi $[G : C(a_i)]$. Juga, karena p membagi $|G|$, maka p membagi $|Z(G)|$. Dengan demikian $|Z(G)| \neq 1$. Selanjunya, karena senter dari G, yaitu $Z(G)$ adalah suatu subgrup dari G, maka $|Z(G)|$ membagi $|G| = p^n$. Dengan demikian $|Z(G)| = p^k$ untuk beberapa k dimana $1 \leq k \leq n$. ✓

Akibat 5.10.1 Bila G adalah suatu grup berorder p^2 dimana p adalah prima maka G adalah grup komutatif dan G isomorpik dengan $\mathbb{Z}_{p^2}$ atau isomorpik dengan $\mathbb{Z}_p \times \mathbb{Z}_p$.

Bukti Andaikan bahwa G bukan grup komutatif, maka $Z(G) \neq G$. Gunakan Teorema 5.10.2, maka $|Z(G)| > 1$. Tetapi $Z(G) < G$ dengan menggunakan teorema Lagrange haruslah $|Z(G)| = p$. Selanjutnya, misalkan $a \in$ tetapi $a \notin Z(G)$. Maka $a \in C(a)$ dan $Z(G) < C(a)$. Lagi dengan menggunakan teorema Langrange didapat $|C(a)| = p^2 = |G|$. Akibatnya $a \in Z(G)$, tetapi hal ini bertentangan dengan kenyataan $a \notin Z(G)$. Jadi haruslah G adalah grup komutatif. Selanjutnya bila G siklik, maka $G \cong \mathbb{Z}_{p^2}$ dan bila G tidak siklik, maka $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. ✓

Pengertian dari konjugasi juga dapat didefinisikan untuk subgrup dan elemen dari suatu grup. Geeneralisasi ini berguna pada pembahasan berikutnya. Faktanya, pengertian yang dibahas ini dapat didefinisikan untuk sebarang himpunan bagian dari suatu grup yang tidak perlu merupakan subgrup.

Definisi 5.10.2 Misalkan G adalah suatu grup dan X adalah himpunan semua subgrup dari G. Tinjau pemetaan $G \times X \to X$ yang memetakan (g, A) menjadi himpunan $gAg^{-1} = \{gag^{-1} \mid a \in A\}$. pemetaan ini adalah suatu tindakan dinamakan **konjugasi**. Dua subgrup $A, B \subseteq G$ dikatakan **berkonjuget** dalam G bila ada suatu $g \in G$ yang memenuhi $B = gAg^{-1}$ atau dengan kata lain bila A dan B adalah dalam orbit yang sama oleh tindakan dari G pada himpunan dari subgrup-subgrupnya melalui konjugasi. Klas konjugasi dari A di G adalah himpunan semua konjuget dari A yaitu

$$K_G(A) = \{gAg^{-1} \mid g \in G\}$$

atau dengan kata lain adalah orbit dari A dalam tindakan tersebut. Ingat bahwa **sentralisir** dari himpunan A di G adalah himpunan dari semua elemen yang komutatif dengan semua elemen A, yaitu

$$C_G(A) = \{g \in G \mid ga = ag \text{ untuk semua } a \in A\} = \{g \in G \mid gag^{-1} \text{ untuk semua } a \in A\}.$$

Normalisir adalah himpunan

$$N_G(A) = \{g \in G \mid gA = Ag\} = \{g \in G \mid gAg^{-1} = A\}$$

merupakan stabiliser dari A dalam tindakan tersebut. Bila konteks yang dimaksud dengan grup G adalah sudah jelas, penulisan indeks G dihapus dan cukup ditulis $K(A), C(A)$ dan $N(A)$. ✓

Proposisi 5.10.2 Misalkan grup G bertindak pada himpunan semua subgrup dari G melalui konjugasi dan $A < G$. Maka banyaknya klas konjugasi dari A sama dengan indeks dari normalisir A, yaitu $|K(A)| = [G : N(A)]$. Bila $|G|$ berhingga, maka $|K(A)| = |G|/|N(A)|$.

Bukti Apa yang dinyatakan dalam proposisi ini adalah pernyataan dalam Teorema 5.2.1 dalam terminilogi Definisi 5.10.2. ∎

Latihan

Latihan 5.10.1 Uraikan klas konjugasi dan tuliskan persamaan klas dari suatu grup komutatif. ∎

Latihan 5.10.2 Diberikan dua grup G_1 dan G_2. Tunjukkan bahwa dalam $G_1 \times G_2$ elemen (a, b) dan (c, d) berkonjuget bila dan hanya bila a dan c berkonjuget di G_1, b dan d berkonjuget di G_2. ∎

Latihan 5.10.3 Uraikan klas konjugasi dan tulis persamaan klas dari grup berikut:

1. $\mathbb{Z}_2 \times S_3$
2. $\mathbb{Z}_2 \times D_4$
3. $\mathbb{Z}_3 \times S_3$
4. $S_3 \times S_3$
5. A_4
6. $\mathbb{Z}_3 \times A_4$. ∎

Latihan 5.10.4 Diberikan sebarang grup G. Tunjukkan bahwa untuk sebarang $a, b \in G$, bila a dan b berkonjuget, maka a dan b mempunyai order yang sama. ∎

Latihan 5.10.5 Diberikan grup G dan $P(G)$ adalah himpunan semua subgrup dari G. Didefinisikan suatu pemetaan $\phi : G \times P(G) \to P(G)$ oleh $\phi(g, A) = gAg^{-1}$, dimana $gAg^{-1} = \{gag^{-1} \mid a \in A\}$.
(a). Tunjukkan bahwa ϕ adalah suatu tindakan grup.
(b). Tunjukkan bahwa sentralisir

$$C(A) = \{g \in G \mid gag^{-1} = a \text{ untuk semua } a \in A\}$$

adalah suatu subgrup dari G.
(c). Tunjukkan bahwa normalisir

$$N(A) = \{g \in G \mid gAg^{-1} = A\}$$

adalah subgrup dari G. ∎

Latihan 5.10.6 Misalkan grup G bertindak pada himpunan dari semua subgrup G melalui konjugasi. Tunjukkan bahwa untuk sebarang $S \subset G$ dan $g \in G$ didapat $gN(S)g^{-1} = N(gSg^{-1})$. ∎

Latihan 5.10.7 Misalkan grup G bertindak pada himpunan dari semua subgrup G melalui konjugasi. Tunjukkan bahwa untuk sebarang $S \subset G$ dan $g \in G$ didapat $gC(S)g^{-1} = C(gSg^{-1})$. ∎

Latihan 5.10.8 Misalkan grup G bertindak pada dirinya sendiri melalui konjugasi. Tunjukkan bahwa bila a dan b berkonjuget dalam G, maka $|C(a)| = |C(b)|$. ∎

Latihan 5.10.9 Misalkan grup G bertindak pada dirinya sendiri melalui konjugasi. Tunjukkan bahwa bila a dan b berkonjuget dalam G, maka $C(a) = C(b)$ bila dan hanya bila masing-masing $C(a)$ dan $C(b)$ adalah subgrup normal dari G.

Latihan 5.10.10 Terangkan mengapa dalam Contoh 5.10.2 dua elemen $a, b \in D_4$ terletak pada orbit yang sama bila dan hanya bila $C(a) = C(b)$.

Latihan 5.10.11 Misalkan indeks dari senter $Z(G)$, $[G : Z(G)] = r$. Tunjukkan bahwa untuk sebarang $g \in G$ banyaknya elemen dari klas konjugasi $K(g)$ adalah lebih kecil atau sama dengan r.

Latihan 5.10.12 Terangkan mengapa untuk sebarang grup berhingga G dan sebarang elemen $g \in G$, maka $|K(g)|$ membagi $|G|$.

Latihan 5.10.13 Terangkan mengapa untuk sebarang elemen $g \in G$, senter $Z(G)$ dari grup G termuat dalam sentralisir $C(g)$ dari elemen g.

Latihan 5.10.14 Terangkan mengapa untuk sebarang elemen $g \in G$, senter $Z(G)$ dari grup G dan sentralisir $C(g)$ dari elemen g adalah sama bila dan hanya bila $g \in Z(g)$.

Latihan 5.10.15 Tunjukkan bahwa untuk sebarang grup tak-komutatif G, indeks dari senter $Z(g)$ yaitu $[G : Z(g)]$ tidak akan sama dengan suatu bilangan prima p.

Latihan 5.10.16 Melalui definisi $a, b \in G$ berkonjuget bila ada suatu elemen $g \in G$ yang memenuhi $b = gag^{-1}$. Berikan suatu contoh untuk menunjukkan bahwa elemen g ini tidak perlu tunggal. Dengan kata lain, ada $h \in G$ dengan $h \neq g$ yang juga memenuhi $b = hah^{-1}$.

Latihan 5.10.17 Dalam situasi Latihan 5.10.16, tunjukkan bahwa banyaknya elemen h yang memenuhi $b = hah^{-1}$ sama dengan $|C(a)|$.

Latihan 5.10.18 Tunjukkan bahwa untuk sebarang elemen $g \in G$ dengan g bukan elemen netral e, maka $|C(g)| \geq 2$.

5.11 Konjugasi dalam S_n dan Simplisitas dari A_5

Pada bagian ini dibahas klas konjugasi dari grup simetri S_n dan digunakan hasil-hasilnya untuk membuktikan bahwa A_5 tidak mempunyai subgrup normal sejati tak-trivial. Dua contoh pertama diberikan untuk mengilustrasikan teorema utama pada bagian ini.

Definisi 5.11.1 Diberikan sebarang $\sigma \in S_n$, σ dapat ditulis sebagai produk dari sikel yang saling asing dimana sikel ditulis dengan urutan dari yang panjangnya pendek keurutan yang lebih panjang. Lagipula, urutan panjang sikel $n_1 \leq n_2 \leq \cdots \leq n_s$ ditentukan secara tunggal dan memenuhi $n = n_1 + n_2 + \cdots + n_s$. Dalam hal ini $n_1, n_2, \ldots, n_s$ dinamakan **tipe sikel** dari σ.

Contoh 5.11.1 Dalam grup simetri S_9, diberikan suatu tipe sikel $2, 3, 4$ yaitu

$$\sigma = (6\ 9)(1\ 4\ 5)(3\ 2\ 7\ 8).$$

Misalkan elemen konjuge $\tau\sigma\tau^{-1}$ dari σ dimana $\tau = (1\ 7\ 2\ 6)(9\ 3\ 5\ 4\ 8)$. Tinjau permutasi ϕ yang mempunyai tipe sikel yang sama dengan tipe sikel dari σ yaitu $2, 3, 4$. Dalam hal ini permutasi ϕ diperoleh dengan mengganti masing-masing i dalam dekomposisi dari sikel σ oleh $\tau(i)$ yaitu

$$\phi = (\tau(6)\ \tau(9))\ (\tau(1)\ \tau(4)\ \tau(5))\ (\tau(3)\ \tau(2)\ \tau(7)\ \tau(8)) = (1\ 3)(7\ 8\ 4)(5\ 6\ 2\ 9).$$

Dengan mudah dapat dilakukan penghitungan berikut

$$\begin{aligned}
\tau\sigma\tau^{-1}(1) &= \tau\sigma(6) = \tau(9) = 3 = \phi(1)\\
\tau\sigma\tau^{-1}(3) &= \tau\sigma(9) = \tau(6) = 1 = \phi(3)\\
\tau\sigma\tau^{-1}(7) &= \tau\sigma(1) = \tau(4) = 8 = \phi(7)\\
\tau\sigma\tau^{-1}(8) &= \tau\sigma(4) = \tau(5) = 4 = \phi(8)\\
\tau\sigma\tau^{-1}(4) &= \tau\sigma(5) = \tau(1) = 7 = \phi(4)\\
\tau\sigma\tau^{-1}(5) &= \tau\sigma(3) = \tau(2) = 6 = \phi(5)\\
\tau\sigma\tau^{-1}(6) &= \tau\sigma(2) = \tau(7) = 2 = \phi(6)\\
\tau\sigma\tau^{-1}(2) &= \tau\sigma(7) = \tau(8) = 9 = \phi(2)\\
\tau\sigma\tau^{-1}(9) &= \tau\sigma(8) = \tau(3) = 5 = \phi(9).
\end{aligned}$$

Terihat bahwa $\tau\sigma\tau^{-1}$ konjuget dari σ mempunyai tipe sikel yang sama dengan tipe sikel dari σ. ●

Contoh 5.11.2 Dalam S_6 diberikan dua sikel dengan tipe sikelyang sama yaitu

$$\sigma = (2)(3\ 6)(4\ 1\ 5) \text{ dan } \rho = (4)(1\ 5)(6\ 3\ 2).$$

Selanjutnya dibuat permutasi τ yang memetakan masing-masing i yang ada dalam dekomposisi σ ke j yang ada dalam dekomposisi dari ρ, yaitu $\tau = (2\ 4\ 6\ 5)(3\ 1)$. Tinjau permutasi $\tau\sigma\tau^{-1}$ konjugasi dari σ, didapat

$$\begin{aligned}
\tau\sigma\tau^{-1}(1) &= \tau\sigma(3) = \tau(6) = 5 = \rho(1)\\
\tau\sigma\tau^{-1}(2) &= \tau\sigma(5) = \tau(4) = 6 = \rho(2)\\
\tau\sigma\tau^{-1}(3) &= \tau\sigma(1) = \tau(5) = 2 = \rho(3)\\
\tau\sigma\tau^{-1}(4) &= \tau\sigma(2) = \tau(2) = 4 = \rho(4)\\
\tau\sigma\tau^{-1}(5) &= \tau\sigma(6) = \tau(3) = 1 = \rho(5)\\
\tau\sigma\tau^{-1}(6) &= \tau\sigma(4) = \tau(1) = 3 = \rho(6).
\end{aligned}$$

Terlihat bahwa tipe sikel dari permutasi σ sama dengan tipe sikel permutasi konjuget dari σ. ●

Teorema 5.11.1 Dua permutasi σ dan ρ dalam S_n berkonjuget bila dan hanya bila σ dan ρ mempunyai tipe sikel yang sama.

Bukti ($\Rightarrow$) Misalkan σ dan ρ berkonjuget, maka pilih τ yang memenuhi $\rho = \tau\sigma\tau^{-1}$. Misalkan tipe sikel dari σ adalah:

$$(x_1 \cdots x_p)(y_1 \cdots y_q)(z_1 \cdots z_r) \cdots$$

Tinjau permutasi ϕ yang mempunyai tipe sikel sama dengan tipe sikel dari σ, yaitu

$$\phi = (\tau(x_1)\cdots\tau(x_p))\,(\tau(y_1)\cdots\tau(y_q))\,(\tau(z_1)\cdots\tau(z_r))\cdots$$

Didapat

$$\rho(\tau(x_i)) = \tau\sigma\tau^{-1}(\tau(x_i) = \tau\sigma(x_i) = \tau(x_{i+1}) = \phi(\tau(x_i)).$$

Dengan cara yang serupa didapat $\rho(\tau(y_j)) = \phi(\tau(y_j))$ dan $\rho(\tau(z_k)) = \phi(\tau(z_k))$. Terlihat bahwa $\rho = \phi$. Jadi ρ mempunyai tipe sikel yang sama dengan tipe sikel dari σ.
($\Leftarrow$) Misalkan diberikan dua permutasi dengan tipe sikel yang sama yaitu:

$$\sigma = (x_1\cdots x_p)(y_1\cdots y_q)(z_1\cdots z_q)\cdots \text{ dan } \rho = (u_1\cdots u_p)(v_1\cdots v_q)(w_1\cdots w_q)\cdots$$

Didefinisikan suatu permutasi τ oleh

$$\tau(x_i) = u_i, \tau(y_j) = v_j, \tau(z_k) = w_k,$$

dan seterusnya. Misalkan $\phi = \tau\sigma\tau^{-1}$ adalah konjuget dari σ. Didapat

$$\phi(u_i) = \tau\sigma\tau^{-1}(u_i) = \tau\sigma(x_i) = \tau(x_{i+1}) = u_{i+1} = \rho(u_i)$$

Dengan cara yang sama didapat $\phi(v_j) = \rho(v_j)$, $\phi(w_k) = \rho(w_k)$ dan seterusnya. Terlihat bahwa $\phi = \rho$. Jadi ρ mempunyai tipe sikel yang sama dengan tipe sikel dari σ.

Definisi 5.11.2 Suatu **partisi** dari suatu bilangan bulat positip n adalah sebarang barisan bilangan positip tak-naik $n_1 \le n_2 \le \cdots \le n_s$ yang memenuhi penjumlahan $n_1+n_2+\cdots+n_s = n$.

Akibat 5.11.1 Banyaknya dari klas konjugasi dalam S_n sama dengan banyaknya partisi dari n.

Bukti Dari pembahasan Teorema 5.11.1, tipe sikel dari sebarang permutasi adalah suatu partisi dan untuk sebarang partisi $n_1 \le n_2 \le \cdots \le n_s$ ada suatu permutasi dengan tipe sikel yang demikian. Misalnya,

$$(1\ \ 2\ \ \cdots\ n_1)(n_1+1\ \ n_1+2\ \cdots\ n_1+n_2)\ \cdots\ (m+1\ \ m+2\ \ \cdots\ n),$$

dimana $m = n_1 + n_2 + \cdots + n_{s-1}$. Dengan demikian $m + n_s = n$ atau $n_1 + n_2 + \cdots + n_{s-1} + n_s = n$.

Bukti dalam Teorema 5.11.1 menunjukkan bahwa diberikan dua permutasi σ dan ρ yang mempunyai tipe sikel yang sama, selanjutnya dikonstruksi permutasi τ yang memenuhi $\rho = \tau\sigma\tau^{-1}$. Contoh berikut mengilustrasikan bahwa τ tidak tunggal.

Contoh 5.11.3 Dalam S_9, diberikan dua permuatsi dengan tipesikel yang sama, yaitu

$$\sigma = (9)(4)(1\ 3)(5\ 8)(2\ 6\ 7)\ \text{ dan }\ \rho = (3)(8)(2\ 5)(9\ 7)(1\ 4\ 6).$$

Dengan menggunakan pengkonstruksian yang sama dilakukan dalam Teorema 5.11.1, didapat $\rho = \tau\sigma\tau^{-1}$ dimana $\tau = (9\ 3\ 5)(4\ 8\ 7\ 6)(1\ 2)$. Tetapi, dengan cara yang sama dapat ditulis dua permutasi dalam urutan yang berbeda, yaitu

$$\sigma = (4)(9)(5\ 8)(1\ 3)(2\ 6\ 7)\ \text{ dan }\ \rho = \text{ sama seperti sebelumnya.}$$

Lagi, menggunakan pengkonstruksian yang sama dilakukan dalam Teorema 5.11.1 didapat $\theta = (4\ 3\ 7\ 6)(9\ 8\ 5\ 2\ 1)$ yang memenuhi $\rho = \theta\sigma\theta^{-1}$.

Tabel 5.11: Klas-klas Konjugasi dalam S_4

Partisi dari 4	Representasi Klas Konjugasi	Banyaknya Konjuget
1, 1, 1, 1	(1)	1
1, 1, 2	(1 2)	6
1, 3	(1 2 3)	8
2, 2	(1 2)(3 4)	3
4	(1 2 3 4)	6

Contoh 5.11.4 Contoh berikut ini adalah menentukan suatu himpunan lengkap yang merupakan representasi dari semua klas konjugasi dari S_n, misalnya untuk $n = 4$. Menurut Teorema 5.11.1 dan Akibat 5.11.1 hanya diperlukan semua partisi yang mungkin dari 4. Hal ini ditampilkan dalam Tabel 5.11 yang juga dihitung banyaknya permutasi dalam masing-masing klas. ●

Contoh berikut mengilustrasikan bagaimana pemahaman tentang klas konjugasi dapat menentukan segi keutamaan yang lain.

Contoh 5.11.5 Misalkan $\sigma = (1\ 2\ 3) \in S_4$. Akan ditentukan sentralisir $C(\sigma)$ dalam S_4. Sentralisisr $C(\sigma)$ harus memuat e, σ, σ^2. Pada satu sisi yang lain, melalui contoh sebelumnya, sebarang sikel $(x\ y\ z)$ adalah berkonjuget dengan $(1\ 2\ 3)$ dalam S_4 dan ada 8 sikel semacam ini. Tetapi dengan menggunakan hubungan stabiliser orbit, didapat bahwa banyaknya elemen dalam klas konjugasi dari σ adalah indeks $[S_4 : C(\sigma)]$. Jadi $|S_4|/|C(\sigma)| = 8$. Karena $|S_4| = 24$, maka $|C(\sigma)| = 3$. Dengan demikian sentralisir $C(\sigma) = \{e, \sigma, \sigma^2\}$. ●

Contoh berikut mengilustrasikan fakta bahwa elemen a dan b berkonjuget dalam suatu grup G dan berada pada suatu subgrup $H \subseteq G$ tidak perlu berkonjuget dalam H.

Contoh 5.11.6 Misalkan $\sigma = (1\ 2\ 3) \in A_4 \subseteq S_4$. Dengan menggunakan Teorema 5.11.1, maka σ berkonjuget dengan $\rho = (1\ 2\ 4)$. Tetapi permutasi τ dapat ditentukan sebagaimana dalam bukti Teorema 5.11.1 adalah $\tau = (3\ 4)$ yang merupakan permutasi ganjil. Jadi $\tau \notin A_4$. Lagipula, tidak ada permutasi yang lain $\chi \in A_4$ yang memenuhi $\rho = \chi\sigma\chi^{-1}$. Bila ada, maka

$$\tau\sigma\tau^{-1} = \chi\sigma\chi^{-1}$$

sehingga didapat

$$\sigma\tau^{-1}\chi = \tau^{-1}\chi\sigma.$$

Jadi $\tau^{-1}\chi \in C(\sigma) \subseteq S_4$. Karena τ adalah permutasi ganjil dan χ adalah permutasi genap, maka permutasi $\tau^{-1}\chi \in C(\sigma)$ adalah permutasi ganjil. Tetapi hal ini tidak mungkin sebab dalam contoh sebelumnya sentralisir $C(\sigma) = \{e, \sigma, \sigma^2\}$ semua elemennya adalah permutasi genap. Jadi σ dan ρ berkonjuget di S_4 tetapi tidak berkonjuget di A_4. ●

Relasi orbit-stabiliser yang digunakan dalam contoh sebelumnya membantu untuk menghitung order sentralisir dari suatu sikel. Hasil berikut ini memberikan cara langsung untuk menentukan sentralisir.

Proposisi 5.11.1

Misalkan $\sigma = (x_1, x_2, \ldots, x_m)$ adalah sikel-m di S_n. Maka

(1) Banyaknya elemen konjuget dari $\sigma \in S_n$ adalah

$$|K(\sigma)| = \frac{n!}{m.(n-m)!}.$$

(2) Banyaknya sentralisir dari $\sigma \in S_n$ adalah

$$|C(\sigma)| = m.(n-m)!.$$

(3) Misalkan subgrup $S_{n-m} < S_n$ dengan m elemen $x_1, x_2, \ldots, x_m$ adalah tetap (fix). Maka

$$C(\sigma) = \{\sigma^i \tau \,|\, 0 \leq i \leq m-1, \tau \in S_{n-m}\}.$$

Bukti
Bagian (1) dan (2) bisa digunakan sebagai latihan. Untuk bagian (3), pertama perhatikan bahwa semua pangkat m σ^i komutatif dengan σ dan berada pada sentralisirnya. Kedua, semua $(n-m)!$ elemen $\tau \in S_{n-m}$ adalah permutasi yang sikel-sikelnya saling asing dengan σ, komutatif dengan σ dengan demikian berada pada sentralisirnya. Lagi pula, hasil kalinya $m.(n-m)!$ semuanya berbeda. Misalkan untuk $\sigma^i\tau_1 = \sigma^j\tau_2$, dengan $0 \leq i, j \leq m$ dan $\tau_1, \tau_2 \in S_{n-m}$. Maka untuk sebarang x_k dengan $1 \leq k \leq m$ didapat $\tau_1(x_k) = \tau_2(x_k) = x_k$, dan dari kenyataan bahwa $\sigma^i\tau_1(x_k) = \sigma^j\tau_2(x_k)$ berakibat $\sigma^i(x_k) = \sigma^j(x_k)$. Karena hal ini berlaku untuk setiap k dengan $1 \leq k \leq m$, maka $\sigma^i = \sigma^j$. Sehingga bersama-sama dengan $\sigma^i\tau_1 = \sigma^j\tau_2$ didapat $\tau_1 = \tau_2$. Dari bagian (2), maka, elemen-elemen sentralisir dari $\sigma^i\tau$ adalah semua elemen yang ada. ∎

Contoh 5.11.7 Ditentukan banyaknya konjuget $\rho = (1\ 2\ 3)$ dalam S_5 dan dalam A_5. Untuk S_5 digunakan Proposisi 5.11.1. Sehingga didapat banyaknya konjuget ρ di S_5 adalah $\frac{5\times4\times3\times2\times1}{3(5-3)!} = 20$, dengan demikian $|C(\sigma)| = 3 \times 2! = 6$, dan

$$C(\sigma) = \left\{e = (), \rho, \rho^2 = (1\ 3\ 2), \theta = (4\ 5), \rho\theta = (1\ 2\ 3)(4\ 5), \rho^2\theta = (1\ 3\ 2)(4\ 5)\right\}.$$

Sentralisir ρ di A_5 terdiri dari permutasi genap yaitu, e, ρ, ρ^2. Oleh karena itu banyaknya sentral adalah 3, dan banyaknya konjuget adalah $|A_5|/3 = 60/3 = 20$. Jadi ρ mempunyai konjuget yang sama di A_5 seperti pada S_5, yaitu semua sikel-3, dengan demikian membentuk satu kelas konjugasi dalam A_5. ●

Contoh 5.11.8 Ditentukan banyaknya konjugasi dari $\sigma = (1\ 2\ 3\ 4\ 5)$ dalam S_5 dan dalam A_5. Untuk S_5 digunakan Proposisi 5.11.1. Sehingga didapat banyaknya konjuget dari σ dalam S_5 adalah $5 \times 4 \times 3 \times 2 \times 1/5 = 24$, dengan demikian $|C(\sigma)| = |S_5|/24 = 120/24 = 5$, dan $C(\sigma) = \{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}$. Karena dalam kasus ini $C(\sigma) \subseteq A_5$, sentralisir pada A_5 adalah sama, dan banyaknya konjuget adalah $|A_5|/5 = 60/5 = 12$, atau setengah banyaknya konjuget dalam S_5. Analisis yang sama berlaku untuk setiap sikel-5 dan menunjukkan bahwa ketika semua sikel-5 membentuk kelas konjugasi tunggal dalam S_5, sikel-sikel ini membentuk dua kelas konjugasi yang berbeda di A_5. ●

Contoh 5.11.9 Ditentukan banyaknya konjuget $\tau = (1\,2)(3\,4)$ dalam S_5 dan A_5. (Perhitungan akan berlaku untuk permutasi dari jenis sikel yang sama.) Dengan teorema utama bagian ini, banyaknya konjugasi τ adalah jumlah permutasi bentuk $(x\ y)(u\ v)$ adalah 15. Oleh karena itu $|C(\tau)| = 120/15 = 8$. Untuk menentukan 8 permutasi yang komutatif dengan τ, pertama-tama perhatikan bahwa jika $\phi = (1\ 3\ 2\ 4)$, maka $\tau = \phi^2$. Jadi τ komutatif dengan semua pangkat ϕ. Selanjutnya jika $\psi = (1\ 2)$, maka $\tau\psi = \psi\tau = (3\ 4)$, jadi τ komutatif dengan ψ. Dari fakta-fakta ini didapat $C(\tau) = \{e, \phi, \phi^2, \phi^3, \psi, \phi\psi, \phi^2\psi, \phi^3\psi\}$. Sentralisir τ dalam A_5 terdiri dari permutasi genap yaitu $\{e, \phi^2, \phi\psi, \phi^3\psi\}$. Oleh karena itu banyaknya sentralisir adalah 4, dan banyaknya konjuget adalah $60/4 = 15$ juga τ memiliki konjuget yang sama dalam A_5 seperti pada S_5, yaitu, semua produk dari dua sikel-2 yang saling asing, dengan demikian membentuk kelas konjugasi tunggal dalam A_5.

Pada pembahasan berikutnya, dikenalkan suatu pengertian dasar dari klasifikasi group berhingga.

Definisi 5.11.3 Suatu grup G dinamakan **sederhana** (***simple***) bila ia tidak mempunyai subgrup normal sejati tak-trivial.

Dari Definisi 5.11.3 dapat langsung terlihat bahwa grup sederhana Abelian tepat sama dengan grup siklik berorder prima. Grup A_n untuk $n \geq 5$ adalah contoh grup sederhana non-Abelian. Hal ini dibuktikan untuk $n \geq 5$. Namum sebelumnya dibuktikan dulu untuk $n = 5$. Tiga contoh yang baru saja dibahas memberikan deskripsi lengkap tentang kelas konjugasi A_5 dan memberikan segala yang dibutuhkan untuk membuktikan A_5 adalah sederhana. Namum sebelumnya dibuktikan lemma berikut.

Lemma 5.11.1 Misalkan G adalah suatu grup dan H adalah suatu subgrup normal berhingga dari G dan misalkan $a_1, a_2, \ldots, a_r$ adalah elemen-elemen di H yang membentuk suatu himpunan lengkap perwakilan dari kelas konjugasi $K_G(b)$ dalam G dari elemen $b \in H$ (berarti bahwa tidak ada dua a_i yang berkonjugasi dalam G satu dengan yang lainnya, tetapi setiap elemen $b \in H$ adalah konjugate dalam G dengan salah satu dari elemen-elemen tsb). Maka

$$|H| = \sum_{i=1}^{r} |K_G(a_i)| .$$

Bukti
Karena tidak ada dua dari a_i berkonjuge dalam G, maka $K_G(a_i)$ adalah saling asing. Karena setiap elemen di H adalah berkonjuget satu dengan yang lainnya, H adalah termuat di gabungan dari $K_G(a_i)$. Lagipula, karena H adalah normal dan $a_i \in H$, maka setiap konjuget $ga_ig^{-1} \in H$. Jadi dengan fakta ini H sama dengan gabungan dari himpunan klas konjugasi $K_G(a_i)$ yang saling asing. Dengan demikian banyaknya elemen H sama dengan jumlah dari banyaknya elemen-elemen dalam klas konjugasi yaitu

$$|H| = \sum_{i=1}^{r} |K_G(a_i)| .$$

Teorema 5.11.2 A_5 adalah grup sederhana.
Bukti
Contoh 5.11.7, 5.11.7 dan 5.11.9 mencakup semua jenis sikel permutasi genap dan bersama-sama menunjukkan bahwa A_5 terdiri dari hanya 5 kelas konjugasi: identitas, dengan 1

elemen; kelas semua sikel-3, dengan 20 elemen; dua kelas sikel-5, masing-masing dengan 12 elemen; dan kelas semua produk dari dua sikel saling asing, dengan 15 elemen. Dengan Lemma 5.11.1, order $|H|$ dari setiap subgrup normal dari A_5 adalah $|H| = 1+12+12+15+20 = 60$. Dalam hal ini, tentu saja, $|H|$ harus membagi $|A_5| = 60$. Untuk subgrup nornal yang sejati non-trivial, $|H|$ pembagi sejati dari 60 yaitu $1 < |H| < |A_5|$. Hal ini menunjukkan tidak mungkin, jadi A_5 tidak memiliki subgrup normal sejati tak-trivial, maka dari itu A_5 adalah grup sederhana.

Sebelum menunjukkan $A_n, n \geq 5$ adalah sederhana, diberikan dua lemma berikut.

Lemma 5.11.2 Sebarang permutasi di $A_n, n \geq 3$ dapat dituliskan sebagai komposisi dari sikel-3.

Bukti
Misalkan sebarang $\sigma \in A_n$. Maka dapat dipilih transposisi $\tau_1, \tau_2, \ldots, \tau_m$ yang memenuhi

$$\sigma = \tau_m \cdots \tau_3 \tau_2 \tau_1,$$

dengan m adalah bilangan bulat genap. Sehingga dapat dipilih bilangan bulat k yang memenuhi $m = 2k$. Dengan demikian dapat dilakukan pengelompokan dua komposi dari τ_i sehingga didapat

$$\sigma = (\tau_{2k}\tau_{2k-1}) \cdots (\tau_4\tau_3)(\tau_2\tau_1).$$

Dalam sebarang pasangan komposisi transposisi $\tau_{2i}\tau_{2i-1}$, bila $\tau_{2i} = \tau_{2i-1}$, maka $\tau_{2i}\tau_{2i-1}$ adalah identitas. Sehingga bisa dihapus dalam σ. Oleh karena itu diasumsikan $\tau_{2i} \neq \tau_{2i-1}$ untuk masing masing-masing komposisi dari transposisi $\tau_{2i}\tau_{2i-1}$. Dengan demikian masing-masing pasangan komposisi dua transposisi mempunyai bentuk $(a\ b)(c\ d)$ dengan $a \neq b, c \neq d$ dan $(a\ b) \neq (c\ d)$ ada dua kasus yang harus dipertimbangkan.

1. Bila semua a, b, c dan d berbeda, maka $(a\ b)(c\ d) = (a\ c\ b)(a\ c\ d)$. Terlihat bahwa komposisi dari transposisi $(a\ b)(c\ d)$ merupakan komposisi dari sikel-3. Dengan demikian sebarang pasangan komposisi transposisi $\tau_{2i}\tau_{2i-1}, i = 1, 2, \ldots k$ merupakan komposisi dari sikel-3. Akibatnya sebarang $\sigma \in A_n$ juga merupakan komposisi dari sikel-3.

2. Bila $b = c$ dan $a \neq d$. Kasus ini ekivalen dengan $a = d$ dan $b \neq c$ atau $a = c$ dan $b \neq d$. Oleh karena itu tampa menghilangkan generalitas diasumsikan bahwa $b = c$ dan $a \neq d$. Maka $(a\ b)(c\ d) = (a\ b)(b\ d) = (a\ b\ d)$. Dalam kasus ini terlihat bahwa komposisi dari transposisi $(a\ b)(c\ d)$ merupakan sikel-3. Dengan demikian sebarang pasangan komposisi transposisi $\tau_{2i}\tau_{2i-1}, i = 1, 2, \ldots k$ merupakan sikel-3. Akibatnya sebarang $\sigma \in A_n$ dengan

   $$\sigma = (\tau_{2k}\tau_{2k-1}) \cdots (\tau_4\tau_3)(\tau_2\tau_1),$$

   merupakan komposisi dari sikel-3.

Lemma 5.11.3 Bila N adalah subgrup normal dari A_n, $n \geq 3$ dan N memuat suatu sikel-3, maka $N = A_n$.

Bukti
Berdasarkan Lemma 5.11.2, cukup dibuktikan bahwa sebarang sikel-3 yaitu $(r\ s\ t)$ berada di N dengan $1 \leq r, s, t \leq n$. Sebagaimana diketahui N memuat suatu sikel-3, misalkan dalam hal ini $(a\ b\ c) \in N$. Selain itu N adalah subgrup normal dari A_n. Maka $\alpha(a\ b\ c)\alpha^{-1} \in N, \forall \alpha \in A_n$. Sehingga didapat

- $(a\ t\ c)(a\ b\ c)(a\ c\ t) = (a\ t\ b) \in N$, hal ini berakibat bahwa
- $(r\ a\ t)(a\ t\ b)(r\ t\ a) = (r\ b\ t) \in N$, hal ini berakibat bahwa
- $(b\ s\ a)(r\ b\ t)(b\ a\ s) = (r\ s\ t) \in N$.

Terlihat sebarang sikel-3 yaitu $(r\ s\ t)$ berada di N. Dengan demikian $N = A_n$.

Berikut ini ditunjukkan bahwa A_n, $n \geq 5$ adalah grup sederhana, yaitu tidak memuat subgrup normal sejati yang tak-trivial.

Teorema 5.11.3 Grup permutasi genap A_n, $n \geq 5$ adalah grup sederhana.

Bukti
Andaikan A_n, $n \geq 5$ memuat subgrup normal tak-trivial N. Misalkan $\sigma \in N$ dengan σ bukan elemen identitas yang mepermutasikan paling sedikit k bilangan bulat. Dalam hal ini adalah tidak ada permutasi $\gamma \in N$ yang bukan identitas dengan γ mempermutasikan bilangan bulat $j < k$. Bila $k = 3$, maka σ adalah sikel-3 dan berdasarkan Lemma 5.11.3 maka $N = A_n$. Kontrakdiksi bahwa N subgrup normal tak-trivial dari A_n. Asumsikan bahwa $k \geq 4$ dan dekomposisikan σ kedalam suatu komposisi sikel yang saling asing, yaitu:

$$\sigma = \sigma_1\sigma_2\sigma_3\cdots\sigma_m.$$

Dalam hal ini ditinjau dua kasus:

- Kasus 1: Untuk beberapa i, σ_i adalah sikel-q dengan $q \geq 3$.
  Pada kasus ini, tampa mengurangi kegeneralitasan diasumsikan bahwa

  $$\sigma = (1\ 2\ 3\cdots)\tau,$$

  dengan τ adalah saling asing dengan $(1\ 2\ 3\cdots)$. Bila σ mempermutasi 4 bilangan bulat, maka $\sigma = (1\ 2\ 3\ a)$ dengan $a \neq 1, 2, 3$. Dalam hal ini σ adalah permutasi ganjil. Jadi $\sigma \notin N$. Dengan demikian σ mempermutasi setidaknya 5 bilangan bulat. Tampa mengurangi kegeneralitasan, diasumsikan $\sigma(4) = a_4$ dan $\sigma(5) = a_5$. Misalkan $\beta = (3\ 4\ 5)$ dan

  $$\gamma = \sigma^{-1}\beta\sigma\beta^{-1}.$$

  Karena N subgrup normal dari A_n, maka $\beta\sigma\beta^{-1} \in N$. Jadi, $\gamma \in N$. Selanjutnya

  $$\gamma(1) = \sigma^{-1}\beta\sigma\beta^{-1}(1) = \sigma^{-1}\beta\sigma(1) = \sigma^{-1}(2) = 1,$$

  jadi $\gamma \neq \sigma$. Lagipula,

  $$\gamma(2) = \sigma^{-1}\beta\sigma\beta^{-1}(2) = \sigma^{-1}\beta\sigma(2) = \sigma^{-1}\beta(3) = \sigma^{-}(4) \neq 2.$$

  Jadi γ bukan permutasi identitas. Juga bila $t > 5$ dan $\sigma(t) = t$, maka juga $\gamma(t) = t$. Karena $\gamma(1) = 1$, maka γ mempermutasi lebih sedikit elemen dari pada σ yaitu lebih kecil dari k. Tetapi telah ditunjukkan bahwa $\gamma \in N$ dan bukan elemen identitas. Hal ini kontradiksi bahwa tidak ada permutasi γ di N yang mempemutasikan bilangan bulat lebih kecil dari k.

- Kasus 2: Untuk masing-masing i, σ_i adalah suatu transposisi.
  Pada kasus ini, tanpa mengurangi kegenaralitasan diasumsikan bahwa

  $$\sigma = (1\ 2)(3\ 4)(5\ 6)\cdots .$$

  Lagi, misalakan $\beta = (3\ 4\ 5)$ dan

  $$\gamma = \sigma^{-1}\beta\sigma\beta^{-1}.$$

  Maka $\gamma(1) = 1$ dan $\gamma(2) = 2$. Bila untuk sebarang $t > 5$, $\sigma(t) = t$, maka $\gamma(t) = t$. Juga

  $$\gamma(3) = \sigma^{-1}\beta\sigma\beta^{-1}(3) = \sigma^{-1}\beta\sigma(5) = \sigma^{-1}(6) = 5 \neq 3.$$

  Jadi γ bukan elemen identitas. Disini juga γ mempermutasikan bilangan bulat yang lebih kecil dari k. Hal ini juga terjadi kontradiksi.

Dari dua kasus yang telah dibahas terjadi kontradiksi. Dengan demikian haruslah A_n tidak memuat suatu subgrup normal sejati tak-trivial. Jadi untuk $n \geq 5$, A_n adalah grup sederhana.

Catatan.
Teorema 5.11.3 menyatakan bahwa grup alternating A_n, $n \geq 5$ adalah sederhana. Lalu bagaimana untuk $n < 5$. Untuk hal ini dibahas sebagai berikut. Sebagaimana telah diketahui, grup alternating A_n adalah grup berorder $n!/2$ dan hanya didefinisikan untuk $n \geq 2$. Bila $n = 2$, maka $A_2 = \{e\}$ adalah grup trivial. Dengan demikian A_2 bukan grup sederhana. Bila $n = 3$, maka $|A_3| = 3!/2 = 3$. Jadi $A_3 \cong \mathbb{Z}_3$. Dengan demikian A_3 adalah grup sederhana. Untuk $n = 4$, mempunyai subgrup normal sejati tak-trivial $N = \{e, (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}$. Jadi A_4 bukan grup sederhana.

Dalam koleksi karya yang luar biasa, matematikawan telah dapat mengklasifikasikan semua grup berhingga sederhana. Hasil akhirnya adalah upaya gabungan dari ratusan peneliti yang menghasilkan lebih dari 500 artikel lebih dari 14.000 halaman jurnal. Pada dasarnya, buktinya menyatakan bahwa grup berhingga sederhana terdiri dalam dua kategori: beberapa kumpulan takhingga grup memiliki pola yang mapan, dan 26 grup lainnya yang dikenal sebagai grup sporadis:

(1) Grup siklik berorder prima,

(2) Grup Alternating A_n berorder $n \geq 5$,

(3) Group Lie bertipe grup Chavalley,

(4) Group Lie bertipe grup Chavalley bengkok atau grup Tit dan

(5) Grup sporadis :

- Grup Mathieu $M_{1,1}, M_{1,2}, M_{2,2}, M_{2,3}, M_{2,4}$
- Grup Janko J_1, J_2 (juga dikenal sebagai grup Hall-Janko HJ), J_3, J_4
- Grup Conway Co_1, Co_2, Co_3
- Grup Fischer $F_{2,2}, F_{2,3}, F_{2,4}$
- Grup Higman-Sims HS
- Group McLaughlin McL

- Grup Held *He*
- Grup Rudvalis *Ru*
- Grup sporadis Suzuki *Suz*
- Grup O'Nan *O'N*
- Grup Harada-Norton *HN*
- Grup Lyons *Ly*
- Grup Thompson *Th*
- Grup Baby Monster *B*
- Grup Monster *M*.

Lima dari grup sporadis ini ditemukan pada sekitar 1860 dan 21 lainnya ditemukan antara 1965 dan 1975. Grup Monster sesuai namanya yang tepat adalah yang terbesar dari grup sporadis dan mempunyai order

808 017 424 794 512 875 886 459 904 961 710 757 005 754 368 000 000 000.

Dari segi besarnya order grup, sungguh tepat disebut monster.

Latihan

Latihan 5.11.1 Misalkan $\sigma = (1\ 2)(3\ 4\ 5)(6\ 7\ 8\ 9) \in S_9$.

(a) Tulis dua permutasi ρ, τ yang merupakan konjugate dari σ di S_9.

(b) Dapatkan permutasi ϕ, χ dan ψ yang memenuhi $\rho = \phi\sigma\phi^{-1}, \tau = \chi\sigma\chi^{-1}$ dan $\tau = \psi\rho\psi^{-1}$.

Latihan 5.11.2 Dalam masing-masing kasus berikut tentukan apakah σ dan ρ berkonjuget di S_{10}. Bila berkonjuget, dapatkan τ yang memenuhi $\rho = \tau\sigma\tau^{-1}$.

$(a)\ \sigma = (1\ 3)(2\ 4\ 5)$,	$\rho = (3\ 1\ 5)(2\ 4)$
$(b)\ \sigma = (1\ 3)(2\ 4\ 5)$,	$\rho = (6\ 2)(8\ 9)(6\ 5)$
$(c)\ \sigma = (1\ 2\ 3)(4\ 5\ 6\ 7)$,	$\rho = (1\ 2)(3\ 4)(5\ 6\ 7)$
$(d)\ \sigma = (2\ 4\ 5)(3\ 5\ 6)$,	$\rho = (6\ 7\ 8\ 9\ 10)$
$(e)\ \sigma = (2\ 4\ 5)(4\ 5\ 6)$,	$\rho = (2\ 4\ 5\ 6\ 8)$
$(f)\ \sigma = (2\ 4)(8\ 3\ 6)(9\ 7\ 5\ 1)$,	$\rho = \sigma^2$.

Latihan 5.11.3 Buat tabel klas konjugasi dari S_5 sebagaimana dalam S_4 yang dibahas pada Contoh 5.11.4.

Latihan 5.11.4 Berapakah banyaknya klas konjugasi dalam grup permutasi S_n untuk $n = 6, n = 7$ dan $n = 8$?

Latihan 5.11.5
(a) Dapatkan senter $Z(S_3)$ dari S_3.
(b) Dapatkan senter $Z(S_n)$ dari S_n untuk $n > 3$.

Latihan 5.11.6 Tunjukkan bahwa bila $\tau = (x\ y)(u\ v)$ merupakan komposisi dari dua sikel-2 yang saling asing di S_n dengan $n \geq 4$, maka banyaknya konjuget dari τ di S_n adalah $n!/8.(n-4)!$.

Latihan 5.11.7 Untuk masing-masing $\sigma = (5\ 2\ 4)$, $\sigma = (3\ 5\ 2\ 4\ 1)$ dan $\sigma = (4\ 1)(5\ 2)$ di S_5.
(a) Dapatkan banyaknya konjuget dari σ di S_5.
(b) Dapatkan sentralisir dari σ di S_5.
(c) Dapatkan sentralisir dari σ di A_5.
(d) Dapatkan konjuget dari σ di A_5.

Latihan 5.11.8 Dapatkan dua permutasi σ dan ρ di S_5 yang berkonjuget di S_5 tetapi tidak berkonjuget di A_5.

5.12 Teorema Sylow

Sylow, nama lengkapnya Peter Ludwig Mejdell Sylow. Ia lahir dan meninggal di Christiania (sekarang Oslo). Sylow adalah putra menteri pemerintah Thomas Edvard von Westen Sylow, dan saudara dari perwira militer dan pejabat olahraga Carl Sylow. Dia bersekolah di Christiania Cathedral School (1850) dan University of Christiania (cand.real. 1856).

Sylow adalah seorang guru sekolah menengah di Hartvig Nissen School, kemudian sebelum menjadi kepala sekolah di Halden dari tahun 1858 hingga 1898. Ia adalah dosen pengganti di Universitas Christiania pada tahun 1862, yang meliput teori Galois. Saat itulah dia mengajukan pertanyaan yang mengarah pada teorema tentang subgrup Sylow. Sylow menerbitkan teorema Sylow pada tahun 1872, dan kemudian mengabdikan delapan tahun hidupnya, bersama Sophus Lie, untuk proyek pengeditan karya matematika rekan senegaranya, Niels Henrik Abel. Pada tahun 1898, ia diangkat sebagai profesor di Universitas Christiania.

Pada tahun 1853, ia dianugerahi medali emas Putra Mahkota (Kronprinsens gullmedalje) oleh Universitas Oslo. Pada tahun 1868 ia terpilih menjadi anggota Akademi Sains dan Sastra Norwegia. Pada tahun 1894 ia dianugerahi gelar doktor kehormatan dari Universitas Kopenhagen dan menjadi editor untuk Acta Mathematica.

Teorema Sylow adalah pernyataan yang kuat tentang struktur grup secara umum, tetapi juga kuat dalam aplikasi teori grup berhingga. Ini karena mereka memberikan metode untuk menggunakan dekomposisi prima dari kardinalitas grup hingga G untuk memberikan pernyataan tentang struktur subgrupnya: pada dasarnya, ini memberikan teknik untuk mengangkut informasi dasar teori bilangan tentang suatu grup ke struktur grupnya. Dari pengamatan ini, mengklasifikasikan kelompok hingga menjadi permainan menemukan kombinasi/konstruksi grup mana yang lebih kecil dapat diterapkan untuk membangun sebuah grup. Sebagai contoh, aplikasi tipikal dari teorema-teorema ini adalah dalam klasifikasi berhingga dari beberapa order grup tetap, misalnya $|G| = 60$.

Teorema Lagrange menyatakan bahwa order subgrup membagi order grupnya. Dalam kasus grup Abelian, hal yang sebaliknya juga benar: Jika suatu bilangan bulat positip m membagi order suatu grup, ada suatu subgrup yang berorder m. Hal ini mengikuti teorema dasar untuk grup berhingga Abelian, yang memberikan lengkap pemahaman tentang struktur grup berhingga Abelian. Struktur grup berhingga yang bukan Abelian lebih rumit. Tetapi kebalikan dari teorema Lagrange memang terpenuhi setidaknya bila order grup

adalah pangkat dari suatu bilangan prima. Ini salah satunya konsekuensi dari klaster hasil yang dikenal sebagai teorema Sylow.

Bukti teorema ini adalah aplikasi langsung dari teori tindakan grup. Khususnya tindakan dengan konjugasi grup G pada himpunan S dari semua subgrupnya. Hasil paling dasar adalah relasi orbit-stabilizer. Berkaitan dengan hal ini, kardinalitas kelas konjugasi $K(H)$ dari suatu subgrup H dalam G sama dengan indeks normalizer $N(H)$ dari H dalam G (Proposisi 5.10.2).

Sebelum membahas teorema Sylow, terlebih dulu dibahas teorema Cauchy yang umum yaitu untuk grup yang Abelian ataupun bukan Abelian. Untuk grup Abelian telah dibahas dalam Teorema 3.4.4.

Teorema 5.12.1 Misalkan G berhingga dan p bilangan prima yang membagi order $|G|$. Maka G mempunyai suatu elemen yang berorder p atau ekivalen memuat suatu subgrup siklik berorder p.

Bukti

Bukti dilakukan untuk dua kasus:

Kasus I : Bila G adalah grup Abelian (komutatif). Ditulis ulang apa yang telah dibuktikan dalam Teorema 3.4.4. Digunakan induksi pada $|G|$. Bila $|G| = 1$ tidak ada yang perlu dibuktikan. Bila $|G| = 2$ atau 3, maka G siklik, dan pernyataan dalam teorema benar. Asumsikan pernyataan benar untuk semua grup komutatif yang mempunyai order lebih kecil dari $|G|$. Bila G tidak mempunyai subgrup sejati tak-trivial, maka G adalah siklik, maka menurut Teorema 2.3.4 pernyataan teorema benar. Selanjutnya, misalkan H adalah suatu subgrup sejati tak-trivial dari G. Bila p membagi $|H|$, maka karena H adalah grup komutatif yang memenuhi $|H| < |G|$, menurut hipotisis induksi ada suatu elemen $a \in H \subset G$ yang berorder p. Dengan demikian benar pernyataan teorema. Berikutnya asumsikan bahwa p tidak membagi $|H|$. Karena G komutatif, maka $H \lhd G$ dan G/H adalah suatu grup komutatif yang memenuhi $|G/H| = |G|/|H|$. Karena H taktrivial, maka $|G|/|H| < |G|$ dan karena p membagi $|G|$ dan tidak membagi $|H|$, maka p membagi $|G|/|H|$. Jadi dengan hipotisis induksi ada suatu elemen $X \in G/H$ yang mempunyai order p. Himpunan X mempunyai bentuk bH untuk beberapa $b \in G$, dimana $bH \neq H$ dan $(bH)^p = H$. Jadi $b \notin H$ (karena $bH \neq H$), tetapi karena $b^pH = (bH)^p = H$, maka $b^p \in H$. Misalkan $c = b^{|H|} \in G$. Maka

$$c^p = \left(b^{|H|}\right)^p = (b^p)^{|H|} = e \text{ (karena } b^p \in H).$$

Tinggal menunjukkan bahwa $c \neq e$. Andaikan $c = e$, maka $e = b^{|H|}$ sehingga didapat

$$H = eH = b^{|H|}H = (bH)^{|H|}$$

dan menurut Akibat 2.3.1, maka p harus membagi $|H|$. Hal ini bertentangan dengan kenyataan asumsi bahwa p tidak membagi $|H|$. Jadi haruslah $c \neq e$ dan $|c| = p$.

Kasus II : grup G bukan Abelian (tak-komutatif) Dibuktikan dengan induksi pada $|G|$. Karena G non-Abelian, maka $|G| = n \neq p$. Sebab bila $|G| = p$ dengan p adalah bilangan prima, maka sebagaimana telah diketahui G adalah grup Abelian. Dengan demikian sebagai hipotesis induksi, misalkan $n > p$ dengan p membagi n dan teorema benar untuk semua grup yang mempunyai order lebih kecil dari $n = |G|$. Selanjutnya, andaikan G tidak memuat elemen berorder p. Akan ditunjukkan terjadi suatu kontrakdiksi. Bila dalam setiap subgrup sejati H dari G tidak memuat elemen yang berorder p. Dalam hal ini H mungkin Abelian atau bukan

Abelian. Jadi, dengan induksi tidak ada subgrup sejati dari G yang mempuyai order bisa dibagi oleh p. Untuk masing-masing subgrup sejati H, didapat

$$|G| = |H|.[G : H]$$

dan $|H|$ tidak bisa dibagi oleh p sedangkan $|G|$ bisa dibagi oleh p. Jadi p bisa membagi $[G : H]$ untuk setiap subgrup sejati H dari G.

Karena G non-Abelian, maka G mempunyai beberapa klas konjugasi dengan kardinalitas lebih besar satu. Misalkan klas-klas konjugasi tersebut secara lengkap direpresentasikan oleh $a_1, a_2, \ldots, a_r$ dengan $a_i \notin Z(G), \forall i, 1 \leq i \leq r$. Perhatikan bahwa klas-klas konjugasi dalam G yang mempunyai kardinalitas sama dengan satu adalah $Z(G)$ senter dari G. Sehingga dengan menggunakan persamaan klas (Teorema 5.10.1) didapat

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C(a_i)],$$

dengan $C(a_i)$ sentralisir dari a_i. Karena klas konjugasi dari masing-masing a_i mempunyai kardinalitas lebih besar dari 1, maka $[G : C(a_i)] > 1$. Jadi $C(a_i) \neq G$ untuk semua i. Maka dari itu p membagi $[G : C(i)]$ untuk semua i. Akibatnya p juga membagi $\sum_{i=1}^{r} [G : C(a_i)]$. Dari persamaan klas didapat

$$|G| - \sum_{i=1}^{r} [G : C(a_i)] = |Z(G)|. \tag{5.10}$$

Karena p bisa membagi G dan juga $\sum_{i=1}^{r} [G : C(a_i)]$, maka berdasarkan Persamaan 5.10 p bisa membagi $|Z(G)|$. Karena tidak ada subgrup sejati dari G mempunyai order yang bisa dibagi oleh p, maka $|Z(G)| = |G|$. Jadi $G = Z(G)$, hal ini berarti G grup Abelian. Bertentangan dengan kenyataan bahwa G grup non-Abelian. Jadi haruslah G memuat elemen berorder p. Dengan demikan subgrup $H = \langle p \rangle$ dari G berorder p. Dengan demikian dari pembahasan Kasus I dan II lengkap sudah bukti.

Definisi 5.12.1 Misalkan p adalah suatu bilangan prima. Ingat kembali bahwa suatu grup berorder p^n untuk beberapa $n \geq 1$ dinamakan p-**grup**. Misalkan G adalah suatu grup berhingga. Sebarang subgrup dari G yang merupakan suatu p-grup dinamakan p-**subgrup** dari G. Bila $|G| = p^n.m$ dengan $n > 0$ dan p tidak membagi m, maka sebarang subgrup-p dari G berorder p^n dinamakan suatu p-**subgrup Sylow** dari G.

Contoh 5.12.1 Misalkan $G = S_3$, maka $|G| = 3! = 2.3$. Untuk $p = 3$, ada 3-subgrup Sylow $A_3 = \langle (1\ 2\ 3) \rangle$. Karena hanya (1 2 3) dan inversnya (1 3 2) yang berorder 3. Maka hanya subgrup $A_3 = \langle (1\ 2\ 3) \rangle = \langle (1\ 3\ 2) \rangle$ yang merupakan 3-subgrup Sylow. Untuk $p = 2$, ada tiga 2-subgrup Sylow dalam S_3 yaitu, $\langle (1\ 2) \rangle, \langle (1\ 3) \rangle$ dan $\langle (2\ 3) \rangle$. Karena (1 3)(1 2)(1 3) = (2 3) dan (2 3)(1 2)(2 3) = (1 3), maka tiga 2-subgrup Sylow saling berkonjuget satu dengan yang lainnya.

Contoh 5.12.2 Misalkan $G = A_4$, maka $|G| = 2^2.3$. Untuk $p = 2$, G mempunyai 2-subgrup Sylow

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}.$$

Karena tiga elemen yang bukan elemen identitas e semuanya adalah elemen-elemen berorder 2 dalam G. Maka hanyalah subgrup H yang merupakan 2-subgrup Sylow. Untuk $p = 3$, grup G juga mempunyai setidaknya empat 3-subgrup Sylow, yaitu $P = \langle(1\ 2\ 3)\rangle$ dan $\langle(1\ 2\ 4)\rangle, \langle(1\ 3\ 4)\rangle, \langle(2\ 3\ 4)\rangle$. Karena semua empat elemen yaitu $(1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (2\ 3\ 4)$ dan inversnya semuanya berorder 3. Maka subgrup-subgrup tersebut semuanya adalah subgrup-3 Sylow. Selanjutnya, perhatikan bahwa

$$\begin{aligned}(1\ 2)(3\ 4)P(1\ 2)(3\ 4) &= \langle(1\ 2\ 4)\rangle\\ (1\ 3)(2\ 4)P(1\ 3)(2\ 4) &= \langle(1\ 3\ 4)\rangle\\ (1\ 4)(2\ 3)P(1\ 4)(2\ 3) &= \langle(2\ 3\ 4)\rangle.\end{aligned}$$

Jadi $P, (1\ 2\ 4), (1\ 3\ 4)$ dan $(2\ 3\ 4)$ saling berkonjugate. Perhatikan bahwa karena $|A_4| = 2^2.3$, maka menurut Teorema Cauchy A_4 mempunyai subgrup berorder 2 dan subgrup berorder 3. Ada enam subgrup dari A_4 berorder 2, yaitu

$$\begin{array}{lll}\{e, (1\ 2)\}, & \{e, (1\ 3)\}, & \{e, (1\ 4)\}\\ \{e, (2\ 3)\}, & \{e, (2\ 4)\}, & \{e, (3\ 4)\}.\end{array}$$

Sebagaimana telah dijelaskan sebelumnya ada empat subgrup dari A_4 yang berorder 3 yaitu

$$\begin{array}{ll}\{e, (1\ 2\ 3), (1\ 3\ 2)\}, & \{e, (1\ 2\ 4), (1\ 4\ 2)\}\\ \{e, (1\ 3\ 4), (1\ 4\ 3)\}, & \{e, (2\ 3\ 4), (2\ 4\ 3)\}.\end{array}$$

Tetapi subgrup dari A_4 yang berorder $4 = 2^2$ yaitu

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

tidak terpredeksi oleh Teorema Cauchy. Tetapi, subgrup H dari A_4 berorder 2^2 ini eksis sebagaimana nantinya ditunjukkan dalam Teorema Sylow Pertama. Juga, walaupun 6 membagi $2^2.3 = |A_4|$, grup A_4 tidak memuat subgrup yang berorder 6. Andaikan $HK < A_4$ dengan $|K| = 6$. Misalkan K memuat beberapa sikel-3 yaitu : α, α^{-1} dan β, β^{-1}. Maka $e, \alpha, \alpha^{-1}, \beta, \beta^{-1}, \alpha\beta$ dan $\alpha\beta^{-1}$ semua tujuh elemen ini di K. Hal ini tidak mungkin sebab $|K| = 6$. Selanjutnya bila K hanya memuat dua sikel-3 , maka sisanya harus terdiri dari elemen-elemen dari A_4, yaitu $e, (1\ 2)(3\ 4), (1\ 3)(2\ 4)$ dan $(1\ 4)(2\ 3)$. Tetapi semua elemen tersebut adalah elemen-elemen di H dan merupakan subgrup dari A_4 dan tidak mungkin merupakan subgrup dari K sebab $4 = |H|$ tidak membagi $6 = |K|$. Dengan demikian tidak akan mungkin A_4 mempunyai subgrup K dengan $|K| = 6$. ●

Contoh 5.12.3 Misalkan

$$G = D_6 = \{\rho_0, \rho, \rho^2, \ldots, \rho^5, \tau, \rho\tau, \rho^2\tau, \ldots, \rho^5\tau\},$$

dengan ρ adalah suatu rotasi 60° dan τ adalah suatu pencerminan pada suatu diagonal tetap, sehingga $\rho\tau = \tau\rho^5$ (sebagaimana dibahas dalam Contoh 5.3.3). Maka order $|G| = 2^2.3$. Untuk $p = 3$, karena hanya elemen ρ^2 dan ρ^4 yang berorder 3. Maka hanya ada satu 3-subgrup Sylow yaitu $\{e, \rho^2, \rho^4\}$. Untuk $p = 2$, G setidaknya mempunyai tiga subgrup-2 Sylow, yaitu

$$Q = \{e, \tau, \rho^3, \rho^3\tau\},\quad \{e, \rho\tau, \rho^3, \rho^4\tau\}\quad \text{dan}\quad \{e, \rho^2\tau, \rho^2, \rho^5\tau\}.$$

Tujuh elemen bukan elemen identitas : $\tau, \rho, \rho^3\tau, \rho\tau, \rho^4\tau, \rho^2\tau$ dan $\rho^5\tau$ semuanya berorder 2 dan tidak ada elemen yang berorder 4. Jadi, setiap subgrup-2 Sylow harus terdiri dari elemen identitas dan tiga dari tujuh elemen tersebut. Dengan demikian tidak ada 2-subgrup Sylow yang lainnya selain tiga subgrup yang telah ditampilkan. Sebab sebarang grup berorder 4 adalah Abelian dan dua dari elemen-elemen $\rho^3\tau, \rho^4\tau, \rho^5\tau$ tidak kumutatif satu dengan yang lainnya. Dapat diselidiki bahwa

$$\rho^2 Q \rho^4 = \{e, \rho^2\tau, \rho^3, \rho^5\tau\} \quad \text{dan} \quad \rho Q \rho^5 = \{e, \rho\tau, \rho^3, \rho^4\tau\}.$$

Dengan demikian, tiga 2-subgrup Sylow semuanya berkonjuget. ●

Dari tiga contoh yang telah dibahas didapat p-subgrup Sylow untuk semua bilangan prima p yang membagi order dari grupnya. Bahkan, teorema pertama dari tiga teorema Sylow menjamin bahwa p-subgrup Sylow ada (exist).

Teorema 5.12.2 (**Teorema Sylow Pertama**) Misalkan p suatu bilangan prima. Bila G adalah suatu grup berhingga berorder $|G| = p^n.m$, dengan $n \geq 1$ dan p tidak membagi m (fpb$(p, m) = 1$). Maka untuk k dengan $1 \leq k \leq n$, G memuat setidaknya satu subgrup berorder p^k (jadi, memuat suatu p-subgrup Sylow).

Bukti
Digunakan induksi pada $|G|$. Bila $|G| = 2$ dalam hal ini $n = 1$, maka $H = \{e, a\} = 2^1$ adalah subgrup yang merupakan G sendiri dan memenuhi kriteria berorder p^n. Dengan demikian secara induktif diasumsikan bahwa teorema benar untuk semua grup yang berorder lebih kecil dari order grup G mempunyai subgrup berorder p^n. Dalam hal ini diasumsikan $n \geq 1$. Ada dua kasus, **kasus pertama** misalkan p membagi $|Z(G)|$, dimana $Z(G) = \{x \in G \,|\, xy = yx, \forall y \in G\}$ adalah senter dari G dan ingat bahwa $Z(G) \lhd G$. Karena p membagi $|Z(G)|$, dan berdasarkan Teorema Cauchy untuk grup komutatif (Teorema 3.4.4), maka ada $b \in Z(G)$ dengan $|b| = p$. Misalkan $H = \langle b \rangle \lhd Z(G)$. Maka H adalah subgrup normal dari G. Sehingga didapat

$$|G/H| = \frac{|G|}{|H|} = \frac{p^n.m}{p} = p^{n-1}.m < p^n.m = |G|.$$

Dengan demikian berdasarkan hipotesis induksi G/H mempunyai subgrup K/H yang berorder p^{n-1}. Jadi, K adalah subgrup dari G yang berorder $|K| = |K/H|.|H| = p^{n-1}.p = p^n$, sebagaimana yang dikehendaki.

Selanjutnya, **kasus kedua** misalkan bahwa p tidak membagi $Z(G)$. Ingat kembali persamaan klas (Teorema 5.10.1)

$$|G| = |Z(G)| + \sum_{i=1}^{r} [G : C(a_i)],$$

dengan $a_1, a_2, \ldots, a_r$ membentuk suatu himpunan lengkap representasi dari klas konjugasi yang tidak berada dalam senter $Z(G)$. Karena $a_i \notin Z(G)$, semua $C(a_i)$ adalah subgrup sejati dari G. Dari hipotesis diketahui bahwa p membagi $p^n.m = |G|$. **Andaikan** p membagi $[G : C(a_i)], \forall i = 1, 2, \ldots, r$, maka dari persamaan klas p juga membagi

$$|G| - \sum_{i=1}^{r} [G : C(a_i)] = |Z(G)|,$$

hal ini kontradiksi dengan p tidak membagi $Z(G)$. Sehingga dapat dipilih a_{i_0} dengan $1 \leq i_0 \leq r$ supaya p tidak membagi $[G : C(a_{i_0})]$. Perhatikan bahwa

$$p^n.m = |G| = [G : C(a_{i_0})].|C(a_{i_0})|.$$

Karena p tidak membagi $[G : C(a_{i_0})]$, maka p^n membagi $|C(a_{i_0})|$. Karena $C(a_{i_0})$ adalah subgrup sejati dari G dan $|C(a_{i_0})| < p^n.m = |G|$ juga p^n membagi $|C(a_{i_0})|$, maka berdasarkan hipotesis induksi $C(a_{i_0})$ mempunyai subgrup P berorder p^n. Dengan demikian P juga merupakan subgrup dari G yang berorder p^n.

Dalam banyak kasus, Teorema Pertama Sylow memberikan lebih banyak informasi tentang order subgrup daripada Teorema Cauchy.

Contoh 5.12.4 Misalkan G adalah suatu grup berorder $12 = 2^2.3$. Maka Teorema Cauchy menginformasikan bahwa G memiliki subgrup (siklik) berorder 2 dan 3, karena ini adalah faktor prima dari 12. Tetapi Teorema Pertama Sylow menginformasikan bahwa G juga harus memiliki subgrup dengan order $4 = 2^2$. Tidak hanya itu, setiap subgrup (normal) berorder 2 termuat dalam subgrup berorder 4.

Contoh 5.12.5 Diberikan grup dengan order 72, dan faktorisasi primanya: $2 = 2^3 3^2$. Dengan Teorema Sylow I, kita mengetahui bahwa terdapat subgrup berorder 8 dan juga subgrup berorder 9, tanpa informasi lebih lanjut tentang struktur grup.

Contoh 5.12.6 Misalkan G adalah suatu grup berorder $8 = 2^3$. Sebagaimana telah diketahui dalam pembahasan grup Abelian berhingga. Grup berorder 8 isomorpik dengan $\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, grup dihedral D_4 dan grup quaternion Q_8. Teorema Cauchy menginformasikan bahwa G harus memiliki setidaknya satu subgrup berorder 2, tetapi Teorema Pertama Sylow juga memastikan keberadaan subgrup berorder 4. Juga, subgrup-subgrup berorder 4 ini harus subgrup normal dalam G.

Tentu saja, sedikit informasi terakhir ini diketahui sebagaimana telah dibahas bahwa setiap subgrup berindeks 2 adalah subgrup normal.Namun, jika $|G| = 27 = 3^3$ maka G harus memiliki subgrup beroder 3 dan 9, juga subgrup berorder 9 semua harus subgrup normal.

Diinginkan informasi lebih banyak tentang subgrup-subgrup yang telah dibahas: bagaimana subgrup-subgrup ini terkait dan ada berapa banyak? Teorema lain Sylow memberikan jawaban untuk pertanyaan-pertanyaan ini. Berikut ini dibahas dengan cermat beberapa contoh kecil. (Lihat juga kembali Contoh-contoh yang telah dibahas dalam Contoh 5.12.1, 5.12.2 dan 5.12.3).

Contoh 5.12.7 Grup dihedral D_3 berorder $6 = 2 \cdot 3$. Grup $D_3 = S_3$, jadi pembahasan disini bisa dilihat lagi dalam pembahasan Contoh 5.12.1. Menurut Teorema Cauchy (dan, juga Teorema Sylow Pertama) D_3 setidaknya mempunyai satu subgrup berorder 2 dan setidaknya satu subgrup berorder 3. Faktanya D_3 mempunyai tiga subgrup berorder 2 yaitu

$$M_1 = \{e, m_1\}, M_2 = \{e, m_2\} \quad \text{dan} \quad M_3 = \{e, m_3\},$$

dengan m_i, $i = 1, 2, 3$ adalah pencerminan pada sumbu segitiga beraturan (sama sisi). Suatu pertanyaan yang mungkin bagaimana ini terkait, jawabannya adalah tiga pencerminan

m_1, m_2 dan m_3 semuanya saling konjugasi satu dengan yang lainnya, dan elemen identitas e membentuk kelas konjugasi tunggal sendiri. Setelah diperiksa lebih lanjut, dapat dikonstruksi subgrup $M_2 = \{e, m_2\}$ dari subgrup $M_1 = \{e, m_1\}$ dengan mengkonjugasikan setiap elemen melalui rotasi r sebesar $\frac{2\pi}{3}$:

$$e = rer^{-1}, \quad m_2 = rm_1r^{-1}.$$

Dengan cara yang sama, dapat dikonstruksi subgrup $M_3 = \{e, m_3\}$ dengan menkonjugasikan setiap elemen melalui rotasi $r^2 = r^{-1}$ sebesar $\frac{4\pi}{3}$:

$$e = r^{-1}er, \quad m_3 = r^{-1}m_1r.$$

Terlihat bahwa subgrup-subgrup tersebut saling berkonjugasi satu dengan yang lainnya, yaitu

$$M_2 = rM_1r^{-1} \quad \text{dan} \quad M_3 = r^{-1}M_1r.$$

Ada hanya satu subgrup berorder 3 yaitu subgrup rotasi $R_3 = \{e, r, r^2\}$. Subgrup R_3 adalah subgrup normal, jadi berkonjugasi dengan dirinya sendiri. ●

Dibahas contoh yang sedikit lebih besar grup simetris S_4.

Contoh 5.12.8 Grup simetris S_4 memiliki order $24 = 2^3.3$, maka dari itu menurut Teorema Pertama Sylow S_4 harus memiliki setidaknya satu subgrup masing-masing berorder $2, 3, 4$ dan 8. Bahkan, S_4 memiliki tiga subgrup berorder 8, masing-masing isomorpik dengan grup dihedral D_4, yaitu

$$\langle (1\ 2\ 3\ 4), (1\ 3)\rangle, \langle (1\ 2\ 4\ 3), (1\ 4)\rangle \quad \text{dan} \quad \langle (1\ 3\ 2\ 4), (1\ 2)\rangle.$$

Ini semua saling berkonjugasi; untuk melihat ini, hanya diperlukan memeriksa dua generator untuk setiap subgrup:

$$\begin{aligned} &(3\ 4)(1\ 2\ 3\ 4)(3\ 4) = (1\ 2\ 4\ 3), \quad (3\ 4)(1\ 3)(3\ 4) = (1\ 4),\\ &(2\ 3)(1\ 2\ 3\ 4)(2\ 3) = (1\ 3\ 2\ 4), \quad (2\ 3)(1\ 3)(2\ 3) = (1\ 2). \end{aligned}$$

Setidaknya harus ada satu subgrup berorder 3; faktanya ada empat:

$$\langle (1\ 2\ 3)\rangle, \langle (1\ 2\ 4)\rangle, \langle (1\ 3\ 4)\rangle \quad \text{dan} \quad \langle (2\ 3\ 4)\rangle.$$

Ini juga saling berkonjugasi:

$$\begin{aligned} &(3\ 4)(1\ 2\ 3)(3\ 4) = (1\ 2\ 4), \quad (2\ 3)(1\ 2\ 4)(2\ 3) = (1\ 3\ 4),\\ &(1\ 2)(1\ 3\ 4)(1\ 2) = (2\ 3\ 4), \quad (1\ 4)(2\ 3\ 4)(1\ 4) = (1\ 2\ 3). \end{aligned}$$ ●

Pola yang mulai terlihat disini jika p adalah faktor prima dari $|G|$, maka subgroup-p maksimal dari G saling berkonjugasi satu dengan lainnya. Apakah ini terjadi pada subgrup-p dari G yang lebih kecil? Hal ini bisa dilihat dalam contoh berikut.

Contoh 5.12.9 Grup S_4 mempunyai tujuh subgrup beroder $4 = 2^2$ yaitu

$$\begin{aligned} &\langle (1\ 2\ 3\ 4)\rangle, \quad \langle (1\ 2\ 4\ 3)\rangle, \quad \langle (1\ 3\ 2\ 4)\rangle,\\ &\langle (1\ 3)(2\ 4)\rangle, \quad \langle (1\ 4)(2\ 3)\rangle, \quad \langle (1\ 2)(3\ 4)\rangle,\\ &\langle (1\ 2)(3\ 4)(1\ 3)(2\ 4)\rangle. \end{aligned}$$

Tiga subgrup yang pertama semuanya isomorpik dengan grup siklik $\mathbb{Z}_4$. Sedangkan empat subgrup sisanya semuanya isomorpik dengan grup Klein $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Tetapi konjugasi oleh suatu elemen $g \in G$ menghasilkan isomporpisma dari subgrup H ke subgrup K yang lainnya yaitu $f_g : H \to K$, dengan $f_g(h) = ghg^{-1}$, $\forall h \in H$. Karena tidak semua subgrup berorder 4 tidak isomorpik, setidaknya beberapa dari mereka tidak dapat saling berkonjugasi.

Dari apa yang dibahas dalam Contoh 5.12.8 dan 5.12.9 dapat disimpulkan bahwa dalam grup S_4 yang berorder $|S_4| = 2^3 \cdot 3$ ada 2-subgrup Sylow dari S_4 yang maksimal dengan order $8 = 2^3$ sebanyak tiga semuanya saling berkonjugasi. Tetapi 2-subgrup dari S_4 yang lebih kecil dengan order 4 tidak semuanya saling berkonjugasi.

Teorema Sylow lainnya memberikan informasi tentang banyaknya p-subgrup Sylow dan hubungan di antara mereka. Sebelum membahas teorema ini, dibutuhkan beberapa lemma.

Lemma 5.12.1 Misalkan p adalah bilangan prima, G grup berhingga, P suatu p-subgrup Sylow dari G, $N_G(P) = \{g \in G \mid gPg^{-1} = P\}$ normalizer dari P di G, dan Q sebarang p-subgrup dari G. Maka $Q \cap N_G(P) = Q \cap P$.

Bukti
Misalkan $N = N_G(P)$. Karena $P \subseteq N$, kita memiliki $Q \cap P \subseteq Q \cap N$, dan hanya perlu membuktikan inklusi sebaliknya $Q \cap N \subseteq Q \cap P$. Berikutnya jelas bahwa $Q \cap N \subseteq Q$, kita hanya perlu membuktikan $Q \cap N \subseteq P$. Tulis $H = Q \cap N$. Maka P dan H keduanya adalah subgrup dari N dan order keduanya adalah pangkat p^n dan p^m dari bilangan prima p yang sama. Selain itu, P adalah subgrup normal dari N. Dengan Proposisi 3.3.3, PH adalah subgrup dari N, dengan Teorema 3.3.5 kita memiliki $|PH| = |P||H|/|P \cap H|$ dan begitu juga merupakan pangkat p^r dari p. Di satu sisi, karena order $|P| = p^n$ adalah pangkat tertinggi dari p Yang membagi $|G|$, kita harus memiliki $r \leq n$. Namun di sisi lain, karena $P \subseteq PH$, kita juga harus memiliki $n \leq r$. Oleh karena itu, $r = n$ dan $PH = P$, jadi $Q \cap N = H \subseteq P$.

Lemma 5.12.2 Misalkan p adalah bilangan prima, G grup berhingga, P suatu subgrup-p Sylow dari G, dan K himpunan semua konjugat dari P di G. Misalkan Q adalah sebarang subrup-p dari G, dan misalkan Q bertindak pada K melalui konjugasi. Misalkan $P = P_1, P_2, \ldots, P_r$ adalah suatu himpunan lengkap representasi orbit dalam tindakan ini. Maka

$$|K| = \sum_{i=1}^{r} [Q : Q \cap P_i].$$

Bukti
Karena P adalah himpunan lengkap representasi, maka $|K|$ sama dengan jumlah dari banyaknya orbit P_i. Dengan hubungan orbit-stabilizer, banyaknya orbit P_i adalah indeks dari stabilizer P_i, artinya, dari himpunan elemen Q yang meninggalkan P; fixed atau dengan kata lain $Q \cap N_G(P_i)$ yang menurut Lemma 5.12.1 sama dengan $Q \cap P_i$.

Teorema 5.12.3 *(Teorema Sylow kedua)* Misalkan p adalah bilangan prima dan G adalah grup berhingga. Maka bila P adalah subgrup-p Sylow dari G dan Q adalah sebarang subgrup-p dari G, maka Q termuat dalam beberapa konjugasi P (dan khususnya semua p-subgrup Sylow saling berkonjugasi satu sama lain).

Teorema 5.12.4 *(Teorema Sylow ketiga)* Misalkan p adalah bilangan prima, dan misalkan G adalah berhingga berhingga, dan anggaplah $|G| = p^n m$, dimana $n \geq 1$ dan p tidak membagi m. Misalkan n_p adalah banyaknya subgrup-p Sylow di G. Maka
(1) $n_p \equiv 1 \mod p$,
(2) n_p membagi m.

Bukti
Kita membuktikan teorema Sylow kedua dan ketiga bersama-sama.

Dengan notasi seperti dalam pernyataan teorema, misalkan K adalah himpunan semua konjugasi dalam G dari subgrup-p Sylow P dari grup G.
Ditunjukkan $|K| \equiv 1 \mod p$. Untuk hal ini, kita menerapkan Lemma 5.12.2 dengan $Q = P$. Di satu sisi, kita memiliki $P_1 = P$, jadi $[P : P \cap P_1] = 1$. Di sisi lain, untuk $i > 1$ kami memiliki $P_i \neq P$, jadi $[P : P \cap P_i] > 1$, dan $[P : P \cap P_i]$ adalah pangkat dari p. Maka dari Lemma 5.12.2 didapat $|K| = 1 +$ (suatu jumlah pangkat dari p). Dengan demikian $|K| \equiv 1 \mod p$, seperti yang kita harapkan.

Sekarang kita siap untuk membuktikan Teorema 5.12.3, dengan mengandaikan ada suatu subgrup-p Q yang tidak termuat dalam konjugasi P dan terjadi kontradiksi. Sekali lagi kita menerapkan Lemma 5.12.2. Bila Q tidak termuat dalam P_i manapun, maka untuk masing-masing i kita memiliki $[Q : Q \cap P_i] > 1$, maka $[Q : Q \cap P_i]$ adalah pangkat dari p. Maka dengan Lemma 5.12.2 didapat $|K| =$ (suat jumlah pangkat dar p). Dengan demikian $|K| \equiv 0 \mod p$, hal bertentangan dengan kenyataan $|K| \equiv 1 \mod p$ yang baru saja kita buktikan. Kontradiksi ini membuktikan Teorema 5.12.3.

Sekarang, membuktikan (1) dalam Teorema 5.12.4. Untuk ini memberitahu kita bahwa banyaknya $|K|$ dari konjugasi di G dari subgrup-p Sylow P memenuhi $|K| \equiv 1 \mod p$, sedangkan Teorema 5.12.3 memberitahu kita bahwa semua subgrup-p Sylow adalah konjugasi dari P di G, sehingga $|K|$ sama dengan jumlah total n_p dari subgrup-p Sylow. Dengan demikian $n_p \equiv 1 \mod p$.

Akhirnya, kita membuktikan (2) dalam Teorema 5.12.4. Karena menurut Proposisi 5.10.2 banyaknya $|K|$ dari konjugasi dari subgrup-p Sylow tertentu, yang sekarang kita ketahui sebagai jumlah total n_p dari subgrup-p Sylow, sama dengan indeks $[G : N] = |G|/|N|$, dimana $N = N_G(P)$ adalah normalizer dari P dalam G. Sekarang kita punyai $|G| = p^n \cdot m$, dengan p tidak membagi m, dan kita juga tahu $p^n = |P|$ membagi $|N|$, karena P adalah subgrup dari N. Maka n_p membagi m. ✓

Berikut ini adalah konsekuensi langsung dari teorema Sylow pertama dan kedua, masing-masing, dan buktinya akan diserahkan kepada pembaca. Bukti alternatif sudah dibahas pada Teorema 5.12.1.

Akibat 5.12.1 (**Teorema Cauchy**) Misalkan p adalah bilangan prima dan G grup berhingga. Jika p membagi order G, maka G memiliki elemen berorder p. ✓

Akibat 5.12.2 Misalkan G adalah grup berhingga dan p bilangan prima yang membagi $|G|$. Maka $n_p = 1$ bila dan hanya bila P Sylow p-subgrup adalah subgrup normal dari G. Oleh karena itu, bila banyaknya Sylow p-subgrup G adalah satu, maka G tidak sederhana. ✓

Kita akhiri bagian ini dengan versi yang lebih kuat dari teorema Sylow yang pertama. Untuk ini kita membutuhkan satu lemma lagi.

Lemma 5.12.3 Misalkan p bilangan prima, G grup berhingga, dan H adalah suatu p-subgrup dari G. Bila p membagi $[G : H]$, maka $H \neq N(H)$.

Bukti
Bukti kita gunakan kontraposisi yaitu bila $H = N(H)$, maka kita tunjukkan bahwa p tidak membagi $[G : H]$. Menurut definisi $[G : H] = |X|$ dimana X adalah himpunan semua koset kiri H dalam G. Misalkan H bertindak pada X dengan perkalian kiri. Maka $|X|$ adalah jumlah dari banyaknya orbit yang berbeda dalam tindakan ini. Sebagaimana telah dibahas, banyaknya setiap orbit membagi $|H|$ dan oleh karena itu salah satu dari 1 atau pangkat p. Banyaknya orbit koset gH akan menjadi tepat 1 dalam kasus dimana $(hg)H = gH$ untuk semua $h \in H$, hal ini ekivalen dengan $g^{-1}hg \in H$ untuk semua $h \in H$, yang menurut definisi ekivalen dengan memiliki $g \in N(H)$ normalisir dari H. Bila $H = N(H)$ maka hanya tepat ada satu orbit yaitu orbit H itu sendiri yang banyaknya 1, maka dalam hal ini $[G : H] = |X| \equiv 1 \mod p$ dan tidak habis dibagi oleh p. ✓

Teorema 5.12.5 Misalkan p adalah bilangan prima, juga misalkan G suatu grup berhingga, dan anggaplah $|G| = p^n m$ dimana $n \geq 1$ dan p tidak membagi m. Maka untuk semua k dengan $1 \leq k < n$, grup G setidaknya memuat satu subgrup berorder p^k yang merupakan subgrup normal dari subgrup berorder p^{k+1}.

Bukti
Menurut Teorema Sylow pertama ada subgrup H dari grup G berorder p^k dengan Teorema Sylow kedua termuat dalam beberapa p-subgrup Sylow P dari grup G. Misalkan N adalah normaliser dari H di P. Karena $k < n$ dan p membagi $[P : H]$ oleh karena itu dengan lemma yang baru dibahas sebelumnya $N \neq H$. Karena H subgrup normal dalam N, grup kuasi N/H terdefinisi, dan ordernya adalah pangkat dari p. Oleh karena itu dengan Akibat 5.12.1, ia memuat subgrup $U \subseteq N/H$ yang berorder p. Misalkan $\phi : N \to N/H$ adalah homomorpisma, memetakan setiap elemen $a \in N$ ke kosetnya aH dan misalkan $T = \phi^{-1}(U) = \{a \in N \mid \phi(a) \in U\}$. Maka T adalah subgrup dari N yang memuat H dan $|T| = |U| \times |H| = p \times p^k = p^{k+1}$. Karena H subgrup normal di N, ia juga subgrup normal di subgrup T. ✓

Contoh 5.12.10 Kita bahas, grup $G = S_4$, jadi $|G| = 4! = 24 = 2^3 \times 3$, dan suatu 2-subgrup Sylow akan memiliki order $2^3 = 8$. Menurut Teorema Sylow pertama, S_4 harus memiliki subgrup berorder 8. Dan sesuai dengan teorema tersebut, kita telah melihat bahwa grup dihedral D_4 memiliki representasi permutasi sebagai subgrup dari S_4. (Lihat Contoh 5.1.7 dan 2.4.11) ●

Contoh 5.12.11 Diberikan grup alternating $G = A_5$, jadi $|G| = 5!/2 = 60 = 2^2 \times 15$, dan 2-subgrup Sylow akan memiliki order $2^2 = 4$. Berikut ini adalah dua 2-subgrup Sylow :

$$\begin{aligned} P &= \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\} \\ Q &= \{e, (1\ 2)(3\ 5), (1\ 3)(2\ 5), (1\ 5)(2\ 3)\}. \end{aligned}$$

Menurut teorema Sylow kedua, ini harus berkonjugasi dalam A_5. Dan sesuai dengan teorema, kita dapat menghitungnya bila $\tau = (2\ 3)(4\ 5)$, maka $\tau(1\ 2)(3\ 4)\tau^{-1} = (1\ 3)(2\ 5)$ dan $\tau(1\ 3)(2\ 4)\tau^{-1} = (1\ 2)(3\ 5)$ dan $\tau(1\ 4)(2\ 3)\tau^{-1} = (1\ 5)(2\ 3)$, dengan demikian didapat $\tau P \tau^{-1} = Q$. ●

Contoh 5.12.12 Diberikan grup alternating $G = A_5$, jadi $|G| = 5!/2 = 60 = 2^2 \times 3 \times 5$, dan 2-subgrup, 3-subgrup dan 5-subgrup Sylow akan memiliki order masing-masing $2^2 = 4, 3,$ dan 5. Tidak ada elemen order 4 (karena ini harus 4-sikel, yang merupakan permutasi ganjil), dan satu-satunya elemen berorder 2 adalah hasil kali 2-siklus yang saling asing, $(x\ y)(u\ v)$. Setiap permutasi tersebut termasuk dalam suatu subgrup

$$\{e, (x\ y)(u\ v), (x\ u)(y\ v), (x\ v)(u\ y)\}$$

seperti pada contoh sebelumnya, dan setiap subgrup tersebut berisi tiga permutasi tersebut. Dalam Contoh 5.11.9 kita melihat bahwa banyaknya permutasi tersebut adalah 15. Oleh karena itu, banyaknya 2-subgrup Sylow adalah $15/3 = 5$. Adapun 3-subgrup Sylow dan 5-subgrup Sylow ini masing-masing akan dihasilkan oleh 3-sikel dan 5-sikel. Dalam Contoh 5.11.7 dan 5.11.8 kita melihat bahwa banyaknya dari 3-sikel adalah 20 dan banyaknya dari 5-sikel adalah 24. Karena setiap subgrup berorder 3 memuat dua 3-sikel dan setiap subgrup berorder 5 memuat empat 5-sikel, jumlah total grup tersebut masing-masing adalah $20/2 = 10$ dan $24/4 = 6$. Perhatikan yang kita miliki

$$\begin{aligned} 5 &\equiv 1 \mod 2 \text{ dan } 5 \text{ membagi } 3 \times 5 \\ 10 &\equiv 1 \mod 3 \text{ dan } 10 \text{ membagi } 2^2 \times 5 \\ 6 &\equiv 1 \mod 5 \text{ dan } 6 \text{ membagi } 2^2 \times 3 \end{aligned}$$

yang sesuai dengan teorema Sylow ketiga. ●

Contoh 5.12.13 Misalkan $P = \{e, \sigma = (1\ 2\ 3), \sigma^2 = (1\ 3\ 2)\}$ adalah suatu 3-subgrup Sylow dari A_5. Kita akan menentukan normalisir $N(P)$ dari P di A_5. Dari pembahasan contoh sebelumnya didapat P mempunyai 10 konjuguget, dengan demikian $[A_5 : N(P)] = 10$. Jadi, $|N(P)| = |A_5|/10 = 60/10 = 6$. Karena $P \subseteq N(P)$, maka kita hanya butuh mendapatkan suatu elemen τ berorder 2 di $N(P)$. Kita bisa memeriksa bahwa bila $\tau = (2\ 3)(4\ 5)$, maka $\tau\sigma\tau = \sigma^2$ dan $\tau\sigma^2\tau = \sigma$. Jadi, $\tau \in N(P)$ dan $N(P) = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. ●

Latihan

1. Tentukan order dari suatu p-subgrup Sylow dari G untuk p dan G sebagaimana berikut:
   - **(a)** $p = 2$ $G = S_5$,
   - **(b)** $p = 2$ $G = A_4$,
   - **(c)** $p = 2$ $G = D_6$,
   - **(d)** $p = 3$ $G =$ sebarang grup berorder 270.
2. Misalkan P adalah 2-subgrup Sylow dari grup G berorder 20. Bila P bukan subgrup normal dari G, berapa banyak konjuget yang dimiliki P di G?
3. Untuk latihan berikut temukan semua p-subgrup Sylow dari G untuk p dan G yang ditunjukkan, dan tunjukkan bahwa mereka adalah berkonjugasi.
   (a) $p = 3,\ G = S_4$ (b) $p = 2,\ G = S_4$ (c) $p = 2,\ G = A_5$.
4. Tentukan semua 3-subgrup Sylow dan 5-subgrup Sylow di S_5.

5. Tunjukkan bahwa irisan dari semua 2-subgrup Sylow di S_4 adalah subgrup normal dari S_4 isomorfik denga 4-grup Klein.

6. Misalkan P sebagaimana dalam Contoh 5.12.11. Dapatkan semua normalisir dari P di A_5.

7. Misalkan P sebagaimana dalam Contoh 5.12.13. Dapatkan semua normalisir dari P di A_5.

8. Dalam grup dihedral D_4, menurut Teorema 5.12.5 terdapat subgrup Q berorder 4 sehingga $P = \{e, \tau\}$ adalah subgrup normal di Q. Tentukan Q yang demikian itu.

9. Misalkan H adalah suatu subgrup normal dari G dan K adalah suatu subgrup normal dari H. Maka K adalah subgrup dari G. Apakah K harus **subgrup normal** dari G? Bila ya, berikan suatu bukti; jika tidak, berikan suatu contoh penyangkalnya.

10. Buktikan Akibat 5.12.2.

11. Tunjukkan bahwa tidak ada grup berorder pq dimana p dan q adalah bilangan prima yang berbeda adalah sederhana. (Petunjuk: Gunakan teorema Sylow ketiga dan Akibat 5.12.2).

12. Misalkan H adalah suatu p-subgrup normal dari grup berhingga G. Tunjukkan bahwa H termuat dalam setiap p-subgrup Sylow dari G.

13. Misalkan G adalah p-grup dan H subgrup sejati dari G. Tunjukkan bahwa terdapat subgrup $K \leq G$ sedemikian rupa sehingga
    (a) $H \leq K$ (b) $K \lhd G$ (c) $[G : K] = p$.

14. Tunjukkan bahwa tidak ada grup G berorder $|G| = n$ yang sederhana untuk
    (a) $n = 45$ (b) $n = 16$
    (c) $n = p^r, p$ prima dan $r > 1$ (d) $n = p^r m, p$ prima dan $r \geq 1, p > m$.

5.13 Aplikasi Teorema Sylow

Pada bagian ini, kita ingin mengeksplorasi beberapa aplikasi teorema Sylow. Kita mulai dengan lemma yang tidak memanggil salah satu teorema Sylow, tetapi akan berguna pada bagian ini.

Lemma 5.13.1 Setiap grup berorder prima adalah siklik.

Bukti
Dengan teorema Lagrange, kita tahu bahwa untuk setiap elemen $g \in G$, kita memiliki $|\langle g \rangle| \mid |G|$. Namun, jika G memiliki order prima dan g bukan elemen identitas, maka ini hanya dapat dipenuhi jika $\langle g \rangle = G$, jadi G adalah siklik. ✓

Sekarang, kita mulai aplikasi dari Teorema Sylow.

Teorema 5.13.1 (Wilson) Suatu bilangan asli p adalah prima jika dan hanya jika $(p-1)! \equiv 1 \mod p$.

Bukti
Kita hanya akan membuktikan bagian "**hanya jika**" dari pernyataan ini, karena menggunakan teorema Sylow. Pertimbangkan grup simetris S_p untuk p prima. Karena $p \mid p!$ dan $p^2 \nmid p!$, kita mendapatkan bahwa p-subgrup Sylow adalah grup siklik dengan order p. Ada $(p-1)!$ banyak p-sikel di S_p, dan setiap p-subgrup Sylow memuat tepat $(p-1)$ sikel seperti itu, sementara tidak ada yang berbagi. Oleh karena itu, ada tepatnya $(p-2)!$ p-subgrup Sylow yang berbeda. Dengan teorema Sylow ketiga, kita memiliki $n_p = (p-2)! \equiv 1 \mod p$, sehingga menyiratkan bahwa $(p-1)! \equiv p-1 \mod p \equiv -1 \mod p$. ✓

Teorema 5.13.2 Setiap grup berorder 15 adalah siklik.

Bukti
Misalkan G adalah grup dengan order 15. Misalkan n_3 dan n_5 masing-masing adalah banyaknya 3-subgrup Sylow dan 5-subgrup Sylow. Maka, dengan Teorema 5.12.4 Sylow III kita mempunyai

$$n_3 \text{ membagi } \frac{|G|}{3} = 5 \quad \text{dan} \quad n_3 = 3m+1,\ m \geq 0$$
$$n_5 \text{ membagi } \frac{|G|}{5} = 3 \quad \text{dan} \quad n_5 = 3n+1,\ n \geq 0.$$

Ini menyiratkan bahwa $n_3 = 1 = n_5$. Oleh karena itu, ada subgrup tunggal A yang berorder 3 di G (perhatikan bahwa 3^1 adalah pangkat terbesar dari 3 membagi $|G|$ dan 5^1 adalah pangkat terbesar 5 membagi $|G|$) dan karenanya A adalah normal. Demikian pula, ada subgrup normal B berorder 5 di G. Karena $|A|$ dan $|B|$ relatif prima, kita mendapatkan $A \cap B = \{e\}$. Dari ini, kita memiliki

$$|AB| = \frac{|A|\,|B|}{|A \cap B|} = |A|\,|B| = 3 \times 5 = 15 = |G|.$$

dan karenanya $AB = G$. Setiap elemen G dapat dinyatakan secara tunggal sebagai ab dengan $a \in A$ dan $b \in B$ (sebab $a_1b_1 = a_2b_2 \Rightarrow a_2^{-1}a_1 = b_2b_1^{-1} \in A \cap B = \{e\} \Rightarrow a_1 = a_2$ dan $b_1 = b_2$). Juga, untuk sebarang $a \in A$ dan $b \in B$, $a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in A \cap B = \{e\}$ dan karenanya $aba^{-1}b^{-1} = e$ atau $ab = ba$. Dari hal ini, dapat diverifikasi bahwa $(a,b) \mapsto ab$ adalah isomorpisma dari $A \times B$ ke G. Selanjutnya, $A \cong \mathbb{Z}_3$ dan $B \cong \mathbb{Z}_5$ (dengan menggunakan Lemma 5.13.1),

$$\therefore G \cong A \times B \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}.$$

Jadi G adalah siklik. ✓

Hasil di atas diperluas ke semua grup order pq, dimana p dan q adalah bilangan prima, $p > q$ dan q tidak membagi $p-1$. Pada hasil di atas, kita memiliki $15 = 5 \times 3$ dan 3 tidak membagi $4 = 5-1$.

Teorema 5.13.3 Misalkan G adalah grup order pq, dimana p dan q adalah bilangan prima yang berbeda, $p > q$ dan q tidak membagi $p-1$. Maka G adalah siklik.

Bukti

Misalkan n_p dan n_q masing-masing adalah banyaknya p-subgrup dan banyaknya q-subgrup Sylow. Maka, dengan Teorema 5.12.4 Sylow III kita mempunyai

$$n_p = mp + 1,\ m \geq 0 \ \text{ dan } \ n_q = nq + 1,\ n \geq 0,$$

n_p membagi q dan n_q membagi p. Karena $p > q$ dan $n_p = mp + 1,\ m \geq 0$, maka $n_p = 1$ dan karenanya ada Sylow p-subgroup A yang tunggal di G dan ini A harus merupakan subgrup normal berorder p. Juga, karena n_q membagi p dan p adalah bilangan prima, maka $n_q = 1$ atau p; tetapi $nq + 1 = n_q \neq p$ (jika tidak, yaitu $nq + 1 = p$ hal ini berarti q membagi $p - 1$, yang merupakan kontradiksi dengan hipotesis). Oleh karena itu, $n_q = 1$ maka G memiliki tunggal q-subgrup Sylow B, yang merupakan subgrup normal berorder q dalam G. Seperti pembahasan sebelumnya, kita mendapatkan bahwa $A \cap B = \{e\}$ dan $AB = G$. Oleh karena itu, kita mempunyai

$$G \cong A \times B \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

Jadi G adalah siklik. ✓

Teorema 5.13.4 Buktikan bahwa tidak ada grup sederhana (simpel) dengan order 63.

Bukti
Misalkan G adalah suatu grup berorder $63 = 3^2 \times 7$. Misalkan n_7 adalah banyaknya 7-subgrup Sylow di G. Maka, $n_7 = 7m + 1,\ m \geq 0$ dan n_7 membagi 63. Dari keduanya, kita dapat menyimpulkan bahwa $m = 0$ dan $n_7 = 1$. Oleh karena itu, ada tunggal 7-subgrup Sylow H dari G. Maka, H adalah subgrup normal berorder 7 di G dan karenanya $H \neq \{e\}$ dan $H \neq G$. Jadi, G tidak sederhana. ✓

Contoh 5.13.1 Misalkan S adalah p-subgrup Sylow dari grup berhingga G. Maka buktikan bahwa $N_G(N_G(S)) = N_G(S)$, dimana $N_G(S)$ adalah normalizer dari S dalam G.

Jawab
Kita mempunyai $N_G(S) = \{a \in G \mid aSa^{-1} = S\}$ dan

$$N_G(N_G(S)) = \{a \in G \mid aN_G(S)a^{-1} = N_G(S)\}$$

Untuk mempermudah, misalkan $N = N_G(S)$. Pertama perhatikan bahwa setiap konjugat dari S adalah p-subgrup Sylow dari G. Juga, jika H adalah subgrup dari G sedemikian hingga $aSa^{-1} \subseteq H$, maka aSa^{-1} adalah p-subgrup Sylow dari H. Jelas S adalah p-subgrup Sylow dari $N_G(S) = N$. Selanjutnya, jika T adalah p-subgroup Sylow dari N, maka $T = aSa^{-1}$ untuk beberapa $a \in N$ dan karenanya $T = S$. Oleh karena itu, S adalah satu-satunya p-subgrup Sylow dari N. Sekarang, pertimbangkan

$$\begin{aligned} a \in N_G(N) &\Rightarrow aNa^{-1} = N \\ &\Rightarrow aSa^{-1} \subseteq aNa^{-1} = N \\ &\Rightarrow aSa^{-1} = S \\ &\Rightarrow a \in N_G(S) = N. \end{aligned}$$

Jadi, $N_G(N) \subseteq N$. Karena N selalu termuat dalam $N_G(N)$, maka $N_G(N) = N$. ●

Latihan

1. Nyatakan apakah setiap pernyataan berikut ini **benar** atau **salah** dan **buktikan** jawaban saudara:

   (i) Untuk p prima dan untuk grup berhingga G, ada p-subgrup Sylow dari G.

   (ii) Order 3-subgrup Sylow dari grup berorder 108 adalah 27.

   (iii) Setiap 3-subgrup Sylow dari grup berorder 54 adalah normal.

   (iv) Terdapat suatu subgrup berorder 16 dalam grup berorder 216.

   (v) Setiap grup beroder 159 adalah sederhana.

   (vi) Setiap grup beroder 159 adalah siklik.

   (vii) Suatu grup dengan order pangkat prima tidak memiliki p-subgroups Sylow.

   (viii) Setiap p-subgrup dari grup berhingga adalah suatu p-subgrup Sylow.

   (ix) Setiap grup berorder 121 adalah Abelian.

   (x) Setiap grup berorder 8 adalah Abelian.

2. Tentukan semua p-subgroup Sylow dari grup-grup berikut untuk semua bilangan prima p.

   (i) Grup $\mathbb{Z}_{24}$, himpunan bilangan bulat modulo 24.

   (ii) S_3, grup simetris dengan derajat 3.

   (iii) S_4, grup simetris dengan derajat 4.

   (iv) A_3, grup *alternating* dengan derajat 4.

   (v) Grup $\mathbb{Z}_3 \times \mathbb{Z}_3$.

3. Buktikan bahwa setiap grup berorder 45 memiliki subgrup normal berorder 9.

4. Buktikan bahwa tidak ada grup sederhana berorder 56.

5. Tunjukkan bahwa suatu p-subgrup normal dari grup berhingga termuat di setiap p-subgrup Sylow.

6. Untuk sembarang p prima tetap, buktikan bahwa irisan semua p-subgrup Sylow dari grup suatu G adalah subgrup normal dari G.

7. Buktikan bahwa tidak ada grup sederhana dengan order 255.

8. Jika p adalah bilangan prima dan r dan n adalah bilangan bulat positif sehingga $n < p$, maka buktikan bahwa tidak ada grup sederhana dengan order $p^r n$.

9. Misalkan G adalah suatu grup dengan order p^n, dimana p adalah bilangan prima dan $n \in \mathbb{Z}^+$. Buktikan bahwa ada subgrup normal A_i untuk $0 \leq i \leq n$ sedemikian hingga $|A_i| = p^i$ dan $A_i \subset A_{i+1}$ untuk semua $0 \leq i \leq n$.

10. Simpulkan dari 9 bahwa tidak ada grup sederhana berorder p^n, untuk sebarang p prima dan $n \geq 2$.

11. Buktikan bahwa tidak ada grup berorder 30 atau 36 atau 48 yang sederhana.
12. Tunjukkan bahwa sembarang grup dengan order 225 adalah siklik.
13. Buktikan bahwa ada tepat satu, hingga isomorpisma, grup berorder 323.
14. Buktikan bahwa setiap grup berorder 899 atau 961 adalah siklik.
15. Buktikan bahwa tidak ada grup berorder 160 yang sederhana.
16. Buktikan berikut ini dalam grup simetris S_n derajat n.
    (i) Jika $a = (i_1 i_2 \dots i_r)$ adalah r-sikel, maka $faf^{-1} = (f(i_1)f(i_2)\dots f(i_r))$, yang lagi-lagi merupakan r-sikel.
    (ii) Setiap dua sikel dengan panjang yang sama adalah konjugasi satu sama lainnya.
    (iii) Dua permutasi f dan g dalam S_n saling konjugasi jika dan hanya jika $f = a_1 a_2 \cdots a_k$ dan $g = b_1 b_2 \cdots b_k$, dimana a_i dan b_i adalah sikel saling-asing sedemikian rupa sehingga $|a_i| = |b_i|$ untuk semua $1 \leq i \leq k$.
    (iv) Barisan berhingga $0 < r_1 \leq r_2 \leq \dots \leq r_k$ dari bilangan bulat positif dikatakan sebagai partisi dari n jika $r_1 + r_2 + \cdots + r_k = n$. Maka, banyaknya kelas konjugasi dalam S_n sama dengan banyaknya partisi n.
17. Tentukan semua kelas konjugasi di S_4 dan tuliskan persamaan kelas S_4.
18. Buktikan bahwa senter dari S_n adalah trivial untuk setiap $n > 2$.
19. Misalkan G adalah grup berorder 341. Buktikan bahwa setiap subgrup berorder 31 adalah subgrup normal dalam G.
20. Misalkan p adalah prima dan N adalah suatu subgrup normal dari grup G. Buktikan bahwa G adalah p-grup jika dan hanya jika N dan G/N keduanya adalah p-grup.
21. Misalkan N adalah suatu subgrup normal berprder p dalam p-grup G, dimana p prima. Maka buktikan bahwa N termuat di senter G.
22. Misalkan p adalah prima dan $n \in \mathbb{Z}^+$ sedemikian hingga $p > n$. Buktikan bahwa setiap subgrup berorder p dalam grup G dengan order p^n adalah subgrup normal dalam G.
23. Jika suatu grup G memuat subgrup sejati dengan indeks berhingga, maka buktikan bahwa G memuat subgrup normal sejati dengan indeks berhingga.
24. Berikan contoh 7-grup dengan order tak berhingga.

Bagian II

Ring dan Lapangan

Bab 6

Ring

Sebagai ide penggunaan dua operasi dalam model sistem bilangan yang telah akrab dilakukan. Maka kajian dalam bab ini dimulai melihat strukur aljabar dengan lebih dari satu operasi. Beberapa sifat penting diidentifikasi berkaitan dengan dua operasi yang akan dibahas ini untuk memberikan pemahaman yang lebih baik dari struktur aljabar yang berbeda dari apa yang telah dibahas dalam beberapa bab yang terdahulu. Bahasan mencakup konsep ring, daerah integral dan lapangan, yang diperkenalkan langkah demi langkah dalam bab ini. Bahasan bab ini membentuk dasar untuk teori aljabar yang dibahas dalam bab berikutnya.

6.1 Contoh-contoh dan Konsep Dasar

Dalam kajian ini yang telah dibahas sebelumnya dibatasi pada suatu himpunan yang takkosong dengan satu operasi yang memeuhi: tertutup, assosiatif, keberadaan elemen netral dan keberadaan elemen invers untuk setiap elemen. Sistem bilangan yang telah dibahas adalah himpunan $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, dan $\mathbb{Z}_n$ adalah grup dengan satu operasi "tambah". Selain itu, himpunan tersebut akan dilengkapi lagi dengan satu operasi yang lain yaitu "perkalian". Selanjutnya diidentifikasi beberapa sifat penting dari operasi "perkalian" ini serta hubungan antara kedua operasi tersebut. Pembahasan dimulai dari himpunan bilangan bulat $\mathbb{Z}$.

Contoh 6.1.1 Dibahas beberapa sifat penting himpunan bilangan bulat $\mathbb{Z}$ terhadap operasi "tambah" dan "perkalian" sebagaimana telah biasa dilakukan memenuhi:

(1) $\mathbb{Z}$ adalah suatu grup komutatif terhadap operasi "tambah".

(2) Diberikan sebarang $a, b \in \mathbb{Z}$, maka perkalian $ab \in \mathbb{Z}$.

(3) Diberikan sebarang $a, b, c \in \mathbb{Z}$, maka perkalian $a(bc) = (ab)c$, dengan kata lain dalam $\mathbb{Z}$ berlaku sifat assosiatif terhadap "perkalian".

(4) Diberikan sebarang $a, b, c \in \mathbb{Z}$, maka $a(b + c) = ab + ac$ dan $(a + b)c = ac + bc$ dengan kata lain dalam $\mathbb{Z}$ berlaku sifat distributif terhadap "perkalian"dan "tambah". ●

Selanjutnya, pembahasan dikonsentrasikan pada himpunan dengan dua operasi yang mempunyai empat sifat sebagaimana diberikan dalam Contoh 6.1.1.

Definisi 6.1.1 Suatu himpunan tak-kosong R dilengkapi dengan dua operasi "tambah" dan "perkalian" dinamakan suatu **ring** bila memenuhi empat **aksioma ring**, yaitu untuk setiap a, b dan c di R:

(1) R adalah suatu grup komutatif terhadap operasi "tambah".

(2) **Tertutup** terhadap perkalian, $ab \in R$.

(3) **Assosiatif** terhadap perkalian, $a(bc) = (ab)c$.

(4) **Distributif** terhadap "perkalian"dan "tambah", $a(b + c) = ab + ac$ dan $(a + b)c = ac + bc$.

Bila dalam ring R memenuhi sifat $ab = ba$ untuk semua $a, b \in R$, maka ring R dinamakan ring komutatif. Juga bila R memuat elemen $1 \in R$ yang memenuhi $1.a = a = a.1, \forall a \in R$, maka ring R dinamakan ring satuan.

Pembahasan dari ring R, elemen 0 di R adalah selalu menyatakan elemen netral dari R terhadap operasi biner + dan elemen invers dari $a \in R$ terhadap operasi tambah ditulis $-a$. Selanjutnya $n.a$ menyatakan $a + a + \ldots + a$ sebanyak n untuk n adalah bilangan bulat positip. Sedangkan bila n bilangan bulat negatip, maka $n.a$ menyatakan $(-a)+(-a)+\ldots+(-a)$ sebanyak $|n|$.

Contoh 6.1.2 Himpunan $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ dan $\mathbb{C}$ adalah ring terhadap operasi "tambah" dan "perkalian" sebagaimana telah biasa dilakukan adalah ring komutatif.

Contoh 6.1.3 Himpunan bilangan bulat modulo n yaitu $\mathbb{Z}_n$ adalah ring komutatif terhadap operasi "tambah" dan "perkalian" sebagaimana telah didefinisikan operasi tambah dan perkalian dalam modulo n.

Contoh 6.1.4 Misalkan ring R adalah himpunan $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ atau $\mathbb{C}$. Maka himpunan semua matriks berukuran 2×2 dengan elemen-elemen di R yaitu $M(2, R)$ adalah suatu ring terhadap operasi tambah dan perkalian matriks sebagaimana telah dikenal operasi tambah dan perkalian dalam matriks.

Contoh 6.1.5 Diberikan himpunan semua fungsi pada $\mathbb{R}$,

$$F(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\},$$

dengan operasi "tambah" dan "perkalian" fungsi untuk $f, g \in F(\mathbb{R})$ didefinisikan oleh

1. $(f + g) \stackrel{\text{def}}{=} f(x) + g(x)$ untuk semua $x \in \mathbb{R}$,
2. $(f.g)(x) \stackrel{\text{def}}{=} f(x).g(x)$ untuk semua $x \in \mathbb{R}$.

Himpunan $F(\mathbb{R})$ dengan operasi "tambah"adalah grup komutatif. Elemen netral di $F(\mathbb{R})$ adalah $e(x) = 0$, $\forall x \in \mathbb{R}$ dan invers dari $f \in F(\mathbb{R})$ adalah $-f$, dimana $-f(x) = -(f(x))$, $\forall x \in \mathbb{R}$. Sifat yang lain dari ring juga dipenuhi oleh $F(\mathbb{R})$.

Contoh 6.1.6 Diberikan ring $R_1, R_2, \ldots, R_n$ adalah ring. Produk ring

$$R = R_1 \times R_2 \times \ldots \times R_n,$$

dengan operasi "tambah" dan "perkalian" dalam R untuk $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in R$ didefinisikan oleh

1. $(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) \stackrel{\text{def}}{=} (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$,
2. $(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) \stackrel{\text{def}}{=} (a_1 b_1, a_2 b_2, \ldots, a_n b_n)$.

Maka R memenuhi semua kriteria ring. ●

Contoh 6.1.7 Himpunan

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

terhadap operasi biner "tambah" dan "perkalian" sebagaimana dilakukan seperti biasanya adalah ring komutatif. Perhatikan bahwa lapangan $\mathbb{Q}(\sqrt{2})$ adalah **lapangan terkecil** yang memuat $\alpha = \sqrt{2}$ dan $\mathbb{Q}$. ●

Berikut ini diberikan sifat-sifat dasar dari suatu ring.

Teorema 6.1.1 Bila R suatu **ring satuan** (memuat elemen satu, $1_R \in R$), maka untuk semua $a, b \in R$:

(1) $a.0 = 0.a = 0$

(2) $a.(-b) = (-a).b = -(a.b)$

(3) $(-a).(-b) = a.b$

(4) $(-1_R).a = -a$

(5) $(-1_R).(-1_R) = 1_R$.

(6) $(m.a).(n.b) = mn.(ab)$ untuk semua bilangan bulat m dan n.

Bukti

(1) Gunakan distributif, $a.0 = a.(0 + 0) = a.0 + a.0$. Tambahkan dengan $-(a.0)$ kedua ruas, didapat $0 = a.0$. Dengan cara serupa didapat $0\ .a = 0$.

(2) Hitung $a.(-b) + a.b = a.(-b + b) = a.0 = 0$. Sehingga didapat $a.(-b) = -(a.b)$.

(3) Dipunyai bahwa $(-a).(-b) = -(a.(-b)) = -(-(a.b)) = a.b$.

(4) Dari (2), $(-1_R).a = -(1_R.a) = -a$.

(5) Gunakan (3), $(-1_R).(-1_R) = 1_R.1_R = 1_R$.

(6) Digunakan induksi dua kali. Bila $m = 0$ atau $n = 0$ tidak ada yang perlu dibuktikan. Misalkan $m = 1$, maka (6) dipenuhi untuk $n = 1$. Asumsikan (6) benar untuk $m = 1$ dan $n = k \geq 0$. Maka dengan menggunakan sifat distributif didapat

$$a[(k + 1).b] = a[k.b + b] = a.(k.b) + ab = k.(ab) + ab = (k + 1).ab,$$

terlihat bahwa (6) dipenuhi untuk $m = 1$ dan $n = k+1$. Hal ini menunjukkan bahwa (6) dipenuhi untuk $m = 1$ dan untuk semua $n \geq 0$. Bila $n < 0$, misalkan $r = -n$. Didapat

$$a[n.b] = a[(-r).b] = a[-(r.b)] = -[a(r.b)] = -r.(ab) = n.(ab).$$

Jadi (6) dipenuhi untuk $m = 1$ dan semua $n \in \mathbb{Z}$. Berikutnya, asumsikan (6) dipenuhi untuk $m = k \geq 0$ dan semua $n \in \mathbb{Z}$. Didapat

$$\begin{aligned}[(k+1).a](n.b) &= (k.a + a)(n.b) = (k.a)(n.b) + a(n.b) = km.(ab) + m.(ab) \\ &= (km + m).(ab) = [(k+1)m].(ab),\end{aligned}$$

terlihat bahwa (6) dipenuhi untuk $m = k + 1$ dan semua $n \in \mathbb{Z}$. Hal ini menunjukkan bahwa (6) dipenuhi oleh $m \geq 0$ dan semua $n \in \mathbb{Z}$. Selanjutnya, bila $m < 0$, misalkan $s = -m$ didapat

$$(m.a)(n.b) = (-s.a)(n.b) = -(s.a)(n.b) = -sn.(ab) = mn.(ab).$$

Lengkap sudah bukti (6).

Dalam pembahasan suatu grup G himpunan bagian tak-kosong dai G yaitu H adalah subgrup dari G bila H adalah grup terhadap operasi biner yang berlaku di G. Bila operasi biner dalam grup G adalah $+$, maka pernyataan H adalah subgrup dari G dapat diganti oleh $H \subset G$ adalah subgrup dari G bila dan hanya bila $a - b \in H$ untuk semua a dan b di H. Pemahaman ini secara intuisi bisa digunakan untuk menunjukkan bahwa himpunan bagian dari suatu ring adalah subring.

Definisi 6.1.2 Suatu himpunan bagian $S \neq \emptyset$ dari suatu ring R adalah suatu **subring** bila S adalah ring terhadap operasi yang berlaku dalam ring R.

Teorema 6.1.2 Suatu himpunan bagian $S \neq \emptyset$ dari suatu ring R adalah suatu subring bila dan hanya bila untuk semua $a, b \in S$ memenuhi

(1) $a - b \in S$

(2) $ab \in S$.

Bukti
($\Leftarrow$) Bila (1) dan (2) dipenuhi maka S adalah subgrup dari R terhadap operasi "tambah" dan subgrup komutatif, juga S tertutup terhadap operasi "perkalian". Sifat assosiatif terhadap "perkalian" dan distributif di S menurun dari ring R. Jadi S adalah subring dari ring R. ($\Rightarrow$) Bila S adalah subring dari R, maka S adalah subgrup dari R terhadap operasi "tambah" hal ini berakibat (1), yaitu $a - b \in S$ untuk semua $a, b \in S$. Sedangkan (2) dipenuhi dari aksiomatik ring yang tetutup terhadap "perkalian".

Contoh 6.1.8 Himpunan $2\mathbb{Z}$ terhadap operasi "tambah" dan "perkalian" sebagaimana biasa dilakukan dalam himpunan bilangan bulat adalah subring dari ring $\mathbb{Z}$. Hal ini bisa diselidiki sebagi berikut. Untuk $2\mathbb{Z} \subseteq \mathbb{Z}$ dan $a, b \in 2\mathbb{Z}$ didapat (1) $a - b \in 2\mathbb{Z}$ dan (2) $ab \in 2\mathbb{Z}$. Jadi $2\mathbb{Z}$ adalah subring dari $\mathbb{Z}$. Secara umum $n\mathbb{Z}$ untuk $n \geq 1$ adalah subring dari $\mathbb{Z}$.

Contoh 6.1.9 Himpunan $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}, i^2 = -1\}$ terhadap operasi "tambah" dan "perkalian" sebagaimana biasa dilakukan dalam himpunan bilangan kompleks adalah subring dari ring $\mathbb{C}$. Hal ini bisa diselidiki sebagi berikut. Untuk $\mathbb{Z}[i] \subseteq \mathbb{C}$ dan $x, y \in \mathbb{Z}[i]$, maka $x = a + bi$ dan $y = c + di$ untuk beberapa $a, b, c, d \in \mathbb{Z}$. Didapat

(1) $x - y = (a + bi) - (c + di) = (a - c) + (b - d)i \in \mathbb{Z}[i]$ (sebab $a - c, b - d \in \mathbb{Z}$)

(2) $xy = (a+bi)(c+di) = (ac-bd)+(ad+bc)i \in \mathbb{Z}[i]$ (sebab $ac-bd, ad+bc \in \mathbb{Z}$).

Jadi $\mathbb{Z}[i]$ adalah subring dari $\mathbb{C}$. Ring $\mathbb{Z}[i]$ dinamakan **ring Gaussian**. ●

Contoh 6.1.10 Himpunan $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ terhadap operasi "tambah" dan "perkalian" sebagaimana biasa dilakukan dalam himpunan bilangan riil adalah subring dari ring $\mathbb{R}$. Hal ini bisa diselidiki sebagi berikut. Untuk $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ dan $x, y \in \mathbb{Q}(\sqrt{2})$, maka $x = a + b\sqrt{2}$ dan $y = c + d\sqrt{2}$ untuk beberapa $a, b, c, d \in \mathbb{Q}$. Didapat

(1) $x - y = (a + b\sqrt{2}) - (c + d\sqrt{2}) = (a-c) + (b-d)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ (sebab $a - c, b - d \in \mathbb{Q}$)

(2) $xy = (a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ (sebab $ac+2bd, ad+bc \in \mathbb{Q}$).

Jadi $\mathbb{Q}(\sqrt{2})$ adalah subring dari $\mathbb{R}$. ●

Catatan bahwa Contoh 6.1.10 dapat diperumum ke $\mathbb{Q}(\sqrt{p})$ untuk p bilangan bulat positip prima, dengan cara ini diperoleh sejumlah tak-hingga banyak subring dari $\mathbb{R}$ yaitu $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{R}$. Untuk $\mathbb{Q}$ adalah suatu subring dari $\mathbb{Q}(\sqrt{p})$ dikarenakan untuk sebarang bilangan rasional a dapat ditulis sebagai $a = a + 0.\sqrt{p}$.

Contoh 6.1.11 Untuk sebarang bilangan kompleks u dan v, didefinisikan matriks berikut

$$h(u,v) \stackrel{\text{def}}{=} \begin{bmatrix} u & v \\ -\overline{v} & \overline{u} \end{bmatrix}$$

dan $\mathbb{H} = \{h(u,v) \mid u, v \in \mathbb{C}\}$. Dapat ditunjukkan bahwa $\mathbb{H}$ adalah subring dari $M(2,\mathbb{C})$. Himpunan $\mathbb{H}$ dinamakan ring **quaternion**. Bila $Q_8 = \{\pm 1, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\}$ sebagaimana diberikan dalam Contoh 2.1.21 dan $u = a + bi, v = c + di$ dimana $a, b, c, d \in \mathbb{R}$, maka $h(u,v)$ dapat diungkapkan sebagai

$$h(u,v) = a\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + b\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} + c\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} + d\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

atau $a1 + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$. Dengan kata lain, elemen-elemen di $\mathbb{H}$ adalah kombinasi linier dari elemen-elemen di Q_8 dengan koefisien riil. ●

Latihan

Latihan 6.1.1 Dalam latihan berikut ini selidiki himpunan berikut terhadap operasi yang diberikan apakah suatu ring.

1. $S = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}$, terhadap operasi "tambah" dan "perkalian" bilangan riil sebagaimana biasanya.
2. $S = \{a + bi \mid a, b \in \mathbb{Q}\}$, terhadap operasi "tambah" dan "perkalian" bilangan kompleks sebagaimana biasanya.
3. $S = \{\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \mid a, b \in \mathbb{R}\}$, terhadap operasi "tambah" dan "perkalian" matriks sebagaimana biasanya.

4. $S = \{\begin{bmatrix} a & b \\ -b & a \end{bmatrix} | a, b \in \mathbb{R}\}$, terhadap operasi "tambah" dan "perkalian" matriks sebagaimana biasanya.
5. $S = \{A \in M(2, \mathbb{R}) | \det(A) = 0\}$, terhadap operasi "tambah" dan "perkalian" matriks sebagaimana biasanya.
6. $S = \{m/n \in \mathbb{Q} | n \text{ ganjil}\}$, terhadap operasi "tambah" dan "perkalian" bilangan riil sebagaimana biasanya.
7. $S = \{ri | r \in \mathbb{R}, i = \sqrt{-1}\}$, terhadap operasi "tambah" dan "perkalian" bilangan kompleks sebagaimana biasanya.

Latihan 6.1.2 Tunjukkan bahwa himpunan $F(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R}\}$ adalah suatu ring terhadap operasi "tambah" dan "perkalian" fungsi sebagaimana didefinisikan dalam Contoh 6.1.5.

Latihan 6.1.3 Misalkan $R_1, R_2, \ldots, R_n$ adalah sebarang ring dan $S = R_1 \times R_2 \times \ldots \times R_n$ terhadap operasi "tambah" dan "perkalian" sebagaimana didefinisikan dalam Contoh 6.1.6. Maka tunjukkan bahwa

(a) S adalah suatu ring.

(b) S komutatif bila dan hanya bila R_i komutatif untuk semua i, $1 \leq i \leq n$.

(c) S adalah suatu ring dengan elemen satuan bila dan hanya R_i ring dengan elemen satuan untuk semua i, $1 \leq i \leq n$.

Latihan 6.1.4 Bila S dan T adalah subring dari ring R, tunjukkan bahwa $S \cap T$ adalah suatu subring dari R.

Latihan 6.1.5 Tentukan semua subring dari ring $\mathbb{Z}$.

Latihan 6.1.6 Misalkan R adalah suatu ring. **Senter** dari R didefinisikan oleh

$$Z(R) = \{x \in R | xy = yx \text{ untuk semua } y \in R\}.$$

Tunjukkan bahwa $Z(R)$ adalah suatu subring dari R.

Latihan 6.1.7 Dapatkan senter $Z(\mathbb{H})$, dimana $\mathbb{H}$ adalah ring quaternion.

Latihan 6.1.8 Berikan suatu contoh dari suatu ring R yang mana elemen-elemen a, b dan c di R dengan $a \neq 0$ memenuhi $ab = ac$ tetapi $b \neq c$.

Latihan 6.1.9 Misalkan R adalah suatu ring. Tunjukkan bahwa $(a + b)(a - b) = a^2 - b^2$ untuk semua $a, b \in R$ bila dan hanya bila R adalah suatu ring komutatif.

Latihan 6.1.10 Misalkan R adalah suatu ring. Tunjukkan bahwa $(a + b)^2 = a^2 + 2ab + b^2$ untuk semua $a, b \in R$ bila dan hanya bila R adalah suatu ring komutatif.

Latihan 6.1.11 Tunjukkan bahwa Teorema Binomial 1.3.3 dipenuhi untuk semua elemen x dan y di ring komutatif R.

Latihan 6.1.12 Suatu ring **Boolean** R adalah suatu ring yang memenuhi $a^2 = a$ untuk semua $a \in R$. Tunjukkan bahwa suatu ring Boolean adalah suatu ring komutatif dan $2a = 0$ untuk semua $a \in R$.

Latihan 6.1.13 Untuk sebarang himpunan X, misalkan $P(X) = \{A || A \subseteq X\}$. Untuk sebarang A dan B di $P(x)$ didefinisikan

$$A + B \stackrel{\text{def}}{=} \{x \,|\, x \in A \cup B, x \notin A \cap B\} \text{ dan } A.B = A \cap B.$$

Tunjukkan bahwa $P(X)$ adalah suatu ring dengan satuan dan juga $P(X)$ adalah suatu ring Boolean.

Latihan 6.1.14 Misalkan R adalah suatu ring dengan satuan 1_R dan $S = \{n.1_R \,|\, n \in \mathbb{Z}\}$. Tunjukkan bahwa S adalah suatu subring dari R. Kesimpulan semacam hal ini dalam beberapa ring bisa tidak benar

6.2 Daerah Integral

Dalam bagian ini diidentifikasi suatu sifat dari beberapa ring yang memainkan peranan penting dalam kajian berikutnya. Lagi, sebagai suatu inspirasi kajian adalah ring himpunan bilangan bulat $\mathbb{Z}$. Dalam sistem bilangan bila pada suatu perhitungan persamaan seperti $ab = ac$ dengan $a \neq 0$ secara langsung disimpulkan $b = c$. Kesimpulan semacam ini dalam beberapa ring bisa tidak benar.

Contoh 6.2.1 Himpunan $\mathbb{Z}_5$ dan $\mathbb{Z}_6$ adalah ring. Telah dikenal tabel operasi tambah dari kedua himpunan tersebut, terhadap operasi tambah membentuk grup komutatif. Selanjutnya dibuat tabel perkalian dari $\mathbb{Z}_5$ dan $\mathbb{Z}_6$ tetapi tanpa elemen nol.

Tabel Perkalian mod 5

.	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Tabel Perkalian mod 6

.	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[2]_6$	$[2]_6$	$[4]_6$	$[0]_6$	$[2]_6$	$[4]_6$
$[3]_6$	$[3]_6$	$[0]_6$	$[3]_6$	$[0]_6$	$[3]_6$
$[4]_6$	$[4]_6$	$[2]_6$	$[0]_6$	$[4]_6$	$[2]_6$
$[5]_6$	$[5]_6$	$[4]_6$	$[3]_6$	$[2]_6$	$[1]_6$

Ada beberapa perbedaan diantara dua tabel perkalian dalam $\mathbb{Z}_5 - \{[0]_5\}$ dan $\mathbb{Z}_6 - \{[0]_6\}$. Tabel perkalian dalam $\mathbb{Z}_5 - \{[0]_5\}$ elemen $[0]_5$ tidak ada dalam setiap baris. Sedangkan tabel perkalian dalam $\mathbb{Z}_6 - \{[0]_6\}$ elemen $[0]_6$ muncul dalam baris ke-2, ke-3 dan ke-4. Elemen $[0]_6$ muncul dari hasil perkalian $[2]_6[3]_6 = [3]_6[2]_6 = [3]_6[4]_6 = [4]_6[3]_6$. Perhatikan bahwa $[3]_6[2]_6 = [3]_6[4]_6$, walaupun $[3]_6 \neq [0]_6$ tetapi $[2]_6 \neq [4]_6$. Hal ini menjelaskan bahwa kedua ruas persamaan tidak bisa dilakukan pembagian oleh $[3]_6$ walaupun $[3]_6 \neq [0]_6$.

Definisi 6.2.1 Bila a dan b adalah dua elemen taknol dari suatu ring R yang memenuhi $ab = 0$, maka a dan b dinamakan **pembagi nol** dalam R.

Contoh 6.2.2 Dalam ring $\mathbb{Z}_6$ pembagi nol adalah $[2]_6, [3]_6$ dan $[4]_6$. Dalam ring $\mathbb{Z}_{12}$ pembagi nol adalah

$[2]_{12}$ sebab $[2]_{12}[6]_{12} = [0]_{12}$,

$[3]_{12}$ sebab $[3]_{12}[4]_{12} = [0]_{12}$,

$[4]_{12}$ sebab $[4]_{12}[3]_{12} = [0]_{12}$,

$[6]_{12}$ sebab $[6]_{12}[2]_{12} = [0]_{12}$,

$[8]_{12}$ sebab $[8]_{12}[3]_{12} = [0]_{12}$,

$[9]_{12}$ sebab $[9]_{12}[4]_{12} = [0]_{12}$,

$[10]_{12}$ sebab $[10]_{12}[8]_{12} = [0]_{12}$.

Perhatikan bahwa semua elemen pembagi nol dalam $\mathbb{Z}_{12}$ adalah elemen yang tidak relatif prima dengan 12. Hal ini bukan sebagai suatu kebetulan dan ditunjukkan dalam sifat berikut. ●

Teorema 6.2.1 Suatu elemen taknol $[r]_n \in \mathbb{Z}_n$ adalah suatu pembagi nol bila dan hanya bila r dan n tidak relatif prima.

Bukti ($\Rightarrow$) Misalkan $[r]_n \in \mathbb{Z}_n$, $[r]_n \neq [0]_n$ dan untuk beberapa $[m]_n \in \mathbb{Z}_n$, $[m]_n \neq [0]_n$ memenuhi $[r]_n[m]_n = [0]_n$. Karena $[m]_n \neq [0]_n$, maka n tidak membagi m dan menggunakan Proposisi 1.3.2 bagian (2) didapat bahwa r dan n tidak relatif prima.
($\Leftarrow$) Misalkan r dan n tidak relatif prima. Maka $\text{fpb}(r, n) = d > 1$ dan $n/d < n$. Didapat $[r]_n[n/d]_n = [r/d]_n[n]_n = [0]_n$. Jadi $[r]_n$ adalah suatu pembagi nol dalam $\mathbb{Z}_n$. ✓

Akibat 6.2.1 Ring $\mathbb{Z}_p$ tidak mempunyai pembagi nol bila dan hanya bila p adalah prima.

Bukti Langsung dari Teorema 6.2.1. ✓

Contoh 6.2.3 Ring $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ dan $\mathbb{Z}_p$ dimana p prima adalah ring tanpa elemem pembagi nol. ●

Hukum **kanselasi** perkalian dipenuhi dalam suatu ring R bila untuk semua a, b dan c di R dengan $a \neq 0_R$, $ab = ac$ berakibat $b = c$ dan $ba = ca$ berakibat $b = c$. Akan terlihat bahwa ring yang memenuhi hukum kanselasi terhadap perkalian secara tepatnya adalah ring yang tidak mempunyai pembagi nol.

Teorema 6.2.2 Dalam suatu ring R memenuhi hukum kanselasi bila dan hanya bila R tidak mempunyai elemen pembagi nol.

Bukti ($\Rightarrow$) Misalkan hukum kanselasi dipenuhi dalam suatu ring R dan untuk beberapa $a, b \in R$, $a \neq 0_R$ dipunyai $ab = 0_R$. Ditunjukkan bahwa hal tersebut dapat terjadi hanya bila

$b = 0_R$. Karena $ab = 0_R$ dan $a.0 = 0_R$, gunakan hukum kanselasi didapat $b = 0_R$. Jadi R tidak mempunyai pembagi nol.
($\Leftarrow$) Misalkan R tidak mempunyai pembagi nol dan untuk beberapa $a, b, c \in R$, $a \neq 0_R$ dipunyai $ab = ac$. Maka $a(b-c) = ab - ac = 0_R$. Karena a bukan pembagi nol, haruslah $b - c = 0_R$ atau $b = c$. Dengan cara yang sama $ba = ca$ berakibat $b = c$.

Definisi 6.2.2 Suatu ring R dinamakan suatu **daerah integral** bila

(1) R komutatif,

(2) R mempunyai elemen satuan, $1_R \in R$,

(3) R tidak mempunyai pembagi nol.

Contoh 6.2.4 Ring $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ dan $\mathbb{Z}_p$ dimana p prima adalah daerah integral.

Definisi 6.2.3 Suatu himpunan takkosong S dari suatu daerah intgral D dinamakan **sub-daerah** (subdomain) dari D bila S terhadap operasi yang sama sebagai mana dalam D adalah suatu daerah integral.

Proposisi 6.2.1 Suatu himpunan bagian takkosong S dari suatu daerah integral D adalah suatu sub-daerah dari D bila dan hanya bila

(1) S adalah subring dari D.

(2) $1_D \in S$ dimana 1_D adalah elemen satuan di D.

Bukti
($\Leftarrow$) Misalkan (1) dan (2) dipenuhi, maka S adalah subring dari D dan $1_D \in S$. Diberikan sebarang $a \neq 0_D$, b dan c di S yang memenuhi $ab = ac$. Maka $a = m.1_D, b = r.1_D$ dan $c = s.1_D$ untuk beberapa $m \neq 0, r$ dan s di $\mathbb{Z}$. Didapat

$$0_D = ab - ac = a(b-c) = m.1_D[(r.1_D) - (s.1_D)] = m.1_D(r-s).1_D = m(r-s).1_D.$$

Jadi $m(r-s) = 0$ di $\mathbb{Z}$, hal ini berakibat $r = s$ atau $r.1_D = s.1_D$. Dengan demikian $b = c$. Dengan cara yang sama dpat ditunjukkan $ba = ca$, maka $b = c$. Hal ini menunjukkan dalam S berlaku hukum kanselasi. Akibatnya S tidak memuat pembagi nol. Jadi S adalah subdaerah.
($\Rightarrow$) Misalkan S adalah subdaerah dari suatu daerah integral D, maka S adalah subring komutatif dari D dan $1_D \in S$.

Contoh 6.2.5 Himpunan $\mathbb{Z}[i]$ adalah suatu daerah integral, sebab $\mathbb{Z}[i]$ adalah subring dari $\mathbb{C}$ dan $1 = 1 + 0\,i \in \mathbb{Z}[i]$.

Contoh 6.2.6 Himpunan $\mathbb{Q}(\sqrt{2})$ adalah suatu daerah integral, sebab $\mathbb{Q}(\sqrt{2})$ adalah subring dari $\mathbb{R}$ dan $1 = 1 + 0\,\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Contoh 6.2.7 Ring $M(2, \mathbb{R})$ bukan suatu daerah integral. Sebab $M(2, \mathbb{R})$ mempunyai pembagi nol, contohnya

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Juga, $M(2, \mathbb{R})$ bukan ring komutatif.

Contoh 6.2.8 Ring $\mathbb{Z}\times\mathbb{Z}$ bukan suatu daerah integral, sebab $(2,0).(0,3) = (0,0)$. Secara lebih umum untuk sebarang dua ring tak-trivial R_1 dan R_2, maka ring $R_1 \times R_2$ bukan suatu daerah integral. Sebab semua bentuk $(r_1, 0)$ dan $(0, r_2)$ dengan $r_1 \neq 0$ dan $r_2 \neq 0$ adalah elemen pembagi nol dalam $R_1 \times R_2$.

Contoh 6.2.9 Sifat lain dari daerah integral $\mathbb{Z}$ yaitu persamaan $a^2 = a$ mempunyai tepat dua penyelesaian $a = 0$ atau $a = 1$. Beda dalam $\mathbb{Z}_6$ yang mana telah diketahui bahwa bukan daerah integral. Maka $a = 3$ juga penyelesaian dari $a^2 = a$. Dalam suatu daerah integral D, $a^2 = a$ berakibat $a(a-1) = a^2 - a = 0$ dan karena tidak memuat pembagi nol, maka hanyalah $a = 0$ atau $a = 1$ adalah penyelesaian dari $a^2 = a$ dalam D.

Latihan

Latihan 6.2.1 Dapatkan semua pembagi nol dari ring berikut.

1. $\mathbb{Z}_4$ 2. $\mathbb{Z}_8$ 3. $\mathbb{Z}_{11}$ 4. $\mathbb{Z}_2 \times \mathbb{Z}_2$
5. $\mathbb{Z}_4 \times \mathbb{Z}_6$ 6. $\mathbb{Z} \times \mathbb{Q}$ 7. $M(2, \mathbb{Z}_2)$.

Latihan 6.2.2 Buat suatu contoh dari suatu ring komutatif yang tidak memuat pembagi nol dan bukan suatu daerah integral.

Latihan 6.2.3 Buat suatu contoh dari suatu ring dengan elemen satuan yang tidak memuat pembagi nol dan bukan suatu daerah integral.

Latihan 6.2.4 Tunjukkan bahwa irisan dari dua subdaerah dari suatu daerah integral D adalah juga subdaerah dari D.

Latihan 6.2.5 Misalkan D adalah suatu daerah integral dan $S = \{n.1 \,|\, n\mathbb{Z}\}$ dengan 1 adalah elemen satuan di D. Tunjukkan bahwa

(a) S adalah subdaerah dari D.

(b) Bila R adalah sebarang subdaerah dari D, maka $S \subseteq R$.

Latihan 6.2.6 Tunjukkan bahwa ring berikut adalah daerah integral.

(a) $\mathbb{Q}(i) = \{a + bi \,|\, a, b \in \mathbb{Q}, i^2 = -1\}$.

(b) $\mathbb{Z}[\sqrt{5}] = \{a + b\sqrt{5} \,|\, a, b \in \mathbb{Z}\}$.

(c) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{2}\sqrt{3} \,|\, a, b, c.d \in \mathbb{Q}\}$.

Latihan 6.2.7 Dapatkan semua subdaerah dari $\mathbb{Z}$.

Latihan 6.2.8 Tunjukkan bahwa subdaerah dari $\mathbb{Z}_p$ dengan p adalah prima hanyalah $\mathbb{Z}_p$ sendiri.

Latihan 6.2.9 Tunjukkan bahwa hanyalah ring Bolean $\mathbb{Z}_2$ adalah suatu daerah integral.

Latihan 6.2.10 Misalkan R adalah suatu ring dengan setidaknya dua elemen yang memenuhi untuk setiap elemen taknol $a \in R$ ada dengan tunggal suatu elemen $b \in R$ sehingga $aba = a$. Tunjukkan bahwa

(a) R tidak mempunyai pembagi nol.

(b) $bab = b$.

(c) R mempunyai elemen satuan.

Latihan 6.2.11 Diberikan ring $\mathbb{Z}_7$.

(a) Tunjukkan bahwa $\mathbb{Z}_7$ adalah suatu ring yang memenuhi kriteria dalam Latihan 6.2.10.

(b) Untuk sebarang elemen taknol $a \in \mathbb{Z}_7$ dapatkan elemen terkait $b \in \mathbb{Z}_7$ yang memenuhi $aba = a$.

6.3 Lapangan

Dalam bagian sebelumnya telah dikenalkan pengertian suatu daerah integral, yaitu suatu ring komutatif mempunyai elemen satuan dan tidak memuat pembagi nol. Dalam suatu daerah integral hukum kanselasi dipenuhi, sebagaimana telah ditunjukkan dengan menyatakan bahwa jika $ab = ac$, $a \neq 0$, maka $a(b-c) = ab - bc = 0$ dan juga karena tidak ada pembagi nol, haruslah $b - c = 0$ dan $b = c$. Dalam hal ini tidak dilakukan pembagian dengan a pada kedua ruas persamaan. Sebab tidak diketahui apakah a mempunyai invers terhadap perkalian.

Contoh 6.3.1 Dalam $\mathbb{Z}$ hanyalah elemen 1 dan -1 yang mempunyai invers terhadap perkalian, sebab $1.1 = 1$ dan $(-1).(-1) = 1$.

Contoh 6.3.2 Dalam ring himpunan $\mathbb{Z}_5$ didapat

$$[1]_5.[1]_5 = [1]_5, \quad [2]_5.[3]_5 = [1]_5, \quad [3]_5.[2]_5 = [1]_5, \quad [4]_5.[4]_5 = [1]_5.$$

Terlihat bahwa dalam ring $\mathbb{Z}_5$ semua elemen yang taknol mempunyai invers di $\mathbb{Z}_5$ terhadap operasi perkalian.

Definisi 6.3.1 Dalam suatu ring R dengan elemen satuan 1, suatu elemen $a \in R$ dinamakan suatu **unit** bila a mempunyai invers terhadap perkalian.

Sebagaimana telah dibahas dalam Grup, bila a mempunyai invers a^{-1}, maka invers tersebut tunggal.

Contoh 6.3.3 Dalam ring $\mathbb{Z}_{12}$ elemen-elemen unit adalah, $[1]_{12}, [5]_{12}, [7]_{12}$ dan $[11]_{12}$ sebab

$$[1]_{12}.[1]_{12} = [3]_{12}.[3]_{12} = [5]_{12}.[5]_{12} = [7]_{12}.[7]_{12} = [11]_{12}.[11]_{12} = [1]_{12}.$$

Perlu diperhatikan bahwa elemen unit dalam $\mathbb{Z}_{12}$ adalah elemen taknol yang merupakan bukan pembagi nol. Juga himpunan unit dari $\mathbb{Z}_{12}$ terhadap perkalian adalah $\mathbb{U}(12)$ merupakan grup. Pembahasan dalam contoh ini secara umum diberikan dalam dua teorema berikut.

Teorema 6.3.1 Dalam suatu ring R dengan elemen satuan 1, bila suatu elemen $a \in R$ adalah suatu unit, maka a bukan suatu pembagi nol.

Bukti Misalkan $a \in R$ adalah suatu unit dalam R, jadi a^{-1} ada dalam R. Bila untuk beberapa $b \in R$ memenuhi $ab = 0$, maka $b = 1.b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}.0 = 0$. Dengan demikian a bukan suatu pembagi nol.

Teorema 6.3.2 Misalkan R adalah suatu ring komutatif yang mempunyai elemen satuan 1, dan

$$\mathbb{U}(R) = \{a \in R \mid a \text{ adalah suatu unit di } R\}.$$

Maka $\mathbb{U}(R)$ adalah suatu grup terhadap operasi perkalian di R.

Bukti Ditunjukkan $\mathbb{U}(R)$ memenuhi empat aksioma grup.
(**Tertutup**) Misalkan $a, b \in \mathbb{U}(R)$, maka a^{-1} dan b^{-1} di $\mathbb{U}(R)$. Dengan demikian $b^{-1}a^{-1} \in R$, didapat

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1,$$

dan

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b^{-1} = b^{-1}b = 1.$$

Terlihat bahwa $b^{-1}a^{-1}$ invers dari ab terhadap perkalian, jadi $ab \in \mathbb{U}(R)$.
(**Assosiatif**) Operasi perkalian dalam $\mathbb{U}(R)$ juga merupakan operasi perkalian dalam R. Karena R ring, maka memenuhi sifat assosiatif.
(**Identitas**) $1.1 = 1$, jadi 1 mempunyai invers dirinya sendiri terhadap operasi perkalian. Elemen 1 adalah suatu unit dan $1 \in \mathbb{U}(R)$.
(**Invers**) Bila $a \in \mathbb{U}(R)$, maka a mempunyai invers terhadap perkalian a^{-1} di R. Tetapi a adalah invers dari a^{-1} terhadap perkalian. Jadi a^{-1} mempunyai invers terhadap perkalian dan $a^{-1} \in \mathbb{U}(R)$.

Teorema 6.3.3 Dalam ring $\mathbb{Z}_n$ grup perkalian dari unit adalah $\mathbb{U}(\mathbb{Z}_n) = \mathbb{U}(n)$.

Bukti Bila $[a]_n \in \mathbb{U}(\mathbb{Z})$ atau dengan kata lain $[a]_n$ adalah suatu unit di $\mathbb{Z}_n$, maka $[a]_n \neq [0]_n$ dan menurut Teorema 6.3.1 $[a]_n$ bukan pembagi nol di $\mathbb{Z}_n$. Dengan demikian menurut Teorema 6.2.1 a dan n adalah relatif prima, jadi $[a]_n \in \mathbb{U}(n)$, maka $\mathbb{U}(\mathbb{Z}_n) \subseteq \mathbb{U}(n)$. Bila $[a]_n \in \mathbb{U}(n)$ dan karena $\mathbb{U}(n)$ adalah grup terhadap operasi perkalian (sebagaimana telah dibahas dalam bagian grup), maka $([a]_n)^{-1}$ adalah invers dari $[a]_n$ di $\mathbb{U}(n) \subseteq \mathbb{Z}_n$ jadi $[a]_n \in \mathbb{U}(\mathbb{Z}_n)$, maka $\mathbb{U}(n) \subseteq \mathbb{U}(\mathbb{Z}_n)$. Dengan demikian $\mathbb{U}(\mathbb{Z}_n) = \mathbb{U}(n)$.

Contoh 6.3.4 $\mathbb{U}(\mathbb{Z}_6) = \{[1]_6, [5]_6\} = \mathbb{U}(6)$ dan $\mathbb{U}(\mathbb{Z}_5) = \mathbb{Z}_5 - \{[0]_5\} = \mathbb{U}(5)$.

Contoh 6.3.5 Untuk himpunan bilangan bulat, $\mathbb{U}(\mathbb{Z}) = \{1, -1\}$ adalah grup terhadap perkalian. Untuk bilangan rasional, $\mathbb{U}(\mathbb{Q}) = \mathbb{Q}^*$ adalah himpunan semua bilangan rasional taknol terhadap perkalian adalah grup.

Contoh 6.3.6 Misalkan akan dihitung elemen unit dari $\mathbb{Z}_4 \times \mathbb{Z}_6$. Disini (a, b) unit di $\mathbb{Z}_4 \times \mathbb{Z}_6$ bila dan hanya bila ada suatu elemen $(c, d) \in \mathbb{Z}_4 \times \mathbb{Z}_6$ yang memenuhi

$$(a, b)(c, d) = (ac, bd) = ([1]_4, [1]_6).$$

Dengan kata lain a harus suatu unit di $\mathbb{Z}_4$ dan b juga harus suatu unit di $\mathbb{Z}_6$. Jadi

$$\mathbb{U}(\mathbb{Z}_4 \times \mathbb{Z}_6) = \{([1]_4, [1]_6), ([1]_4, [5]_6), ([3]_4, [1]_6), ([3]_4, [5]_6)\} = \mathbb{U}(\mathbb{Z}_4) \times \mathbb{U}(\mathbb{Z}_6).$$

Berikut ini dibahas suatu definisi dari pengertian yang paling mendasar dalam teori ring.

Definisi 6.3.2 Suatu ring $\mathbb{F}$ dinamakan suatu lapangan bila

(1) Ring $\mathbb{F}$ adalah ring komutatif.

(2) Ring $\mathbb{F}$ mempunyai elemen satuan, $1 \in F$.

(3) Setiap elemen taknol di $\mathbb{F}$ adalah suatu unit. ✓

Perhatikan bahwa berdasarkan Teorema 6.3.2, kondisi (3) bisa diganti oleh

(3') Himpunan semua elemen tak nol di $\mathbb{F}$ adalah suatu grup komutatif terhadap operasi perkalian.

Kondisi (1) penting, bila kondisi (1) tidak dipenuhi maka ring $\mathbb{F}$ tidak bisa dikatakan sebagai suatu lapangan.

Contoh 6.3.7 Himpunan $\mathbb{Q}, \mathbb{R}$ dan $\mathbb{C}$ adalah lapangan dan $\mathbb{Z}$ adalah daerah integral yang bukan suatu lapangan. ●

Hubungan diantara daerah integral dan lapangan diberikan oleh teorema berikut.

Teorema 6.3.4 Setiap lapangan adalah suatu daerah integral.

Bukti Hal ini akibat langsung dari Definisi 6.2.3, Definisi 6.3.2 dan Teorema 6.3.1. Yaitu, misalkan dalam suatu lapangan $\mathbb{F}$, untuk sebarang $a, b \in F$ berlaku $ab = 0$. Bila $a \neq 0$, maka ada invers $a^{-1} \in \mathbb{F}$ dan didapat

$$b = 1.b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}.0 = 0.$$

Terlihat bahwa bila sebarang $a \neq 0$ di $\mathbb{F}$ dan $ab = 0$ berakibat bahwa $b = 0$. Jadi $a \in F$ bukan elemen pembagi nol. Oleh karena itu $\mathbb{F}$ tidak memuat pembagi nol. Jadi $\mathbb{F}$ adalah suatu daerah integral. ✓

Teorema 6.3.4 tidak berlaku sebalinya. Contohnya adalah himpunan bilangan bulat $\mathbb{Z}$ adalah suatu daerah integral tetapi bukan suatu lapangan. Teorema berikut memberikan syarat bahwa suatu daerah integral adalah suatu lapangan.

Teorema 6.3.5 Setiap daerah integral berhingga D dengan $|D| = n$ adalah suatu lapangan.

Bukti Misalkan D adalah suatu daerah integral berhingga dan sebarang $x \in D$ dengan $x \neq 0_D$ akan ditunjukkan bahwa x mempunyai invers terhadap perkalian. Dihimpun semua elemen taknol di D yaitu

$$D - \{0_D\} = \{1, x_1, x_2, \ldots, x_{n-1}\},$$

jadi $x \in D - \{0_D\}$. Karena D daerah integral dan $x \neq 0_D$ didapat himpunan

$$x(D - \{0_D\}) = \{x, xx_1, xx_2, \ldots, xx_{n-1}\}$$

yang semua elemennya taknol. Selanjutnya ditunjukkan bahwa himpunan $x(D - \{0\})$ sama dengan $D - \{0\}$ sebab bila $xx_i = xx_j$ untuk beberapa $1 \leq i, j \leq n - 1$. Maka $x(x_i - x_j) = 0_D$. Karena $x \neq 0_D$ dan D adalah Daerah integral, maka haruslah $x_i - x_j = 0_D$ sehingga didapat

$x_i = x_j$. Hal ini menunjukkan bahwa semua elemen di $x(D - \{0\})$ adalah berbeda dan karena $|D - \{0\}| = |x(D - \{x\})|$ dan D tertutup terhadap perkalian, maka $D - \{0\} = x(D - \{0\})$. Bila $x = 1$, maka $x^{-1} = 1$. Bila $x \neq 1$, maka haruslah $1 = xx_i$ untuk suatu $i, 1 \leq i \leq n-1$. Jadi $x^{-1} = x_i$ untuk suatu $i, 1 \leq i \leq n-1$. Dengan demikian sebarang $x \neq 0$ di D mempunyai invers di D. Jadi D adalah suatu lapangan.

Akibat 6.3.1 Himpunan $\mathbb{Z}_p$ adalah suatu lapangan bila dan hanya bila p adalah prima.

Bukti ($\Leftarrow$). Misalkan p prima dan dari Teorema 6.3.3 didapat $\mathbb{U}(\mathbb{Z}_p) = \mathbb{U}(p)$. Karena p prima, maka $\mathbb{U}(p) = \mathbb{Z}_p - \{[0]_p\}$. Jadi $\mathbb{Z}_p$ adalah daerah integral. Dengan menggunakan Teorema 6.3.5, maka $\mathbb{Z}_p$ adalah suatu lapangan.
($\Rightarrow$) Misalkan $\mathbb{Z}_p$ adalah suatu lapangan, maka $\mathbb{Z}_p$ tidak memuat pembagi nol. Dengan menggunakan Akibat 6.2.1 maka p adalah prima.

Definisi 6.3.3 Himpunan bagian takkosong S dari suatu lapangan $\mathbb{F}$ dinamakan **sub-lapangan** dari $\mathbb{F}$ bila S adalah suatu lapangan terhadap dua operasi yang sama seperti di $\mathbb{F}$.

Teorema 6.3.6 Suatu himpunan bagian takkosong S dari suatu lapangan $\mathbb{F}$ adalah suatu sub-lapangan terhadap dua operasi yang sama seperti di $\mathbb{F}$ bila dan hanya bila untuk semua $x, y \in S$ berlaku

(1) $x - y \in S$.

(2) Untuk $y \neq 0$, $xy^{-1} \in S$

Bukti ($\Rightarrow$) Misalkan S adalah sub-lapangan dari suatu lapangan $\mathbb{F}$, maka S terhadap operasi "tambah" adalah subgrup dari $\mathbb{F}$ dengan demikikian $x - y \in S$ untuk semua $x, y \in S$. Himpunan $S - \{0\}$ terhadap operasi "perkalian" adalah subgrup dari $\mathbb{F}$, maka $xy^{-1} \in S - \{0\}$ dan untuk $x = 0$ didapat $0.y^{-1} = 0 \in S$. jadi $xy^{-1} \in S$ untuk semua $x, y \in S$ dimana $y \neq 0$.
($\Leftarrow$) Misalkan $x - y \in S$ untuk semua $x, y \in S$, maka S adalah subgrup dari $\mathbb{F}$. Dan misalkan xy^{-1} untuk semua $x, y \in S$ dimana $y \neq 0$, maka $x, y^{-1} \in S - \{0\}$ untuk semua $x, y \in S - \{0\}$. Jadi $S - \{0\}$ terhadap operasi perkalian adalah subgrup dari $\mathbb{F}$. Elemen satuan $1 \neq 0$, jadi $1 = 1.1^{-1} \in S - \{0\} \subset S$. Himpunan S terhadap operasi perkalian adalah komutatif sebab $\mathbb{F}$ komutatif terhadap perkalian. Dengan demikian S adalah sub-lapangan dari $\mathbb{F}$.

Contoh 6.3.8 Dengan menggunakan Teorema 6.3.6 dapat ditunjukkan himpunan

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

terhadap dua operasi tambah dan perkalian sebagaimana dilakukan adalah sub-lapangan dari lapangan $\mathbb{R}$. Sudah ditunjukkan dalam Contoh 6.1.10 bahwa $\mathbb{Q}(\sqrt{2})$ adalah subring dari $\mathbb{R}$. Untuk menunjukkan bahwa $\mathbb{Q}(\sqrt{2})$ adalah sub-lapangan dari $\mathbb{R}$ cukup dibuktikan kondisi (2) dalam Toerema 6.3.6. Misalkan $x, y \in \mathbb{Q}(\sqrt{2})$ dimana $y \neq 0$. Maka

$$x = a + b\sqrt{2},\ y = c + d\sqrt{2} \text{ untuk beberapa } a, b, c, d \in \mathbb{Q}.$$

Didapat

$$\begin{aligned} xy^{-1} &= (a+b\sqrt{2})\frac{1}{c+d\sqrt{2}} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \left(\frac{a+b\sqrt{2}}{c+d\sqrt{2}}\right).\left(\frac{c-d\sqrt{2}}{c-d\sqrt{2}}\right) \\ &= \frac{(ac-2bd)+(bc-ad)\sqrt{2}}{c^2-2d^2} = \underbrace{\frac{ac-2bd}{c^2-2d^2}}_{\in\mathbb{Q}} + \underbrace{\frac{bc-ad}{c^2-2d^2}}_{\in\mathbb{Q}}\sqrt{2} \in \mathbb{Q}(\sqrt{2}). \end{aligned}$$

Catatan bahwa karena $c+d\sqrt{2} = y \neq 0$, maka $c^2-2d^2 \neq 0$. Sebab bila tidak demikian yaitu $c^2-2d^2 = 0$, maka berakibat bahwa $\sqrt{2} = \pm(c/d)$ adalah suatu hal yang tidak mungkin untuk $c, d \in \mathbb{Q}$. ●

Contoh 6.3.9 Sebegitu jauh contoh-contoh yang dibahas adalah lapangan takhingga $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ dan $\mathbb{Q}(\sqrt{2})$; dan lapangan berhingga seperti $\mathbb{Z}_p$ dengan banyaknya elemen adalah p dan p adalah bilangan bulat prima. Dalam contoh ini diberikan suatu lapangan dengan n elemen dimana n bukan suatu bilangan bulat prima. Diberikan himpunan

$$\mathbb{Z}_3[i] = \{a+bi \,|\, a, b \in \mathbb{Z}_3, i^2 = -1\}.$$

Karena a dan b adalah $[0]_3, [1]_3$ atau $[2]_3 = [-1]_3$, maka

$$\mathbb{Z}_3[i] = \{[0]_3, [1]_3, [2]_3, [1]_3 i, [1]_3 + [1]_3 i, [2]_3 + [2]_3 i, [2]_3 i, [1]_3 + [2]_3 i, [2]_3 + [2]_3 i\}.$$

Terlihat bahwa $n = |\mathbb{Z}_3[i]| = 9$. Operasi "+" dan "." dalam $\mathbb{Z}_3[i]$ didefinisikan sebagai berikut. Untuk $x, y \in \mathbb{Z}_3[i]$ dimana $x = [a]_3 + [b]_3 i$ dan $y = [c]_3 + [d]_3 i$,

$$x + y \stackrel{\text{def}}{=} ([a]_3 + [c]_3) + ([b]_3 + [d]_3)i \;\text{ dan }\; x.y \stackrel{\text{def}}{=} ([a]_3[c]_3 - [b]_3[d]_3) + ([a]_3[d]_3 + [b]_3[c]_3)i.$$

Dengan dua operasi tersebut $\mathbb{Z}_3[i]$ adalah suatu ring komutatif. Setiap elemen taknol di $\mathbb{Z}_3[i]$ adalah unit sebab

$$[1]_3^{-1} = [1]_3, \;\; [2]_3^{-1} = [2]_3, \;\; ([1]_3 i)^{-1} = [2]_3 i$$

dan

$$([1]_3 + [1]_3 i)^{-1} = [2]_3 + [1]_3 i, \;\; ([1]_3 + [2]_3 i)^{-1} = [2]_3 + [2]_3 i.$$

Dengan demikian $\mathbb{Z}_3[i]$ adalah suatu lapangan. ●

Contoh 6.3.10 Diberikan grup kuoternion

$$Q_8 = \{\pm 1, \pm \boldsymbol{i}, \pm \boldsymbol{j}, \pm \boldsymbol{k}\},$$

maka $\mathbb{H}$ ring kuoternion sebagaimana dibahas dalam Contoh 6.1.11 dapat didefinisikan sebagai

$$\mathbb{H} = \{a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \,|\, a, b, c, d \in \mathbb{R} \text{ dan } \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k} \in Q_8\}.$$

Himpunan $\mathbb{H}$ adalah suatu ring dengan elemen satuan 1. Selanjutnya bila $x \in \mathbb{H}$ dimana $x \neq 0$ dan $x = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$, maka didapat $x^* = a - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}$. Juga

$$xx^* = a^2 + b^2 + c^2 + d^2 \neq 0 \;\text{ dan }\; x(x^*/xx^*) = 1.$$

Jadi semua $x \in \mathbb{H}$ dengan $x \neq 0$ adalah unit. Apapun hal tersebut, karena $\boldsymbol{ij} = \boldsymbol{k}$ dan $\boldsymbol{ji} = -\boldsymbol{k}$, maka $\mathbb{H}$ bukan suatu ring komutatif. Dengan demikian $\mathbb{H}$ bukan suatu lapangan. ●

Definisi 6.3.4 Suatu ring R dengan elemen satuan yang memenuhi setiap elemen taknol $a \in R$ adalah suatu unit dinamakan suatu **ring pembagian** (division ring).

Contoh 6.3.11 Setiap lapangan adalah suatu ring pembagian dan ring kuoternion $\mathbb{H}$ adalah suatu contoh ring pembagian yang bukan suatu lapangan.

Dikenalkan suatu konsep terakhir dalam bagian ini yang dinamakan kharakteristik.

Contoh 6.3.12 Dalam $\mathbb{Z}_6$ bisa didapat suatu bilangan bulat positip terkecil n yang memenuhi $na = [0]_6$ untuk semua $a \in \mathbb{Z}_6$, yaitu $n = 6$. Dengan cara yang sama, dalam $\mathbb{Z}_4 \times \mathbb{Z}_6$ didapat $n = 12$, yang memenuhi $12(a, b) = (12a, 12b) = ([0]_4, [0]_6)$ untuk semua $(a, b) \in \mathbb{Z}_4 \times \mathbb{Z}_6$ dan tidak ada bilangan bulat positip lebih kecil dari bilangan bulat tersebut yang memenuhi sifat tersebut. Dalam ring $\mathbb{Z}$, tidak ada bilangan bulat positip terkecil n yang memenuhi $na = 0$ untuk semua $a \in \mathbb{Z}$.

Definisi 6.3.5 Dalam suatu ring R, **kharakteristik** dari R dinotasikan oleh khar(R) adalah bilangan bulat positip terkecil n yang memenuhi $n.r = 0_R$ untuk semua $r \in R$. Bila tidak ada bilngan n yang demikian, maka khar(R) = 0.

Contoh 6.3.13 Untuk setiap bilangan bulat positip n ada suatu ring yang mempunyai karakter sama dengan n yaitu $\mathbb{Z}_n$ himpunan bilangan bulat modulo n. Sedangkan khar($\mathbb{Z}$) = khar($\mathbb{Q}$) = khar($\mathbb{R}$) = khar($\mathbb{C}$) = 0.

Bila ring R mempunyai elemen satuan, maka mudah untuk menentukan kharakteristik dari R sebagaimana ditunjukan berikut.

Teorema 6.3.7 Misalkan R adalah ring dengan elemen satuan 1_R. Maka

(1) khar(R) = 0 bila elemen satuan 1_R mempunyai order tak-berhingga terhadap operasi "tambah".

(2) khar(R) = n bila elemen satuan 1_R mempunyai order n terhadap operasi "tambah".

Bukti (1) Bila $|1_R| = +\infty$, maka tidak akan ada bilangan bulat berhingga n yang memenuhi $n.1_R = 0_R$. Jadi khar(R) = 0. (2) Bila $|1_R| = n$, maka n adalah bilangan bulat positip terkecil yang memenuhi $n.1_R = 0_R$ dan untuk semua $a \in R$ didapat $n.a = n(1_R.a) = (n.1_R)a = 0_R.a = 0_R$. Terlihat bahwa khar($R$) = n

Contoh 6.3.14 Dalam $R = \mathbb{Z}_4 \times \mathbb{Z}_6$ elemen satuan adalah $([1]_4, [1]_6)$ dan khar(R) = $|([1]_4, [1]_6)|$ = 12. Tinjau himpunan bagian $S = \mathbb{Z}_4 \times \{[0]_6\} \subseteq R$. Maka S adalah subring dari R dengan elemen satuan $([1]_4, [0]_6)$ dan khar(S) = $|([1]_4, [0]_6)| = 4 \neq$ khar(R). Dengan kata lain karakteristik dari subring S bisa berbeda dengan kharakteristik dari ring R.

Apa yang terjadi dalam Contoh 6.3.14 tidak akan terjadi dalam suatu daerah integral. Contoh berikut menjelaskan hal tersebut.

Contoh 6.3.15 Misalkan D adalah sebarang daerah integral dan S adalah suatu sub-daerah dari D. Berdasarkan Proposisi 6.2.1 bila elemen satuan $1_D \in D$, maka $1_D \in S$. Dengan kata lain D dan S mempunyai elemen satuan yang sama. Jadi khar(D) = $|1_D|$ = khar(S).

Diakhir bagian ini diberikan suatu sifat karakteristik dari suatu daerah integral.

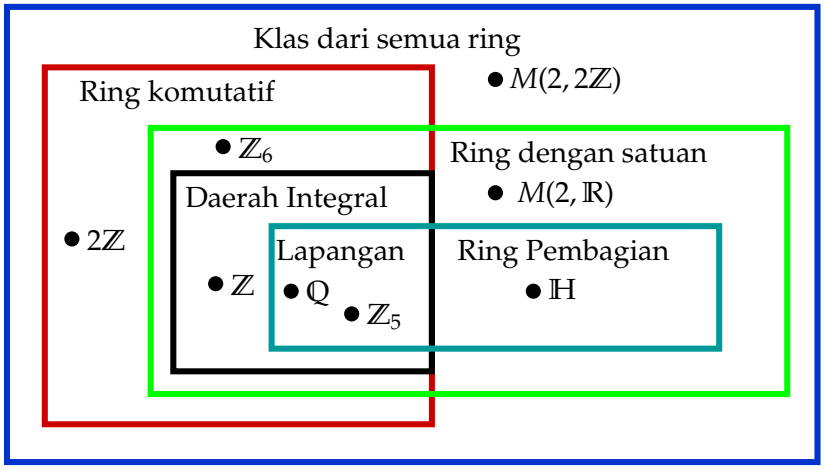
Teorema 6.3.8 Misalkan D adalah suatu daerah integral. Maka khar$(D) = 0$ atau khar$(D) = p$, dimana p adalah prima.

Bukti Asumsikan D adalah daerah integral dengan khar$(D) \neq 0$. Pilih bilangan bulat positip terkecil n yang memenuhi $n.1_D = 0_D$. Andaikan n bukan prima, maka $n = uv$ untuk beberapa bilangan bulat $u < n$ dan $v < n$. Didapat

$$0_D = n.1_D = (uv).1_D = (u.1_D)(v.1_D) \in D.$$

Karena D adalah suatu daerah integral maka $u.1_D = 0_D$ atau $v.1_D = 0_D$. Hal ini bertentangan dengan kenyataan pilihan n adalah bilangan bulat positip terkecil yang memenuhi $n.1_D = 0_D$. Dengan demikian haruslah n adalah prima. ∎

Visualisasi Gambar 6.1 membantu kita untuk mengenal lebih baik berbagai macam ring yang telah dikenalkan dalam bab ini. Dalam masing-masing macam bagian suatu contoh yang mewakili diberikan. Bila diinginkan bisa dikonstruksi contoh-contoh yang lain sebagaimana yang dikehendaki untuk masing-masing macam dari 6 bagian yang ada.



Gambar 6.1: Semua klas Ring

Latihan

Latihan 6.3.1 Dapatkan semua unit dari ring berkut.

1. $\mathbb{Z}_{10}$
2. $\mathbb{Z}_2 \times \mathbb{Z}_4$
3. $\mathbb{Z}[i]$
4. $\mathbb{Z} \times \mathbb{Z}$
5. $\mathbb{H}$
6. $\mathbb{C}$
7. $\mathbb{Q}(\sqrt{3})$
8. $M(2, \mathbb{Z}_2)$
9. $M(2, \mathbb{Z})$
10. $M(2, \mathbb{R})$.

∎

Latihan 6.3.2 Misalkan a adalah suatu unit dalam suatu ring R dengan satuan. Tunjukkan bahwa invers terhadap perkalian dari a adalah suatu unit di R. ∎

Latihan 6.3.3 Misalkan R adalah suatu ring dengan satuan $1 \in R$ dan S suatu subring dari R dengan $1 \in S$. Tunjukkan bahwa bila $a \in S$ adalah suatu unit di S, maka a adalah suatu unit di R. Tunjukkan dengan suatu contoh bahwa hal yang sebaliknya tidak perlu benar. ∎

Latihan 6.3.4 Misalkan R_1 dan R_2 adalah ring komutatif yang mempunyai elemen satuan. Tunjukkan bahwa grup unit berikut $\mathbb{U}(R_1 \times R_2) \cong \mathbb{U}(R_1) \times \mathbb{U}(R_2)$.

Latihan 6.3.5 Misalkan R adalah suatu ring komutatif yang mempunyai elemen satuan dan $M(2, R)$ adalah himpunan matriks berukuran 2×2 dengan elemen-elemen di R. Tunjukkan bahwa $A \in M(2, R)$ adalah suatu unit bila dan hanya bila $\det(A)$ adalah suatu unit di R.

Latihan 6.3.6 Dari ring berikut tentukan mana yang merupakan lapangan.

1. $\mathbb{Z}[i]$
2. $\mathbb{Q} \times \mathbb{Q}$
3. $\mathbb{Z}_{13}$
4. $\mathbb{Q}(\sqrt{3})$
5. $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$
6. $\mathbb{H}$
7. $\mathbb{Z}_2[i] = \{a + bi \mid a, b \in \mathbb{Z}_2\}$.

Latihan 6.3.7 Misalkan S dan T adalah sub-lapangan dari suatu lapnagn $\mathbb{F}$. Tunjukkan bahwa $S \cap T$ adalah suatu sub-lapngan dari $\mathbb{F}$.

Latihan 6.3.8 Tentukan karakteristik dari ring berikut.

1. $\mathbb{Z}_{10} \times \mathbb{Z}_8$
2. $\mathbb{C}$
3. $\mathbb{Z} \times \mathbb{Z}$
4. $\mathbb{H}$
5. $\mathbb{Q}(\sqrt{2})$
6. $\mathbb{Z}_3[i]$
7. $\mathbb{Z}_2 \times \mathbb{Q} \times \mathbb{Z}_3$.

Latihan 6.3.9 Misalkan $\mathbb{F}$ adalah suatu lapangan dengan $\text{khar}(F) = p > 0$. Tunjukkan bahwa untuk sebarang elemen $a, b \in F$ didapat $(a + b)^p = a^p + b^p$.

Latihan 6.3.10 Tunjukkan bahwa D adalah suatu daerah integral dengan $\text{khar}(D) = 0$, maka D adalah tak-berhingga.

Latihan 6.3.11 Misalkan $\mathbb{F}$ adalah suatu lapangan dengan $|\mathbb{F}| = q$. Tunjukkan bahwa untuk semua $a \in \mathbb{F}$ didapat $a^q = a$.

Latihan 6.3.12 Misalkan p adalah bilangan prima dan persamaan $x^p - 1 = 0$. Tunjukkan bahwa
(a) dalam $\mathbb{C}$, $x^p - 1 = 0$ mempunyai p penyelesaiaan yang berbeda.
(b) Dalam suatu lapangan $\mathbb{F}$ dengan $\text{khar}(F) = p$, maka $x^p - 1 = 0$ mempunyai hanya satu penyelesaiaan (Pentunjuk: Gunakan Latihan 6.3.9).

Latihan 6.3.13 Suatu elemen a dalam suatu ring R dikatakan **nilpoten** bila untuk beberapa $k \geq 1$ didapat $a^k = 0$. Tunjukkan bahwa himpunan dari elemen nilpoten dalam suatu ring komutatif R membentuk suatu subring dari R.

Latihan 6.3.14 Dapatkan semua elemen nilpoten dalam $\mathbb{Z}_{24}$.

Latihan 6.3.15 Tunjukkan bahwa bila D adalah suatu daerah integral, maka 0 adalah satu-satunya elemen nilpoten dalam D.

Latihan 6.3.16 Misalkan a adalah suatu elemen nilpoten dalam suatu ring komutatif R dengan elemem satuan. Tunjukkan bahwa:
(a) $a = 0$ atau a adalah suatu pembagi nol.
(b) ax adalah nilpoten untuk semua $x \in R$.
(c) $1 + a$ adalah suatu unit di R.
(d) Bila u adalah suatu unit di R, maka $u + a$ juga suatu unit di R.

Latihan 6.3.17 Dalam suatu ring R suatu elemen $a \in R$ dinamakan **idempoten** bila $a^2 = a$. Tunjukkan bahwa dalam suatu daerah integral D hanyalah 0 dan 1 elemen idempoten di D.

Latihan 6.3.18 Dapatkan semua elemen idempoten di $\mathbb{Z}_6, \mathbb{Z}_{12}$ dan $\mathbb{Z}_6 \times \mathbb{Z}_{12}$.

Latihan 6.3.19 Tunjukkan bahwa suatu ring R adalah suatu ring pembagian bila dan hanya bila untuk sebarang $a \in R$ ada suatu elemen tunggal $b \in R$ yang memenuhi $aba = a$.

Latihan 6.3.20 Tunjukkan bahwa senter dari suatu ring pembagian adalah suatu lapangan.

Latihan 6.3.21 Tunjukkan bahwa suatu ring berhingga R dengan elemen satuan dan tanpa elemen elemen pembagi nol adalah suatu ring pembagian.

Latihan 6.3.22 Didefinisikan **kuoternion integral** sebagai berikut:

$$I = \{a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \mid a, b, c, d \in \mathbb{Z}\} \subseteq \mathbb{H}.$$

(a) Tunjukkan bahwa I adalah suatu subring dari $\mathbb{H}$.
(b) Misalkan $N : I \to \mathbb{Z}$ adalah fungsi dinamakan **norm** yang didefinisikan oleh

$$N(a + b\boldsymbol{i}, +c\boldsymbol{j} + d\boldsymbol{k}) = a^2 + b^2 + c^2 + d^2 \in \mathbb{Z}.$$

Tunjukkan bahwa untuk semua $z = a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} \in I$, $N(z) = zz^*$, dimana

$$z^* = a - b\boldsymbol{i} - c\boldsymbol{j} - d\boldsymbol{k}.$$

(c) Tunjukkan bahwa $N(zw) = N(z)N(w),\ \forall z, w \in I$.
(d) Tunjukkan bahwa $z \in I$ adalah suatu unit bila dan hanya bila $N(z) = 1$.
(e) Tunjukkan bahwa grup dari unit di I adalah $\mathbb{U}(I) = Q_8$.

Bab 7

Homomorpisma Ring

Dalam Bab 2 telah dibahas pemetaan dari suatu grup G ke group yang lain G' dinamakan homomorpisma grup. Dalam bab ini didefinisikan homomorpisma ring. Ditunjukkan bahwa bagaimana homomorpisma ring memberikan sesuatu yang lebih penting terhadap pemahaman dari suatu macam subring khusus yang dinamakan suatu ***ideal***. Dapat ditunjukkan bahwa image homomorpisma dari suatu ring isomorpik dengan suatu ***ring kuasi***. Homomorpisma ring, ideal dan ring kousi mempunyai keterkaitan yang dekat tepatnya seperti cara dalam homomorpisma grup. Pengkonstruksian ***lapangan kuasi*** dari suatu daerah integral dibahas pada akhir bab ini.

7.1 Definisi dan Sifat-sifat Dasar

Seperti halnya dalam grup, pemetaan diantara ring yang digunakan haruslah pemetaan yang mempertahan struktur aljabar dari ring. Untuk itu ditinjau pemetaan yang dikaitkan dengan dua operasi dalam ring. Karena suatu ring adalah suatu grup terhadap operasi "tambah", maka pemetaan yang dipertimbangkan adalah suatu pemetaan homomorpisma grup terhadap operasi "tambah" begitu juga terhadap operasi "perkalian".

Contoh 7.1.1 Diberikan ring $\mathbb{Z}$ dan $2\mathbb{Z}$, dan pemetaan natural $\phi(n) = 2n$ untuk semua $n \in \mathbb{Z}$. Telah diketahui bahwa ϕ adalah suatu homomorpisma grup terhadap $+$, sebab $\phi(m+n) = 2(m+n) = 2m + 2n = \phi(m) + \phi(n)$. Tetapi terhadap operasi perkalian (.), didapat $2 = \phi(1) = \phi(1.1) \neq \phi(1).\phi(1) = 2.2 = 4$. Dengan kata lain terhadap operasi perkalian (.) dalam $\mathbb{Z}$ tidak memenuhi seperti yang akan diharapkan. ●

Contoh 7.1.2 Diberikan pemetaan dari ring $\mathbb{Z}$ ke ring $\mathbb{Z}_3$ oleh $\phi(n) = n \mod 3$ untuk semua $n \in \mathbb{Z}$. Sebagaimana telah diketahui, untuk semua m dan n di $\mathbb{Z}$ didapat
$\phi(m+n) = (m+n) \mod 3 = (m \mod 3) + (n \mod 3) = \phi(m) + \phi(n)$,
$\phi(m.n) = (m.n) \mod 3 = (m \mod 3).(n \mod 3) = \phi(m).\phi(n)$.
Terlihat bahwa dalam contoh ini pemetaan ϕ memenuhi kriteria sebagaimana yang akan diharapkan. ●

Definisi 7.1.1 Suatu pemetaan dari suatu ring R ke suatu ring R' yaitu $\phi : R \to R'$ dinamakan suatu ***homomorpisma ring*** bila untuk semua $x, y \in R$ didapat

(1) $\phi(x+y) = \phi(x) + \phi(y)$,

(2) $\phi(x.y) = \phi(x).\phi(y)$.

Perlu diperhatikan bahwa dua operasi yang digunakan pada persamaan bagian kiri adalah di ring R, sedangkan pada sebelah kanan di ring R'.

Catatan bahwa kondisi (1) dalam Definisi 7.1.1 menjelaskan bahwa pemetaan ϕ adalah suatu homomorpisma grup terhadap operasi "tambah".

Contoh 7.1.3 Diberikan pemetaan $\phi : \mathbb{Z}_4 \to \mathbb{Z}_6$ didefinisikan oleh $\phi(x) = [3x]_6$ untuk semua $x \in \mathbb{Z}_4$. Sebagaimana telah diketahui operasi tambah dan kali dalam modulo, maka untuk setiap $x, y \in \mathbb{Z}_4$ didapat
$\phi(x+y) = 3(x+y) \mod 6 = (3x \mod 6) + (3y \mod 6) = \phi(x) + \phi(y)$,
$\phi(x.y) = 3(x.y) \mod 6 = 9(x.y) \mod 6 = (3x \mod 6).(3y \mod 6) = \phi(x).\phi(x)$.
Terlihat bahwa dalam contoh ini pemetaan ϕ adalah suatu homomorpisma ring.

Contoh 7.1.4 Diberikan pemetaan homomorpisma $\phi : \mathbb{Z} \to \mathbb{Z}$, diselidiki ada berapa banyak pemetaan homomorpisma tersebut. Pemetaan homomorpisma ϕ haruslah suatu homomorpisma grup terhadap tambah. Karena $\mathbb{Z}$ adalah grup siklik dibangun oleh 1, maka image dari 1 yaitu $\phi(1)$ secara lengkap menentukan ϕ. Dengan demikian, misalkan $\phi(1) = n \in \mathbb{Z}$. Maka didapat

$$n = \phi(1) = \phi(1.1) = \phi(1).\phi(1) = n^2.$$

Jadi $n^2 = n$ di $\mathbb{Z}$, hal ini ekivalen dengan $n(n-1) = 0$. Tetapi, karena $\mathbb{Z}$ tidak memuat pembagi nol, maka $n = 0$ atau $n = 1$. Selanjutnya bila $\phi(1) = n = 0$, maka $\phi(m) = 0$ untuk semua $m \in \mathbb{Z}$. Dengan demikian homomorpisma ϕ adalah pemetaan nol. Bila $\phi(1) = n = 1$, maka $\phi(m) = m$ untuk semua $m \in \mathbb{Z}$. Dengan demikian homomorpisma ϕ adalah pemetaan identitas. Jadi hanya ada dua pemetaan homomorpisma yang mungkin yaitu pemetaan nol dan pemetaan identitas.

Contoh 7.1.5 Diberikan pemetaan homomorpisma $\phi : \mathbb{Z}_6 \to \mathbb{Z}_{12}$, diselidiki ada berapa banyak pemetaan homomorpisma tersebut. Lagi, dengan menggunakan fakta bahwa $\mathbb{Z}_6$ adalah grup siklik terhadap operasi tambah dengan generator $[1]_6$, maka $\phi([1]_6) = x \in \mathbb{Z}_{12}$ secara lengkap menentukan ϕ. Dari Proposisi 3.2.2 bagian (4) didapat $|\phi([1]_6)| \in \mathbb{Z}_{12}$ membagi $|[1]_6| = 6$. Jadi
$|x| = 1$ dan $x = [0]_{12}$, atau $|x| = 2$ dan $x = [6]_{12}$, atau
$|x| = 3$ dan $x = [4]_{12}$ atau $x = [8]_{12}$, atau $|x| = 6$ dan $x = [2]_{12}$ atau $x = [10]_{12}$.
Sebegitu jauh apa yang dibahas hanya menggunakan kondisi (1) dari pengertian homomorpisma ring. Berikutnya, digunakan kondisi (2) dalam definisi homomorpisma ring, didapat

$$x = \phi([1]_6) = \phi([1]_6.[1]_6) = \phi([1]_6).\phi([1]_6) = x^2.$$

Dengan demikian nilai x yang mungkin haruslah memenuhi $x^2 = x \in \mathbb{Z}_{12}$. (Elemen yang demikian dalam suatu ring dinamakan idempoten). Karena dalam $\mathbb{Z}_{12}$ berlaku

$$[6]_{12}^2 = [0]_{12}, [8]_{12}^2 = [2]_{12}^2 = [10]_{12}^2 = [4]_{12}.$$

Jadi nilai $x \in \mathbb{Z}_{12}$ yang mungkin hanyalah $x = [0]_{12}$ dan $x = [4]_{12}$. Dengan demikian didapat $\phi(y) = [0]_{12}$, $\forall y \in \mathbb{Z}_6$ atau $\phi(y) = [4y]_{12}$, $\forall y \in \mathbb{Z}_6$. Jadi hanya ada dua pemetaan homomorpisma ring yang mungkin dari $\mathbb{Z}_6$ ke $\mathbb{Z}_{12}$, yaitu pemetaan nol dan pemetaan yang didefinisikan oleh $\phi(y) = [4y]_{12}$, $\forall y \in \mathbb{Z}_6$.

Dalam suatu homomorpisma ring didefinisikan kernel seperti kernel dari homomorpisma grup terhadap operasi tambah.

Definisi 7.1.2 Misalkan $\phi : R \to R'$ adalah suatu homomorpisma ring. Maka **kernel** dari ϕ adalah himpunan $\text{Ker}(\phi) = \{x \in R \,|\, \phi(x) = 0_{R'}\} \subseteq R$.

Dalam beberapa contoh sudah terlihat berulang kali penggunaan sifat-sifat yang telah dikenal dari homomorpisma grup. Karena ring adalah grup terhadap operasi tambah, sifat-sifat berikut dari homomorpisma ring mengikuti Proposisi 3.2.2 dan 3.2.3.

Proposisi 7.1.1 Misalkan $\phi : R \to R'$ adalah suatu homomorpisma ring. Maka

(1) $\phi(0_R) = 0_{R'}$,

(2) $\phi(-x) = -\phi(x)$, untuk semua $x \in R$,

(3) $\phi(nx) = n\phi(x)$, untuk semua $x \in R$ dan $n \in \mathbb{Z}$,

(4) ϕ adalah satu-satu bila dan hanya bila $\text{Ker}(\phi) = \{0_R\}$.

Berikut ini dibahas beberapa sifat homomorpisma ring yang melibatkan kondisi (1) dan (2) dari definisi homomorpisma ring.

Proposisi 7.1.2 Misalkan $\phi : R \to R'$ adalah suatu homomorpisma ring. Maka

(1) $\phi(x^n) = \phi(x)^n$, untuk semua $x \in R$ dan untuk semua $n > 0$, $n \in \mathbb{Z}$.

(2) Bila A adalah suatu subring dari R, maka $\phi(A) = \{\phi(x) \in R' \,|\, x \in A\} \subseteq R'$ adalah suatu subring dari R'.

(3) Bila R adalah suatu ring dengan satuan 1_R, maka $\phi(1_R)$ adalah suatu satuan di $\phi(R)$ dan $\phi(1_R)^2 = \phi(1_R)$.

(4) Bila R adalah suatu ring dengan satuan 1_R dan $x \in \mathbb{U}(R)$ adalah suatu unit di R, maka $\phi(x^n) = \phi(x)^n$ di $\phi(R)$ untuk semua $n \in \mathbb{Z}$.

(5) Bila B adalah suatu subring dari R', maka $\phi^{-1}(B) = \{x \in R \,|\, \phi(x) \in B\} \subseteq R$ adalah subring dari R dan $\text{Ker}(\phi) \subseteq \phi^{-1}(B)$.

(6) $\text{Ker}(\phi)$ adalah suatu subring dari R.

(7) Bila R adalah suatu ring komutatif, maka $\phi(R)$ adalah suatu ring komutatif.

Bukti

(1) Untuk $n = 1$, didapat $\phi(x^1) = \phi(x) = \phi(x)^1$. Bila $k > 0$ dan $\phi(x^k) = \phi(x)^k$, maka

$$\phi(x^{k+1}) = \phi(x^k.x) = \phi(x^k).\phi(x) = \phi(x)^k.\phi(x) = \phi(x)^{k+1}.$$

Jadi (1) terbukti melalui induksi matematika.

(2) Bila A subring dari R, maka menurut Proposisi 3.2.2 bagian (5), $\phi(A)$ adalah suatu subgrup dari R' terhadap operasi tambah. Selanjutnya untuk sebarang $x, y \in \phi(A)$, dapat dipilih beberapa $a, b \in A$ yang memenuhi $\phi(a) = x$ dan $\phi(b) = y$. Catatan bahwa karena A adalah subring dari R, didapat $ab \in A$. Dengan demikian

$$xy = \phi(a)\phi(b) = \phi(ab) \in \phi(A).$$

Maka dari itu menggunakan sifat-sifat subring (Teorema 6.1.2) $\phi(A)$ adalah subring dari R'.

(3) Diberikan sebarang $x \in \phi(R)$ dapat dipilih beberapa $a \in R$ yang memenuhi $\phi(a) = x$. Dengan demikian didapat

$$x.\phi(1_R) = \phi(a).\phi(1_R) = \phi(a.1_R) = \phi(a) = x.$$

Dengan cara yang sama didapat

$$\phi(1_R).x = \phi(1_R).\phi(a) = \phi(1_R.a) = \phi(a) = x.$$

Terlihat bahwa $\phi(1_R)$ adalah elemen satuan di $\phi(R)$. Selanjutnya, juga

$$\phi(1_R).\phi(1_R) = \phi(1_R.1_R) = \phi(1_R).$$

Jadi $\phi(1_R)^2 = \phi(1_R)$.

(4) Misalkan $x \in \mathbb{U}(R) \subseteq R$. Untuk $n > 0$ dari (1) didapat $\phi(x^n) = \phi(x)^n$. Untuk $n = 0$, $\phi(x^0) = \phi(1_R)$ dari (3) didapat $\phi(1_R)$ adalah elemen satuan di $\phi(R)$ dan $\phi(1_R) = \phi(x)^0$. Maka $\phi(x^0) = \phi(x)^0$. Untuk $n = -1$, didapat $\phi(x).\phi(x^{-1}) = \phi(x.x^{-1}) = \phi(1_R)$ dan dari (3) merupakan elemen satuan di $\phi(R)$. Juga dengan cara yang sama didapat $\phi(x^{-1}).\phi(x) = \phi(x^{-1}.x) = \phi(1_R)$ adalah elemen satuan di $\phi(R)$. Hal ini berakibat $\phi(x)^{-1} = \phi(x^{-1})$ adalah invers dari $\phi(x)$ di $\phi(R)$. Untuk sebarang $n < 0$, misalkan $n = -s$ dimana $s > 0$. Gunakan (1) dan kasus $n = -1$ didapat

$$\phi(x^n) = \phi(x^{-s}) = \phi((x^{-1})^s) = (\phi(x^{-1}))^s = (\phi(x)^{-1})^s = \phi(x)^{-s} = \phi(x)^n.$$

(5) Bila B adalah suatu subring dari R', maka menggunakan Proposisi 3.2.2 bagian (6) $\phi^{-1}(B)$ adalah subgrup dari R terhadap operasi tambah. Untuk sebarang $x, y \in \phi^{-1}(B)$ dan karena B adalah subring R' didapat $\phi(xy) = \phi(x)\phi(y) \in B$. Akibatnya $xy \in \phi^{-1}(B)$. Dengan menggunakan Teorema 6.1.2 maka $\phi^{-1}(B)$ adalah subring dari R. Selanjutnya, karena $0_{R'} \in B$, maka $\text{Ker}(\phi) = \phi^{-1}(0_{R'}) \subseteq \phi^{-1}(B)$.

(6) Misalkan $B = \{0_{R'}\} \subseteq R'$ adalah subring trivial dari R'. Maka dari (5) didapat $\phi^{-1}(B) = \phi^{-1}(0_{R'}) = \text{Ker}(\phi)$ adalah subring dari R.

(7) Diberikan sebarang $x, y \in \phi(R)$ dapat dipilih beberapa $a, b \in R$ yang memenuhi $x = \phi(a)$ dan $y = \phi(b)$. Bila R adalah komutatif, maka

$$xy = \phi(a).\phi(b) = \phi(a.b) = \phi(b.a) = \phi(b).\phi(a) = yx.$$

Dengan demikian $\phi(R)$ adalah komutatif. ∎

Definisi 7.1.3 Suatu homomorpisma ring $\phi : R \to R'$ yang bijektif dinamakan **isomorpima ring**. Dua ring R dan R' dikatakan **isomorpik** ditulis $R \cong R'$ bila ada suatu isomorpisma $\phi : R \to R'$.

Untuk menunjukkan bahwa dua ring adalah isomorpik mengikuti empat langkah yang telah dibahas dalam isomorpisma grup. Sebagai latihan untuk dibuktikan Proposisi 3.2.5 juga berlaku untuk isomorpisma ring. Sedangkan Proposisi 3.2.6 memberikan alat yang penting untuk menentukan apakah dua grup adalah isomorpik. Proposisi berikut memberikan beberapa hal perbandingan untuk ring melalui pengertian ring isomorpik. Bukti dapat dilakukan sebagai latihan.

Proposisi 7.1.3 Diberikan ring isomorpik $R \cong R'$. Maka

(1) Ring R adalah suatu ring komutatif dan mempunyai elemen satuan bila dan hanya bila ring R' adalah suatu ring komutatif dan mempunyai elemen satuan.

(2) Himpunan R adalah suatu daerah integral bila dan hanya bila R' juga adalah suatu daerah integral.

(3) Himpunan R adalah suatu lapangan bila dan hanya bila himpunan R' juga adalah suatu lapangan.

Contoh 7.1.6 Untuk sebarang $a, b \in \mathbb{R}$, misalkan matriks $A(a,b) \in M(2,\mathbb{R})$ didefinisikan oleh

$$A(a,b) \stackrel{\text{def}}{=} \begin{bmatrix} a & b \\ -b & a \end{bmatrix}.$$

Misalkan $R = \{A(a,b) \,|\, a, b \in \mathbb{R}\} \subseteq M(2,\mathbb{R})$. Dapat ditunjukkan bahwa $R \cong \mathbb{C}$ sebagai berikut.

(1) Misalkan pemetaan $\phi : R \to \mathbb{C}$ didefinisikan oleh $\phi(A(a,b)) = a + bi \in \mathbb{C}$ untuk setiap $A((a,b)) \in R$.

(2) Ditunjukkan bahwa ϕ adalah suatu homomorpisma ring. Untuk operasi tambah, didapat

$$\begin{aligned}
\phi(A(a,b) + A(c,d)) &= \phi(\begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix}) \\
&= \phi(\begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix}) \\
&= \phi(A(a+c, b+d)) \\
&= (a+c) + (b+d)i \\
&= (a+bi) + (c+di) \\
&= \phi(A(a,b)) + \phi(A(c,d)).
\end{aligned}$$

Sedangkan untuk perkalian didapat

$$\begin{aligned}
\phi(A(a,b).A(c,d)) &= \phi(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}.\begin{bmatrix} c & d \\ -d & c \end{bmatrix}) \\
&= \phi(\begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix}) \\
&= \phi(A(ac-bd, ad+bc)) \\
&= (ac-bd)+(ad+bc)i \\
&= (a+bi).(c+di) \\
&= \phi(A(a,b)).\phi(A(c,d)).
\end{aligned}$$

Terlihat bahwa ϕ adalah suatu homomorpisma ring.

(3) Pemetaan ϕ adalah satu-satu, sebab $\phi(a,b) = a+bi = 0$ bila dan hanya bila $a = b = 0$. Dengan demikian $\text{Ker}(\phi) = \{A(0,0)\}$ adalah trivial subring dari R.

(4) Pemetaan ϕ adalah **pada**, sebab diberikan sebarang $a+bi \in \mathbb{C}$ dapat dipilih matriks $A(a,b) \in R$ yang memenuhi $\phi(A(a,b)) = a+bi$. ●

Contoh berikut merupakan bahasan di akhir bagian ini. Contoh ini memberikan suatu pemahaman yang penting bahwa suatu permasalahan yang sangat sulit bisa diselesaikan dengan memahami pengertian-pengertian dan sifat-sifat yang telah dibahas.

Contoh 7.1.7 Ditunjukkan bahwa persamaan $2x^3 - 5x^2 + 7x - 8 = 0$ tidak mempunyai penyelesaian untuk semua $x \in \mathbb{Z}$. Hal ini ditunjukkan sebagai berikut. Misalkan $\phi : \mathbb{Z} \to \mathbb{Z}_3$ homomorpisma natural $\phi(x) = x \mod 3$ untuk semua $x \in \mathbb{Z}$. Andaikan ada suatu $a \in \mathbb{Z}$ yang memenuhi $2a^3 - 5a^2 + 7a - 8 = 0$. Maka

$$[0]_3 = \phi(0) = \phi(2a^3 - 5a^2 + 7a - 8) = 2\phi(a)^3 - 5\phi(a)^2 + 7\phi(a) - 8.$$

Karena $-5 \equiv 7 \equiv -8 \equiv 1 \mod 3$, didapat

$$2\phi(a)^3 - 5\phi(a)^2 + 7\phi(a) - 8 = 2\phi(a)^3 + \phi(a)^2 + 1\phi(a) + 1.$$

Bila $b = \phi(a) \in \mathbb{Z}_3$, maka $2b^3 + b^2 + b + 1 = [0]_3$. Tetapi mudah diselidiki bahwa untuk $b = [0]_3, [1]_3, [2]_3$, maka $2b^3 + b^2 + b + 1 \neq [0]_3$. Hal ini bertentangan dengan kenyataan $2b^3 + b^2 + b + 1 = [0]_3$. Dengan demikian tidak ada bilangan bulat $a \in \mathbb{Z}$ yang memenuhi $2a^3 - 5a^2 + 7a - 8 = 0$. Jadi persamaan $2x^3 - 5x^2 + 7x - 8 = 0$ tidak mempunyai penyelesaian di $\mathbb{Z}$. ●

Latihan

Latihan 7.1.1 Dapatkan semua homomorpisma yang mungkin diantara ring berikut.

1. $\phi : \mathbb{Z} \to \mathbb{Z}_3$
2. $\phi : 3\mathbb{Z} \to \mathbb{Z}$
3. $\phi : \mathbb{Z}_4 \to \mathbb{Z}_6$
4. $\phi : \mathbb{Z}_6 \to \mathbb{Z}_{10}$
5. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_6$
6. $\phi : \mathbb{Q} \to \mathbb{Q}$
7. $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$
8. $\phi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$
9. $\phi : \mathbb{Z}[i] \to \mathbb{C}$. ●

Latihan 7.1.2 Tunjukkan bahwa $\mathbb{Z}_m \times \mathbb{Z}_n$ dan $\mathbb{Z}_{mn}$ adalah ring isomorpik bila dan hanya bila m dan n adalah prima relatif.

Latihan 7.1.3 Untuk sebarang $a, b \in \mathbb{Z}$, misalkan $B(a,b) \in M(2,\mathbb{Z})$ didefinisikan oleh

$$B(a,b) \stackrel{\text{def}}{=} \begin{bmatrix} a & 3b \\ b & a \end{bmatrix}.$$

Bila $S = \{B(a,b) \,|\, a, b \in \mathbb{Z}\} \subseteq M(2,\mathbb{Z})$, maka tunjukkan bahwa

$$S \cong \mathbb{Z}[\sqrt{3}] = \{a + b\sqrt{3} \,|\, a, b \in \mathbb{Z}\}.$$

Latihan 7.1.4 Tunjukkan bahwa $\mathbb{R}$ dan $\mathbb{C}$ tidak merupakan ring isomorpik.

Latihan 7.1.5 Tunjukkan bahwa bila $R_1 \cong R_2$ ring isomorpik, maka $\text{khar}(R_1) = \text{khar}(R_2)$.

Latihan 7.1.6 Tunjukkan bahwa $\mathbb{Q}(\sqrt{3})$ dan $\mathbb{Q}(\sqrt{5})$ tidak merupakan ring isomorpik.

Latihan 7.1.7 Misalkan R adalah suatu ring komutatif dengan $\text{khar}(R) = p$ dimana p adalah prima. Tunjukkan bahwa pemetaan $\phi : R \to R$ didefinisikan oleh $\phi(x) = x^p$, untuk semua $x \in R$ adalah suatu homomorpisma ring (ϕ dinamakan **pemetaan Frobenius**).

Latihan 7.1.8 Diberikan ring R_1 dan R_2.

(a) Misalkan $\phi : R_1 \times R_2 \to R_1$ didefinisikan oleh $\phi(a,b) = a$. Tunjukkan bahwa ϕ adalah suatu homomorpisma ring.

(b) Tunjukkan bahwa $\mathbb{R}_1 \times R_2 \cong R_2 \times R_1$.

Latihan 7.1.9 Tunjukkan bahwa relasi isomorpisma $\cong$ adalah suatu relasi ekivalen pada klas dari semua ring.

Latihan 7.1.10 Tunjukkan bahwa persamaan $x^3 + 10x^2 + 6x + 1 = 0$ tidak mempunyai penyelesaian di $\mathbb{Z}$.

Latihan 7.1.11 Selidiki apakah persamaan $x^3 + 6x^2 + 22x + 1 = 0$ mempunyai suatu penyelesaian di $\mathbb{Z}$.

7.2 Ideal

Dalam kasus suatu homomorpisma grup $\phi : G \to G'$, kernel $\text{Ker}(\phi)$ adalah suatu subgrup dari G dengan sifat bahwa setiap koset kiri adalah suatu koset kanan. Dinamakan subgrup yang demikian adalah subgrup normal. Dari kajian subgrup normal telah ditunjukkan bahwa memberikan hasil grup kuasi (grup pecahan). Hal yang sama untuk kasus dari suatu homomorpisma ring $\phi : R \to R'$, sebagaimana telah ditunjukkan $\text{Ker}(\phi)$ adalah suatu subring dari ring R. Faktanya, $\text{Ker}(\phi)$ adalah suatu subring dengan suatu sifat ekstra yang akan memberikan pengertian dari suatu ring kuasi (ring pecahan).

Contoh 7.2.1 Misalkan $K = \text{Ker}(\phi)$, dimana ϕ adalah suatu homomorpisma $\phi : \mathbb{Z} \to \mathbb{Z}_2$ didefinisikan oleh $\phi(x) = x \mod 2$, $\forall x \in \mathbb{Z}$. Dalam hal ini $K = 2\mathbb{Z} \subseteq \mathbb{Z}$. Perhatikan bahwa untuk sebarang $n \in \mathbb{Z}$ dan sebarang $k = 2x \in K$ didapat

$$\phi(nk) = \phi(n.2x) = \phi(n).\phi(2x) = [0]_2$$

dan

$$\phi(kn) = \phi(2x.n) = \phi(2x).\phi(n) = [0]_2.$$

Hal ini menunjukkan bahwa untuk sebarang $n \in \mathbb{Z}$ dan $k \in K$ didapat $nk \in K$ dan $kn \in K$. Sifat ini berlaku untuk kernel dari sebarang homomorpisma ring sebagaimana ditunjukkan berikut ini.

Proposisi 7.2.1 Misalkan $\phi : R \to R'$ adalah suatu homomorpisma ring dan $K = \text{Ker}(\phi)$. Maka

(1) K adalah suatu subring dari R.

(2) Untuk semua $r \in R$ dan semua $k \in K$, maka $rk \in K$ dan $kr \in K$.

Bukti

(1) Telah ditunjukkan dalam Proposisi 7.1.2 bagian (6) bahwa $\text{Ker}(\phi)$ adalah subring dari R.

(2) Misalkan sebarang $r \in R$ dan sebarang $k \in K$. Maka didapat

$$\phi(rk) = \phi(r)\phi(k) = \phi(r).0_{R'} = 0_{R'}$$

dan

$$\phi(kr) = \phi(k)\phi(r) = 0_{R'}.\phi(r) = 0_{R'}.$$

Terlihat bahwa $rk \in K$ dan $kr \in K$.

Definisi 7.2.1 Misalkan R adalah suatu ring dan I adalah suatu himpunan bagian takkosong dari R. Maka I dinamakan suatu **ideal** dari R bila

(1) I adalah suatu subring dari R.

(2) Untuk semua $r \in R$ dan semua $x \in I$ maka $rx \in I$ dan $xr \in I$.

Akibat 7.2.1 Misalkan $\phi : R \to R'$ adalah suatu homomorpisma ring dengan $K = \text{Ker}(\phi)$. Maka K adalah suatu ideal dari R.

Bukti Langsung dari Proposisi 7.2.1 dan Definisi 7.2.1.

Contoh 7.2.2 Diselidiki semua ideal dari $\mathbb{Z}$. Bila I adalah suatu ideal dari $\mathbb{Z}$, maka menurut Definisi 7.2.1 bagian (1), I adalah subring dari $\mathbb{Z}$. Jadi $I = n\mathbb{Z}$ untuk beberapa $n \geq 1$ dan misalkan sebarang $a \in \mathbb{Z}$ dan sebarang $b \in I$. Didapat $b = nk$ untuk beberapa $k \in \mathbb{Z}$ dan

$$ab = a(nk) = n(ak) \in n\mathbb{Z} = I$$

juga

$$ba = (nk)a = n(ak) \in n\mathbb{Z} = I.$$

Terlihat bahwa I adalah suatu ideal dari $\mathbb{Z}$. Jadi semua ideal dari $\mathbb{Z}$ adalah $n\mathbb{Z}$ untuk sebarang $n \geq 1$.

Contoh berikut menjelakan bahwa supaya tidak membuat kesimpulan yang salah. Yaitu semua subring dari suatu ring yang diberikan tidak harus merupakan suatu ideal dari ring tersebut.

Contoh 7.2.3 Himpunan $\mathbb{Z}$ adalah suatu subring dari $\mathbb{Q}$, tetapi bukan suatu ideal dari $\mathbb{Q}$. Sebab, untuk $1/2 \in \mathbb{Q}$ dan $5 \in \mathbb{Z}$ didapat $(1/2).5 \notin \mathbb{Z}$. ●

Contoh 7.2.4 Dalam sebarang ring R, himpunan $\{0_R\}$ adalah suatu ideal dari R yang dinamakan ideal **trivial** dan R sendiri adalah suatu ideala dari R yang dinamakan ideal **sejati**. ●

Contoh 7.2.5 Misalkan R adalah suatu ring komutatif dan sebarang $a \in R$. Didefinisikan **ideal utama yang dibangun oleh** a, dinotasikan oleh $\langle a \rangle$ sebagai berikut

$$\langle a \rangle \stackrel{\text{def}}{=} \{ra \,|\, r \in R\}.$$

Dengan kata lain $\langle a \rangle$ adalah kelipatan dari semua a dengan sebarang elemen $r \in R$. Catatan bahwa $\langle a \rangle$ adalah suatu ideal dari R sebab memenuhi kondisi ideal yaitu:

(1) Diberikan sebarang x dan y di $\langle a \rangle$ dapat dipilih beberapa r dan s di R yang memenuhi $x = ra$ dan $y = sa$. Juga

$$x - y = ra - sa = \underbrace{(r-s)}_{\in R} a \in \langle a \rangle \quad \text{dan} \quad xy = ra.sa = \underbrace{(ras)}_{\in R} a \in \langle a \rangle .$$

Terlihat bahwa $\langle a \rangle$ adalah subring dari R.

(2) Untuk sebarang $r \in R$ dan sebarang $x = sa \in \langle a \rangle$ didapat

$$rx = r(sa) = \underbrace{(rs)}_{\in R} a \in \langle a \rangle \quad \text{dan} \quad xr = rx = r(sa) = \underbrace{(rs)}_{\in R} a \in \langle a \rangle . \quad ●$$

Contoh 7.2.6 Setiap ideal di $\mathbb{Z}$ adalah suatu ideal utama. Dari Contoh 7.2.2 didapat bahwa setiap ideal dari $\mathbb{Z}$ adalah $I = n\mathbb{Z}$ untuk $n \geq 1$. Jadi $I = \langle n \rangle$ adalah ideal utama yang dibangun oleh n. ●

Contoh 7.2.7 Diselidiki semua ideal dari $\mathbb{Q}$. Misalkan $I \neq \{0\}$ adalah suatu ideal nontrivial dari $\mathbb{Q}$. Jadi ada suatu elemen $a \in I$ dengan $a \neq 0$. Karena $a \in \mathbb{Q}^* = \mathbb{Q} - \{0\}$ dan $\mathbb{Q}$ adalah suatu lapangan, maka a adalah suatu unit. Dengan kata lain, ada invers terhadap perkalian $a^{-1} \in \mathbb{Q}$ yang memenuhi $a^{-1}a = 1$. Tetapi karena $a^{-1} \in \mathbb{Q}$, $a \in I$ dan I adalah ideal, didapat

$$1 = a^{-1}a \in I.$$

Lagi, dengan menggunakan fakta bahwa I adalah suatu ideal dan diberikan sebarang $b \in \mathbb{Q}$ didapat

$$b = b.1 \in I.$$

Jadi $\mathbb{Q} \subset I$, hal ini berakibat $I = \mathbb{Q}$. Maka dari itu, hanya $\{0\}$ dan $\mathbb{Q}$ yang merupakan ideal dari $\mathbb{Q}$. ●

Contoh ini adalah kesimpulan yang mencolok. Bila secara teliti apa yang dibahas dalam contoh kuncinya adalah fakta bahwa $a \neq 0$ berakibat a adalah suatu unit. Dengan kata lain $\mathbb{Q}$ adalah suatu lapangan. Dengan demikian proposisi berikut ini bukan sebagai suatu kejutan.

Proposisi 7.2.2 Misalkan R adalah suatu ring komutatif yang mempunyai elemen satuan. Maka R adalah suatu lapangan bila dan hanya bila ideal dari R hanyalah $\{0_R\}$ dan R sendiri.

Bukti ($\Rightarrow$) Bila R adalah suatu lapangan dan ideal $I \neq \{0_R\}$ adalah suatu ideal dari R. Maka ada suatu elemen $a \in I$ dan $a \neq 0_R$. Karena R suatu lapangan, maka setiap elemen taknol adalah unit. Juga karena I adalah ideal dari R, maka $1 = a^{-1}a \in I$. Maka dari itu, untuk semua $r \in R$ didapat $r = r.1 \in I$. Jadi $R \subseteq I$, akibatnya $R = I$.
($\Leftarrow$) Misalkan R adalah suatu ring komutatif yang mempunyai elemen satuan. Untuk menunjukkan R adalah suatu lapangan cukup ditunjukkan bahwa semua elemen taknol di R adalah unit. UNtuk itu, misalkan $0_R \neq a \in R$ dan $I = \langle a \rangle$ adalah ideal utama yang dibangun oleh a. Jelas bahwa $I \neq \{0_R\}$ sebab $0_R \neq a \in I$. Bila ideal dari R hanyalah $\{0_R\}$ dan R sendiri. Maka $I = R$. Sebagaimana telah diketahui bahwa R adalah suatu ring dengan satuan, maka $1 \in I = \langle a \rangle$. Dapat dipilih $r = a^{-1} \in R$ yang memenuhi $1 = ra = a^{-1}a$. Dengan demikian a adalah elemen unit sebagaimana dikehendaki. ●

Dari Proposisi 7.2.2 didapat bahwa ideal dari lapangan $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ dan $\mathbb{Z}_p$ dimana p adalah prima hanyalah ideal trivial dan ideal sejati.

Contoh 7.2.8 Diberikan ideal $I = 5\mathbb{Z}$ dari $R = \mathbb{Z}$. Sebagaimana telah diketahui $\mathbb{Z}$ adalah grup komutatif terhadap tambah dengan demikian $5\mathbb{Z}$ adalah suatu subgrup normal dan didapat

$$\mathbb{Z}/5\mathbb{Z} = \{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$$

adalah grup terhadap operasi tambah pada koset di $\mathbb{Z}/5\mathbb{Z}$:

$$(a + 5\mathbb{Z}) + (b + 5\mathbb{Z}) = (a + b) + 5\mathbb{Z}.$$

Selanjutnya secara natural perkalian koset mengikuti operasi tambah pada koset adalah

$$(a + 5\mathbb{Z}).(b + 5\mathbb{Z}) = (ab) + 5\mathbb{Z}.$$

Perkalian koset tersebut diselidiki apakah terdefinisi secara baik. Bila $x + 5\mathbb{Z} = a + 5\mathbb{Z}$ dan $y + 5\mathbb{Z} = b + 5\mathbb{Z}$, maka

$$x \in a + 5\mathbb{Z} \quad \text{dan} \quad y \in b + 5\mathbb{Z}$$

Jadi

$$x = a + 5k \quad \text{dan} \quad y = b + 5j, \text{ untuk beberapa } k, j \in \mathbb{Z}.$$

Dengan demikian didapat

$$xy = (a + 5k)(b + 5j) = ab + \underbrace{b(5k) + a(5j) + (5k)(5j)}_{\in 5\mathbb{Z}}.$$

Terlihat bahwa $xy \in ab + 5\mathbb{Z}$ akibatnya $xy + 5\mathbb{Z} = ab + 5\mathbb{Z}$. Jadi perkalian koset terdefinisi dengan baik. ●

Suatu ring adalah suatu grup terhadap operasi tambah dan suatu ideal I dalam R adalah subring dari R. Maka dari itu I adalah suatu subgrup dari R terhadap operasi tambah. Karena R adalah grup komutatif terhadap operasi tambah, maka I adalah suatu subgrup normal dari R terhadap operasi tambah. Menurut Teorema 3.4.1 dan Proposisi 3.4.1 bagian (3), R/I adalah suatu grup komutatif terhadap operasi tambah pada koset di R/I. Dalam Lemma 3.4.1 ditunjukkan bahwa suatu subgrup adalah subgrup normal ekivalen dengan operasi yang didefinisikan pada koset adalah terdefinisi secara baik. Pada pembahasan berikut ditunjukkan bahwa suatu subring yang merupakan suatu ideal adalah ekivalen dengan operasi perkalian koset terdefinisi secara baik. Yang demikian ini sama halnya membandingkan Lemma 3.4.1 dengan Lemma 7.2.1 dan Teorema 3.4.1 dengan Teorema 7.2.1.

Lemma 7.2.1 Misalkan I adalah suatu subring dari suatu ring R. Maka I adalah suatu ideal dari R bila dan hanya bila perkalian $(a+I)(b+I) = (ab)+I$ adalah suatu operasi terdefinisi secara baik pada koset dari I dalam R.

Bukti ($\Rightarrow$) Asumsikan I adalah suatu ideal dalam R selanjutnya misalkan $a_1 + I = a_2 + I$ dan $b_1 + I = b_2 + I$. Hal ini berakibat bahwa $a_1 = a_2 + k$ dan $b_1 = b_2 + j$ untuk beberapa $k, j \in I$. Maka

$$a_1b_1 = a_2b_2 + a_2j + kb_2 + kj.$$

Karena I adalah suatu subring dari R, maka tertutup terhadap operasi tambah dan perkalian, jadi $kj \in I$. Karena I adalah suatu ideal , maka $a_2j \in I$ dan $kb_2 \in I$. Dengan demikian $a_2j + kb_2 + jk \in I$. Maka dari itu $a_1b_1 \in (a_2b_2) + I$ (hal ini juga berarti bahwa $a_1b_1 \sim a_2b_2$) dengan menggunakan Teorema 3.1.2 didapat $(a_1b_1) + I = (a_2b_2) + I$. Jadi perkalian pada himpunan dari elemen koset dari I terdefinisi secara baik.
($\Leftarrow$) Asumsikan operasi perkalian koset terdefinisi secara baik. Dibutuhkan untuk membuktikan bahwa untuksemua $r \in R$ dan $x \in I$ berlaku $rx \in I$ dan $xr \in I$. Untuk hal demikian, misalkan $r \in R$ dan $x \in I$. Karena $x \in I$, dengan menggunakan Teorema 3.1.2 didapat $x + I = 0_R + I$. Akibatnya

$$rx + I = (r + I)(x + I) = (r + I)(0_R + I) = 0_R + I = I.$$

Lagi dengan menggunakan Teorema 3.1.2 terlihat bahwa $rx \in I$. Dengan cara yang sama dapat ditunjukkan bahwa $xr \in I$. Dengan demikian I adalah suatu daerah integral dalam R.

Teorema 7.2.1 Misalkan I adalah suatu ideal dalam suatu ring R. Maka R/I adalah suatu ring terhadap operasi yang didefiniskan oleh

$$(1)\ \ (a+I)+(b+I) = (a+b)+I \quad \text{dan} \quad (2)\ \ (a+I).(b+I) = (ab)+I,$$

untuk semua $a + I, b + I \in R/I$.

Bukti

(1) Sudah ditunjukkan bahwa R/I berdasarkan Teorema 3.4.1 dan Proposisi 3.4.1 bagian (3), R/I adalah suatu grup komutatif terhadap operasi tambah pada koset di R/I.

(2) Berdasarkan Lemma 7.2.1 perkalian koset terdefinisi secara baik dengan definisi ini operasi perkalian tertutup.

(3) Untuk sebarang $a+I, b+I, c+I \in R/I$, dengan menggunakan fakta bahwa perkalian dalam R adalah asosiatif, didapat

$$\begin{aligned}[(a+I)(b+I)](c+I) &= ((ab)+I)(c+I)\\ &= (ab)c+I\\ &= a(bc)+I\\ &= (a+I)((bc)+I)\\ &= (a+I)[(b+I)(c+I)].\end{aligned}$$

Jadi perkalian dalam R/I adalah asosiatif.

(4) Sifat distributif dalam R/I juga dipenuhi dan pembuktian bisa digunakan sebagai latihan.

Definisi 7.2.2 Misalkan I adalah suatu ideal dalam suatu ring R. Maka R/I terhadap operasi yang telah diberikan dalam Teorema 7.2.1 dinamakan **ring kuasi** dari R oleh I.

Proposisi berikut sebagai akibat langsung dari Definisi 7.2.2 dalam ring kuasi R/I berkaitan dengan operasi perkalian.

Proposisi 7.2.3 Misalkan I adalah suatu ideal dalam suatu ring komutatif R dengan elemen satuan 1_R. Maka R/I adalah suatu ring komutatif dengan elemen satuan $1_R + I$.

Bukti Sudah ditunjukkan bahwa dalam Teorema 7.2.1 R/I terhadap operasi tambah dan perkalian pada koset di R/I adalah suatu ring. Karena R suatu ring komutatif, maka untuk sebarang $a+I, b+I \in R/I$ didapat

$$(a+I)(b+I) = (ab)+I = (ba)+I = (b+I)(a+I).$$

Hal ini menunjukkan bahwa R/I adalah suatu ring komutatif. Karena 1_R adalah elemen satuan di R dan R/I adalah suatu ring komutatif, maka untuk semua $a+I \in R/I$ didapat

$$(1_R+I)(a+I) = (1_R.a)+I = a+I$$

dan

$$(a+I)(1_R+I) = (a.1_R)+I = a+I.$$

Hal ini menunjukkan bahwa $1_R + I$ adalah elemen satuan di R/I. Dengan demikian maka R/I adalah suatu ring komutatif dengan elemen satuan $1_R + I$.

Berikut ini diberikan teorema berkaitan dengan isomorpisma ring.

Teorema 7.2.2 Teorema Isomorpisma Pertama Untuk Ring Misalkan $\phi : R \to R'$ adalah suatu homomorpisma ring dengan kernel $\ker(\phi) = K$. Maka $R/K \cong \phi(R)$.

Bukti Juga karena $\phi : R \to R'$ adalah suatu homomorpisma grup terhadap operasi "+", maka pemetaan $\chi : R/K \to \phi(R)$ didefinisikan oleh $\chi(a+K) = \phi(a)$ adalah suatu pemetaan isomorpisma grup (Torema 3.4.2). Selanjutnya hanya dibutuhkan bahwa pemetaan χ adalah suatu homomorpisma ring dengan kata lain bahwa diselidiki terhadap operasi "perkalian".

Misalkan $a + K$ dan $b + K$ adalah sebarang elemen di R/K dan karena ϕ adalah suatu homomorpisma ring maka didapat

$$\chi[(a + K)(b + K)] = \chi(ab + K) = \phi(ab) = \phi(a)\phi(b) = \chi(a + K)\chi(b + K).$$

dengan demikian lengkap sudah bukti. ✓

Teorema 7.2.3 Diberikan suatu ring R dan suatu ideal K di R, ada suatu homomorpisma pada $\phi : R \to R/K$ dengan $\ker(\phi) = K$.

Bukti Digunakan Teorema 3.4.3, maka pemetaan $\phi : R \to R/K$ yang didefinisikan oleh $\phi(a) = a + K$ adalah suatu homomorpisma grup terhadap operasi "+" dengan $\ker(\phi) = K$. Selanjutnya tinggal hanya menyelidiki terhadap operasi perkalian. Misalkan sebarang $a, b \in R$, maka

$$\phi(ab) = ab + K = (a + K)(b + K) = \phi(a)\phi(b).$$

Terlihat bahwa ϕ adalah suatu homomorpisma ring. Terakhir, dengan menggunakan Teorema 7.2.2 maka ϕ adalah pemetaan pada. ✓

Teorema berikut menunjukkan bahwa suatu homomorpisma ring mempertahan ideal.

Teorema 7.2.4 Misalkan bahwa $\phi : R \to R'$ adalah suatu homomorpisma ring. Maka

(1) Bila I adalah suatu idealdi R, maka $\phi(I)$ adalah suatu ideal di $\phi(R)$.

(2) Bila J adalah suatu ideal di R', maka $\phi^{-1}(J) = \{r \in R \,|\, \phi(r) \in J\}$ adalah suatu ideal di R dengan $\ker(\phi) \subseteq \phi^{-1}(J)$.

Bukti Sebagai latihan! ✓

Bila Toerama 7.2.4 digunakan pada homomorpisma $\phi : R \to R/K$ sebagaimana didefinisikan dalam Teorema 7.2.3, maka terdapat korespondensi diantara ideal di R/K dengan ideal di R yang memuat K.

Proposisi 7.2.4 Misalkan K adalah suatu ideal dalam suatu ring R. Maka

(1) Diberikan suatu ideal I di R dengan $K \subseteq I$, maka $I^* = I/K = \{a + K \,|\, a \in I\}$ adalah suatu ideal di R/K.

(2) Diberikan suatu ideal J^* di R/K, maka ada suatu ideal J di R dengan $K \subseteq J$ yang memenuhi $J^* = J/K = \{a + K \,|\, a \in J\}$.

(3) Diberikan ideal I dan J di R keduanya memuat K, maka $I \subseteq J$ bila dan hanya bila $I/K \subseteq J/K$.

Bukti
Bukti (1) dan (2) langsung dari Teorema 7.2.4 dan Teorema 7.2.3.
(3) Bila $I \subseteq J$, maka

$$I/K = \{a + K \,|\, a \in I\} \subseteq \{a + K \,|\, a \in J\} = J/K.$$

Bila $I/K \subseteq J/K$, maka untuk sebarang $a \in I$ didapat $a + K \in I/K$ dengan demikian $a + K \in J/K$. Jadi $a + K = b + K$ untuk beberapa $b \in J$. Karena $a \in a + K$, maka $a \in b + K$. Jadi $a = b + k$ untuk beberapa $k \in K$. Karena $K \subseteq J$, maka $k \in J$ dan $b + k \in J$. Jadi $a \in J$, hal ini menunjukkan bahwa $I \subseteq J$. ✓

Contoh 7.2.9 Dalam $\mathbb{Z}$ diberikan dua ideal $5\mathbb{Z}$ dan $6\mathbb{Z}$, maka dengan menggunakan Lemma Euclide 1.3.2 bila b dan c adalah bilangan bulat yang memenuhi $bc \in 5\mathbb{Z}$, maka $5|b$ dalam hal ini $b \in 5\mathbb{Z}$ atau $5|c$ dan dalam hal ini $c \in 5\mathbb{Z}$. Dilain pihak, dapat dipilih bilangan bulat x dan y yang memenuhi $x \notin 6\mathbb{Z}$ dan $y \notin 6\mathbb{Z}$ tetapi $xy \in 6\mathbb{Z}$, misalnya $x = 4$ dan $y = 9$.Perlu diperhatikan bahwa homomorpisma ring $\phi : \mathbb{Z} \to \mathbb{Z}_n$ yang didefinisikan oleh $\phi(x) = [x]_n$, maka $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Jadi $\mathbb{Z}/5\mathbb{Z}$ adalah daerah integral, sedangkan $\mathbb{Z}/6\mathbb{Z}$ adalah ring yang mempunyai pembagi nol. Selanjutnya tinjau dua ideal $5\mathbb{Z}$ dan $6\mathbb{Z}$. Catatan bahwa $6\mathbb{Z} \subset 3\mathbb{Z} \subset \mathbb{Z}$ dimana $6\mathbb{Z} \neq 3\mathbb{Z}$ dan $3\mathbb{Z} \neq \mathbb{Z}$. Misalkan bahwa J adalah suatu ideal dimana $5\mathbb{Z} \subseteq J \subseteq \mathbb{Z}$. Pilih suatu bilangan bulat n yang memenuhi $J = n\mathbb{Z}$. Karena $5\mathbb{Z} \subseteq J = n\mathbb{Z}$, maka $5 \in n\mathbb{Z}$ atau $5 = nk$ untuk beberapa $k \in \mathbb{Z}$. Hal ini memberikan $n = 5$ dan $k = 1$, sehingga didapat $5\mathbb{Z} = J$ atau $n = 1$ dan $k = 5$ dalam hal ini $J = \mathbb{Z}$. ●

Contoh 7.2.9 memberikan penjelasan dari bahasan berikut berkaitan dengan dua macam ideal yang khusus.

Definisi 7.2.3 Suatu ideal sejati taktrivial $I \neq R$ dalam suatu ring komutatif R dinamakan suatu ***ideal prima*** bila $ab \in I$ berakibat bahwa $a \in I$ atau $b \in I$ untuk semua a dan b di R. ✓

Definisi 7.2.4 Suatu ideal sejati taktrivial $I \neq R$ dalam suatu ring komutatif R dinamakan suatu ***ideal maximal*** bila hanya ideal J di R yang memenuhi $I \subseteq J \subseteq R$, maka $J = I$ atau $J = R$. ✓

Dalam Contoh 7.2.9, maka ideal $5\mathbb{Z}$ dalam $\mathbb{Z}$ adalah ideal prima sekaligus ideal maksimal. Sedangkan ideal $6\mathbb{Z}$ bukan keduanya.

Contoh 7.2.10 Dalam ring $\mathbb{Z}$ ideal I adalah suatu ideal prima bila dan hanya bila $I = p\mathbb{Z}$, dimana p adalah suatu bilangan bulat prima. Bila p adalah suatu bilangan bulat prima dan $ab \in p\mathbb{Z}$, maka dengan menggunakan Lemma Euclide 1.3.2 didapat $a \in p\mathbb{Z}$ atau $b \in p\mathbb{Z}$. Jadi $I = p\mathbb{Z}$ adalah ideal prima dalam $\mathbb{Z}$. Sebaliknya, bila $I = n\mathbb{Z}$ dimana $n > 1$ bukan suatu ideal prima, maka $n = uv$ untuk beberapa bilangan positip $u, v < n$. Jadi $uv \in n\mathbb{Z}$ sedangkan $u \notin n\mathbb{Z}$ dan $v \notin n\mathbb{Z}$. Dengan demikian $n\mathbb{Z}$ bukan suatu idealprima. ●

Contoh 7.2.11 Dalam ring $\mathbb{Z}$ ideal I adalah suatu ideal maximal bila dan hanya bila I ideal prima. Bila $I = p\mathbb{Z}$ adalah ideal prima dan $p\mathbb{Z} = I \subseteq r\mathbb{Z} \subseteq \mathbb{Z}$, maka $p = rk$ untuk beberapa $k \in \mathbb{Z}$. Didapat $r = p$ dan $k = 1$, maka $r\mathbb{Z} = p\mathbb{Z} = I$ atau $r = 1$ dan $k = p$, dalam hal ini $r\mathbb{Z} = 1\mathbb{Z} = \mathbb{Z}$. Hal ini menunjukkan bahwa $I = p\mathbb{Z}$ adalah ideal maksimal. Sebaliknya, bila $I = n\mathbb{Z}$, $n > 1$ bukan suatu ideal prima, maka n bukan bilangan bulat prima. Jadi $n = uv$ untuk beberapa bilangan bulat positip u, v dimana $1 < u < n$ dan $1 < v < n$. Maka $I = n\mathbb{Z} \subset u\mathbb{Z} \subseteq \mathbb{Z}$, dimana $n\mathbb{Z} \neq u\mathbb{Z}$ (sebab $u < n$) dan $u\mathbb{Z} \neq \mathbb{Z}$ (sebab $1 < u$). Jadi $I = n\mathbb{Z}$ bukan ideal maksimal. ●

Contoh 7.2.12 Contoh ini menjelaskan bahwa ideal prima dan ideal maksimal tidak selalu sama. Dalam ring $R = \mathbb{Z} \times \mathbb{Z}$, tinjau ideal

$$I = \mathbb{Z} \times \{0\} = \{(n, 0) \,|\, n \in \mathbb{Z}\}.$$

Diberikan sebarang $x = (n_1, m_1)$ dan $y = (n_2, m_2)$ elemen di R yang memenuhi $xy \in I$. Maka

$$(n_1n_2, m_1m_2) = (n_1, m_1)(n_2, m_2) = xy \in I,$$

akibatnya $m_1 m_2 = 0$. Tetapi, karena $\mathbb{Z}$ tidak memuat pembagi nol maka $m_1 = 0$, jadi $x = (n_1, 0) \in I$ atau $m_2 = 0$ jadi $y = (n_2, 0) \in I$. Dengan demikian I adalah ideal prima, tetapi bukan ideal maksimal sebab

$$I = \mathbb{Z} \times \{0\} \subset \mathbb{Z} \times 2\mathbb{Z} \subset \mathbb{Z} \times \mathbb{Z} = R,$$

dimana $\mathbb{Z} \times \{0\} \neq \mathbb{Z} \times 2\mathbb{Z}$ dan $\mathbb{Z} \times 2\mathbb{Z} \neq \mathbb{Z} \times \mathbb{Z}$ sedangkan $\mathbb{Z} \times 2\mathbb{Z}$ adalah suatu ideal di R. ●

Pentingnya pengertian ideal prima dan ideal maksimal menjadi jelas dalam teorema berikut.

Teorema 7.2.5 Misalkan R adalah suatu ring komutatif disertai elemen satuan dan I adalah suatu ideal di R. Maka

(1) I adalah ideal prima di R bila dan hanya bila R/I adalah suatu daerah integral,

(2) I adalah ideal maksimal bila dan hanya bila R/I adalah suatu lapangan.

Bukti Dari informasi Teorema 7.2.1 dan Proposisi 7.2.3 R/I adalah suatu ring komutatif disertai elemen satuan.

(1) Maka R/I adalah suatu daerah integral bila dan hanya bila R/I tidak memuat pembagi nol. Kondisi ini ekivalen dengan kondisi bahwa

$$(a + I)(b + I) = I$$

bila dan hanya bila $a + I = I$ atau $b + I = I$. Jadi R/I adalah suatu daerah integral bila dan hanya bila $ab + I = I$ berakibat bahwa $a + I = I$ atau $b + I = I$. Dengan kata lain bila dan hanya bila $ab \in I$ berakibat bahwa $a \in I$ atau $b \in I$ yang artinya bahwa I adalah suatu ideal prima.

(2) Dengan menggunakan Proposisi 7.2.2 maka R/I adalah suatu lapangan bila dan hanya bila ideal di R/I adalah $\{0\} = I$ dan R/I sendiri. Misalkan R/I adalah suatu lapangan dan tinjau sebarang ideal J di R yang memenuhi $I \subseteq J \subseteq R$. Dengan menggunakan Proposisi 7.2.4 maka, $\{0\} \subseteq J/I \subseteq R/I$ dan J/I adalah suatu ideal di R/I. Jadi $J/I = \{0\}$ dalam hal ini $J = I$, atau $J/I = R/I$ dalam kasus ini $J = R$. Jadi I adalah ideal maksimal. Sebaliknya, misalkan bahwa I adalah ideal maksimal di R dan tinjau sebarang ideal J^* di R/I. Lagi gunakan Proposisi 7.2.4 maka, $J^* = J/I$ untuk beberapa ideal J di R yang memenuhi $I \subseteq J \subseteq R$. Karena I adalah suatu ideal maksimal maka $J = I$ dalam kasus ini $J^* = \{0\}$ atau $J = R$ dalam kasus ini $J^* = R/I$. Jadi R/I adalah suatu lapangan. ●

Akibat 7.2.2 Dalam suatu ring komutatif disertai elemen satuan, setiap ideal maksimal adalah ideal prima.

Bukti Bila I adalah suatu ideal maksimal di R, maka R/I adalah suatu lapangan. Setiap lapangan adalah suatu daerah integral, jadi R/I adalah daerah integral. Dengan demikian I adalah suatu ideal prima. ●

Contoh 7.2.13 Misalkan $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ adalah suatu ring homomorpisma didefinisikan oleh $\phi(m, n) = n, \quad \forall (m.n) \in \mathbb{Z} \times \mathbb{Z}$. Maka $\ker(\phi) = \mathbb{Z} \times \{0\}$ dengan menggunakan Teorema 7.2.2 didapat

$$(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times \{0\}) \cong \mathbb{Z}$$

yang merupakan daerah integral, tetapi bukan suatu lapangan. Hal ini sesuai dengan bahasan dalam Contoh 7.2.12 bahwa $\mathbb{Z} \times \{0\}$ adalah suatu ideal prima tetapi bukan suatu ideal maksimal. ●

Contoh 7.2.14 Misalkan $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}_3$ adalah homomorpisma ring didefinisikan oleh

$$\phi(m, n) = [n]_3, \quad \forall (m, n) \in \mathbb{Z} \times \mathbb{Z}.$$

Maka $\ker(\phi) = \mathbb{Z} \times 3\mathbb{Z}$ dan $(\mathbb{Z} \times \mathbb{Z})/(\mathbb{Z} \times 3\mathbb{Z}) \cong \mathbb{Z}_3$ yang mana adalah suatu lapangan. Jadi $\mathbb{Z} \times 3\mathbb{Z}$ adalah suatu ideal maksimal di $\mathbb{Z} \times \mathbb{Z}$. ●

Teorema 7.2.5 memberikan suatu korespondensi diantara ideal-ideal prima atau ideal-ideal maksimal. Disamping itu juga, ring-ring kuasi yang merupakan daerah integral atau lapangan. Dalam bab berikutnya, teorema tersebut terlihat sangat penting sebagai dasar untuk pengkonstruksian contoh-contoh baru dari daerah integral dan lapangan.

Latihan

7.3 Lapangan Pecahan

Ring dari himpunan bilangan bulat $\mathbb{Z}$ adalah contoh dasar dari suatu daerah integral yang bukan lapangan. Hanya elemen -1 dan 1 yang merupakan elemen unit dalam $\mathbb{Z}$. Apapun itu, diketahui bahwa invers terhadap perkalian dari elemen-elemen bilangan bulat taknol yang lain ada diluar $\mathbb{Z}$ yaitu elemen-elemen di $\mathbb{Q}$ yang merupakan lapangan dari himpunan bilangan rasional. Dalam bagian ini dibahas hubungan yang mirip diantara $\mathbb{Z}$ dan $\mathbb{Q}$. Diamati pengkonstruksian $\mathbb{Q}$ dari $\mathbb{Z}$ yang merupakan fakta bahwa $\mathbb{Z}$ adalah daerah integral. Pengamatan ini mengijinkan untuk mengkonstruksi suatu lapangan melalui sebarang daerah integral sebagai mana cara lapangan $\mathbb{Q}$ dikonstruksi melalui $\mathbb{Z}$.

Contoh 7.3.1 Dibahas pengkonstruksian lapangan dari himpunan bilangan rasional $\mathbb{Q}$ dari ring himpunan bilangan bulat $\mathbb{Z}$. Untuk memulainya, ditinjau himpunan semua ungkapan pecahan S dari pembilang dan penyebut yang merupakan bilangan bulat:

$$S = \left\{ \frac{a}{b} \,\middle|\, a, b \in \mathbb{Z} \text{ dan } b \neq 0 \right\}.$$

Untuk memperoleh semua bilangan rasional dari S dibutuhkan perhitungan fakta bahwa suatu bilangan rasional dapat disajikan oleh banyak pecahan yang berbeda. Misalnya

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \frac{4}{8} = \frac{5}{10} = \frac{6}{12} \cdots$$

Perlu diperhatikan bahwa kondisi $a/b = c/d$ adalah ekivalen dengan $ad = bc$.

(1) Pada himpunan S, didefinisikan suatu relasi "$\sim$" oleh

$$\frac{a}{b} \sim \frac{c}{d} \qquad \text{bila dan hanya bila} \qquad ad = bc.$$

Dapat ditunjukkan bahwa relasi "$\sim$" adalah suatu relasi ekivalen sebagaimana berikut.

(i) Karena $ab = ba$, maka $\frac{a}{b} \sim \frac{a}{b}$.

(ii) Bila $\frac{a}{b} \sim \frac{c}{d}$, maka $ad = bc$. Hal ini berkibat bahwa $cb = da$, jadi $\frac{c}{d} \sim \frac{a}{b}$.

(iii) Bila

$$\frac{a}{b} \sim \frac{c}{d} \qquad \text{dan} \qquad \frac{c}{d} \sim \frac{e}{f},$$

maka $ad = bc$ dan $cf = de$. Hal ini berakibat bahwa

$$0 = bcf - bcf = (ad)f - b(ed) = (af - be)d$$

Karena $d \neq 0$ dan $\mathbb{Z}$ tidak memuat pembagi nol, maka $af = be$ atau $\frac{a}{b} \sim \frac{e}{f}$. Terlihat bahwa "$\sim$" adalah relasi ekivalen.

Ketika ditulis bilangan rasional 1/2 apa yang dimaksud dengan klas ekivalen [1/2] dengan cara yang sama untuk bilangan rasioanl lainnya, misalnya

$$\left[\frac{3}{5}\right] = \left\{ \frac{3k}{5k} \,\middle|\, k \in \mathbb{Z}, k \neq 0 \right\}.$$

Dengan demikian himpunan semua bilangan rasional dapat digambarkan sebagai himpunan klas ekivalen

$$\mathbb{Q} = \left\{ [\frac{a}{b}] \,\middle|\, a, b \in \mathbb{Z}, b \neq 0 \right\}.$$

(2) Operasi pada $\mathbb{Q}$ diberikan sebagai berikut

$$[\frac{a}{b}] + [\frac{c}{d}] = [\frac{ad + bc}{bd}] \qquad \text{dan} \qquad [\frac{a}{b}].[\frac{c}{d}] = [\frac{ac}{bd}].$$

Operasi yang diberikan adalah terdefinisi secara baik (well defined). Dengan kata lain operasi tersebut hasilnya adalah bebas dari pilihan penyajian yang diberikan dalam klas ekivalen dan untuk memudahkan pengoperasiannya penulisan $[\frac{a}{b}]$ ditulis sebegai $\frac{a}{b}$. Bila

$$\frac{a}{b} = \frac{a'}{b'} \qquad \text{dan} \qquad \frac{c}{d} = \frac{c'}{d'},$$

maka $ab' = a'b$ dan $cd' = c'd$. Didapat

$$\begin{aligned} (ad + bc)(b'd') &= (ab')dd' + bb'(cd') \\ &= (a'b)dd' + bb'(c'd) \\ &= (a'd' + b'c')(bd) \\ &= (bd)(a'd' + b'c'). \end{aligned}$$

Hal ini menunjukkan bahwa

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'} = \frac{a'}{b'} + \frac{b'}{d'},$$

dengan demikian menunjukkan bahwa operasi penjumlahan adalah well defined. Juga didapat $acb'd' = a'c'bd$ atau $\frac{ac}{bd} \sim \frac{a'c'}{b'd'}$. Terlihat bahwa perkalian juga well defined.

(3) Elemen nol di $\mathbb{Q}$ adalah $[\frac{0}{b}]$ atau ditulis $\frac{0}{b}$ dengan $0 \neq b \in \mathbb{Z}$ dan invers dari $\frac{a}{b}$ terhadap operasi "tambah" adalah $-\frac{a}{b}$. Elemen satuan di $\mathbb{Q}$ adalah $\frac{a}{a}$ untuk $a \neq 0$ dan untuk $a \neq 0$ invers dari $\frac{a}{b}$ terhadap operasi "perkalian" adalah $\frac{b}{a}$. Ring $\mathbb{Z}$ isomorpik dengan subring dari $\mathbb{Q}$ yang mempunyai elemen-elemen berbentuk $\frac{a}{1}$ untuk $s \in \mathbb{Z}$. ●

Pembahasan mengenai lapangan $\mathbb{Q}$ merupakan suatu petunjuk untuk pengkosntruksian suatu lapangan yang demikian melalui sebarang daerah integral.

Lemma 7.3.1 Misalkan D adalah suatu daerah integral dan misalkan

$$S = \{(a,b) \,|\, a,b \in D, b \neq 0\}.$$

Didefinisikan suatu relasi pada S oleh

$$(a,b) \sim (c,d) \qquad \text{bila dan hanya bila} \qquad ad = bc.$$

Maka $\sim$ adalah suatu relasi ekivalen.

Bukti

(1) (**Refleksif**) $(a,b) \sim (a,b)$ sebab $ab = ba$ hal ini karena D adalah ring komutatif.

(2) (**Simetri**) Bila $(a,b) \sim (c,d)$, maka $ad = bc$ yang berakibat bahwa $cd = da$ karena D adalah ring komutatif. Dengan demikian $(c,d) \sim (a,b)$.

(3) (**Transitif**) Bila $(a,b) \sim (c,d)$ dan $(c,d) \sim (e,f)$, maka $ad = bc$ dan $cf = de$. Jadi, $adf = bcf = bde$ dan karena perkalian adalah komutatif, maka $(af)d = (be)d$. Karena $(c,d) \sim S$ dan $d \neq 0$, juga D adalah daerah integral yaitu tidak memuat pembagi nol maka didapat $af = be$. Dengan demikian $(a,b) \sim (e,f)$. ✓

Catatan bahwa fakta D adalah suatu ring komutatif dan tidak mempunyai pembagi nol digunakan untuk membuktikan bahwa $\sim$ adalah relasi ekivalen. Relasi ekivalen $\sim$ mempartisi himpunan S kedalam klas ekivalen yang saling asing. Seperti halnya pembahasan lapangan pecahan $\mathbb{Q}$, untuk menjadikan notasi lebih intuitif, maka sebarang elemen $(a,b) \in S$ klas ekivalenya adalah $[(a,b)]$ dinotasikan oleh $\frac{a}{b}$. Sehingga didapat

$$\frac{a}{b} = \frac{c}{d} \quad \text{bila dan hanya bila} \quad ad = bc.$$

Selanjutnya ditinjau himpunan

$$F = \left\{ \frac{a}{b} \,\middle|\, a,b \in D, b \neq 0 \right\}.$$

Agar supaya himpunan $\mathbb{F}$ adalah suatu lapangan, didefinisikan dua operasi dalam $\mathbb{F}$.

Lemma 7.3.2 Untuk sebarang elemen $\frac{a}{b}, \frac{c}{d} \in \mathbb{F}$ dua operasi yang didefinisikan berikut adalah ekivalen:

(1) **Penjumlahan**

$$\frac{a}{b} + \frac{c}{d} \stackrel{\text{def}}{=} \frac{ad + bc}{bd}.$$

(2) **Perkalian**

$$\frac{a}{b}.\frac{c}{d} \stackrel{\text{def}}{=} \frac{ac}{bd}.$$

Bukti Perluh diingat bahwa $ad + bc$ dan ac keduanya di D dan karena D adalah suatu daerah integral dan $b \neq 0, d \neq 0$, maka $bd \neq 0$. Jadi masing-masing bagian kanan persamaan dalam (1) dan (2) adalah suatu elemen di $\mathbb{F}$.

(1) Misalkan $\frac{a}{b} = \frac{a'}{b'}$ dan $\frac{c}{d} = \frac{c'}{d'}$. Untuk menunjukkan bahwa **penjumlahan** adalah well defined, perlu ditunjukkan bahwa

$$\frac{ad + bc}{bd} = \frac{a'd' + b'c'}{b'd'}$$

atau dengan kata lain

$$b'd'(ad + bc) = bd(a'd' + b'c').$$

Karena $ab' = a'b$ dan $cd' = c'd$ dan menggunakan fakta bahwa D adalah suatu ring komutatif didapat

$$\begin{aligned} b'd'(ad + bc) &= (b'd')ad + (b'd')bc \\ &= (ab')d'd + (cd')b'b \\ &= (a'b)d'd + (c'd)b'b \\ &= (bd)a'd' + (bd)c'b' \\ &= bd(a'd' + c'b'). \end{aligned}$$

Terlihat bahwa menghasilkan sesuai yang diharapkan.

(2) Misalkan bahwa $\frac{a}{b} = \frac{a'}{b'}$ dan $\frac{c}{d} = \frac{c'}{d'}$. Untuk menunjukkan bahwa **perkalian** adalah well defined perlu ditunjukkan bahwa

$$\frac{ac}{bd} = \frac{a'c'}{b'd'},$$

atau dengan kata lain,

$$(b'd')(ac) = (bd)(a'c').$$

Karena $ab' = a'b$ dan $cd' = c'd$ dengan menggunakan fakta bahwa D adalah ring komutatif didapat

$$\begin{aligned} (b'd')(ac) &= (ab')(cd') \\ &= (a'b)(cd') \\ &= (a'b)(c'd) \\ &= (bd)(a'c'). \end{aligned}$$

Lemma 7.3.2 menjelaskan bahwa dua operasi **penjumlhan** dan **perkalian** dalam $\mathbb{F}$ adalah well defined. Berkutnya ditunjukkan bahwa $\mathbb{F}$ dengan dua operasi tersebut adalah suatu lapangan.

Lemma 7.3.3 Himpunan $\mathbb{F}$ sebagaimana telah didefinisikan sebelumnya adalah suatu lapangan terhadap operasi **penjumlahan** dan **perkalian**.

Bukti

(1) Penjumlhan di $\mathbb{F}$ adalah assosiatif:

$$\begin{aligned}\frac{a}{b}+\left(\frac{c}{d}+\frac{e}{f}\right) &= \frac{a}{b}+\frac{cf+ed}{df}\\ &= \frac{a(df)+(cf+ed)b}{b(df)}\\ &= \frac{(ad+cb)f+e(db)}{(bd)f}\\ &= \frac{ad+bc}{bd}+\frac{e}{f}\\ &= \left(\frac{a}{b}+\frac{c}{d}\right)+\frac{e}{f}.\end{aligned}$$

(2) Penjumlahan di $\mathbb{F}$ adalah komutatif:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd}=\frac{cb+da}{db}=\frac{c}{d}+\frac{a}{b}.$$

(3) Elemen $\frac{0}{1}$ adalah elemen nol terhadap penjumlahan:

$$\frac{0}{1}+\frac{a}{b}=\frac{0.b+a.1}{1.b}=\frac{a}{b}=\frac{a.1+0.b}{1.b}=\frac{a}{b}+\frac{0}{1}.$$

Catatan bahwa $\frac{0}{1}=\frac{0}{c}$ untuk semua $c\neq 0$.

(4) Elemen invers dari $\frac{a}{b}$ terhadap penjumlahan adalah $-\frac{a}{b}$:

$$\frac{a}{b}+\frac{-a}{b}=\frac{ab-ba}{b.b}=\frac{0}{bb}=\frac{0}{1}.$$

Terlihat bahwa $\mathbb{F}$ adalah grup komutatif terhadap operasi penjumlahan. Lima sifat berikutnya ini dapat dibuktikan sebagai latihan.

(5) Perkalian dalam $\mathbb{F}$ adalah assosiatif.

(6) Hukum distributif dipenuhi dalam $\mathbb{F}$.

(7) Perkalian dalam $\mathbb{F}$ adalah komutatif.

(8) Elemen $\frac{1}{1}$ adalah elemen identitas terhadap perkalian. Catatan bahwa $\frac{1}{1}=\frac{a}{a}$ untuk semua $a\neq 0$.

(9) Bila $\frac{a}{b}\neq 0$ di $\mathbb{F}$, maka $a\neq 0$ di D dan $\frac{b}{a}$ adalah invers dari $\frac{a}{b}$ terhadap operasi perkalian. ∎

Lemma 7.3.4 Himpunan $D' = \left\{\frac{a}{1} \mid a \in D\right\}$ adalah subring dari $\mathbb{F}$ dengan $D' \cong D$.

Bukti Karena $\frac{a}{1} - \frac{b}{1} = \frac{a-b}{1} \in D'$ dan $\frac{a}{1}\frac{b}{1} = \frac{ab}{1} \in D'$, maka D' adalah subring dari $\mathbb{F}$. Misalkan $\phi : D \to D'$ didefinisikan oleh $\phi(a) = \frac{a}{1}$, $\forall a \in D$. Maka

$$\begin{aligned} \phi(a+b) &= \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \phi(a) + \phi(b) \\ \phi(ab) &= \frac{ab}{1} = \frac{a}{1}\frac{b}{1} = \phi(a)\phi(b). \end{aligned}$$

Jadi ϕ adalah suatu homomorpisma ring. Pemetaan ϕ jelas pada dan satu-satu. Sebab, $\phi(a) = \phi(b)$ berarti bahwa $\frac{a}{1} = \frac{b}{1}$, maka $a.1 = 1.b$ dan $a = b$. Jadi ϕ adalah suatu isomorpisma ring.

Teorema 7.3.1 ***(Existence dari lapangan pecahan)*** Misalkan D adalah suatu daerah integral. Maka ada suatu lapangan $\mathbb{F}$ yang berisi pecahan $\frac{a}{b}$ dimana $a, b \in D$ dan $b \neq 0$. Lagipula, dapat diidentifikasi setiap elemen $a \in D$ dengan elemen $\frac{a}{1} \in F$, maka D menjadi suatu subring dari $\mathbb{F}$ dan masing-masing elemen dari $\mathbb{F}$ mempunyai bentuk $\frac{a}{b} = ab^{-1}$ dimana $a, b \in D$ dan $b \neq 0$.

Bukti Suatu yang hanya belum ditunjukkan adalah untuk semua $\frac{a}{b} \in F$ didapat $\frac{a}{b} = ab^{-1}$. Tetapi hal ini jelas, sebab

$$\frac{a}{b} = \frac{a}{1}.\frac{1}{b} = \frac{a}{1}.\left(\frac{b}{1}\right)^{-1}.$$

Jadi bila diidentifikasi setiap elemen $x \in D$ dengan $\frac{x}{1} \in F$, didapat $\frac{a}{b} = ab^{-1}$.

Definisi 7.3.1 Sebarang lapangan $\mathbb{F}$ dalam Teorema 7.3.1 dinamakan **lapangan pecahan** dari daerah integral D.

Dari pengkonstruksian lapangan pechan $\mathbb{F}$ dapat terlihat bahwa $\mathbb{F}$ terdiri dari elemen-elemen asli dari D, elemen-elemen invers dari D terhadap perkalian dan hasil perkalian elemen-elemen dari D dengan elemen-elemen invers dari D terhadap perkalian. Dengan kata lain, $\mathbb{F}$ diperoleh melalui menambahkan minimum kebutuhan mutlak untuk memperluas D menjadi suatu lapangan. Teorema berikut bahkan menunjukkan bahwa $\mathbb{F}$ adalah lapangan terkecil yang memuat D dan bahwa sebarang dua lapangan pecahan dari D harus isomorpik.

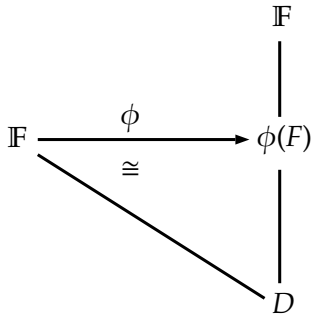
Teorema 7.3.2 Misalkan $\mathbb{F}$ adalah lapangan pecahan dari suatu daerah integral D dan E adalah sebarang lapangan yang memuat D. Maka ada suatu homomorpisma ring $\phi : F \to E$ yang memenuhi ϕ adalah pemetaan satu-satu dan $\phi(a) = a$ untuk semua $a \in D$.

Bukti Definisikan ϕ sebagai berikut. Untuk sebarang $a \in D$, misalkan $\phi(a) = a$ dan untuk sebarang $ab^{-1} \in F$, misalkan

$$\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} \in E.$$

Catatan bahwa karena $b \neq 0$ di D, maka $\phi(b) = b \neq 0$ di E. Pemetaan ϕ adalah well defined, sebab bila $ab^{-1} = cd^{-1}$ di $\mathbb{F}$, maka $ad = bc$ di D dan karena ϕ adalah pemetaan identitas pada D, di D maka

$$\phi(a)\phi(d) = ad = bc = \phi(b)\phi(c) \in E.$$



Dapat diselidiki bahwa ϕ adalah suatu homomorpisma ring. Pemetaan ϕ adalah satu-satu, sebab bila $\phi(ab^{-1}) = \phi(cd^{-1})$ maka

$$\phi(a)\phi(d) = \phi(b)\phi(c) \in E$$

jadi $ad = bc$. Akibatnya $ab^{-1} = cd^{-1}$ di $\mathbb{F}$. ✓
Catatan bahwa dalam bukti teorema yang baru saja dibahas, setiap elemen dari sub-lapangan $\phi(F) \subseteq E$ mempunyai bentuk $\phi(a)\phi(b)^{-1}$, yaitu adalah suatu elemen pecahan dari D di E.

Akibat 7.3.1 Setiap lapangan yang memuat daerah integral D memuat suatu lapangan pecahan dari D.

Bukti Langsung dari hasil Teorema 7.3.2 dan dari beberapa catatan. ✓

Akibat 7.3.2 (**Ketunggalan dari Lapangan Pecahan**) Sebarang dua lapangan pecahan dari suatu daerah integral D adalah isomorpik.

Bukti Misalkan $\mathbb{F}$ dan $\mathbb{F}'$ adalah dua lapangan pecahan dari daerah integral D. Hal ini berarti bahwa, setiap elemen dari $\mathbb{F}'$ berbentuk $ab^{-1} \in \mathbb{F}'$ untuk $a, b \in D$ dengan $b \neq 0$. Oleh karena itu, $\mathbb{F}' = \phi(\mathbb{F})$ dimana ϕ sebagaimana diberikan dalam bukti Teorema 7.3.2. Jadi $\mathbb{F}' \cong \mathbb{F}$. ✓

Diringkas apa yang baru saja telah dibahas tersebut tentang lapangan pecahan $\mathbb{F}$ dari suatu daerah integral D.
Misalkan D suatu daerah integral. Maka

(1) Lapangan pecahan $\mathbb{F}$ dari D adalah **ada** .

(2) Lapangan pecahan $\mathbb{F}$ dari D adalah tunggal dalam arti isomorpik.

(3) Himpunan $\mathbb{F} = \{\frac{a}{b} \mid a, b \in D, b \neq 0\}$.

(4) Bila $\mathbb{E}$ adalah suatu lapangan yang memuat D yatitu $D \subseteq \mathbb{E}$, maka ada suatu sub-lapangan $\mathbb{F}' \subseteq \mathbb{E}$ dengan $\mathbb{F} \cong \mathbb{F}'$. Hal ini menyatakan bahwa $\mathbb{F}$ adalah lapangan terkecil yang memuat D.

Untuk mengakhiri sub-bagian ini, dibicarakan lagi konsep karakteristik dari suatu daerah integral yang telah dibahas. Sudah dikembangkan beberapa alat baru yang mengijikan

untuk menghargai pentingnya karakteristik. Ditunjukkan bahwa $\mathbb{Q}$ dan $\mathbb{Z}_p$ dengan p adalah prima merupakan lapangan terkecil dari karakteristiknya. Sebagaimana nantinya dalam bagian berikutnya ditunjukkan bahwa, sebarang lapangan yang lain adalah suatu perluasan dari lapangan-lapangan terkecil tersebut.

Teorema 7.3.3 Misalkan D adalah suatu daerah integral. Ada suatu sub-daerah $D' \subseteq D$ yang memenuhi

(1) bila khar$(D) = 0$, maka $\mathbb{Z} \cong D' \subseteq D$.

(2) Bila khar$(D) = p$, maka $\mathbb{Z}_p \cong D' \subseteq D$.

Bukti Misalkan $D' = \{m.1' \mid m \in \mathbb{Z}\}$ dimana $1'$ adalah elemen satuan di D' dan tinjau pemetaan $\phi : \mathbb{Z} \to D'$ didefinisikan oleh $\phi(n) = n.1'$, $\forall n \in \mathbb{Z}$. Pemetaan ϕ adalah suatu homomorpisma ring, sebab

$$\begin{aligned} \phi(n+m) &= (n+m).1' = n.1' + m.1' = \phi(n) + \phi(m) \\ \phi(nm) &= (nm).1' = (nm).(1'.1') = (n.1')(m.1') = \phi(n)\phi(m), \end{aligned}$$

dengan menggunakan Teorema 6.1.1 bagian (6).

(1) Bila khar$(D) = 0$, maka menggunakan Teorema 6.3.7, untuk semua bilangan bulat positip $m \in \mathbb{Z}$ didapat $m.1' \neq 0$. Dalam hal ini, didapat $\ker(\phi) = \{0\}$ dan ϕ adalah pemetaan satu-satu dan $\mathbb{Z} \cong \phi(\mathbb{Z}) = D' \subseteq D$.

(2) Bila khar$(D) = p$, lagi gunakan Teorema 6.3.7, maka $|1'| = p$ dan $\ker(\phi) = p\mathbb{Z} \subseteq \mathbb{Z}$. Jadi, dengan menggnakan Teorema didapat $\mathbb{Z}/p\mathbb{Z} \cong \phi(\mathbb{Z}) = D' \subseteq D$, dengan demikian $\mathbb{Z}_p \cong D'$.

Catatan bahwa untuk kasus D' adalah image dari suatu ring terhadap suatu homomorpisma ring dengan Proposisi 7.1 bagian (2), maka D' adalah suatu subring dari D. Karena $1' \in D'$, maka dengan menggunakan Proposisi 6.2.1 D' adalah suatu sub-daerah dari D. ✓

Hasil berikut adalah akibat dari teorema yang baru dibahas, merupakan teorema untuk lapangan dan begitu penting.

Teorema 7.3.4 Misalkan $\mathbb{F}$ adalah suatu lapangan. Maka ada suatu sub-lapangan $\mathbb{F}' \subseteq \mathbb{F}$ yang memenuhi:

(1) Bila khar$(F) = 0$, maka $\mathbb{Q} \cong \mathbb{F}' \subset \mathbb{F}$.

(2) Bila khar$(F) = 0$, maka $\mathbb{Z}_p \cong \mathbb{F}' \subset \mathbb{F}$.

Bukti

(1) Bila khar$(\mathbb{F}) = 0$, maka karena $\mathbb{F}$ juga merupakan daerah integral, dengan menggunakan Teorema 7.3.3 didapat $\mathbb{Z} \cong D' = \{n.1' \mid n \in \mathbb{Z}\} \subseteq \mathbb{F}$, dimana $1'$ elemen satuan di $\mathbb{F}$, D' adalah suatu daerah integral termuat di $\mathbb{F}$, dengan demikian menggunakan Akibat 7.3.1 lapangan $\mathbb{F}$ memuat lapangan pecahan F' dari daerah integral D'. Karena $\mathbb{Z} \cong D' \subseteq F$, maka $\mathbb{Q} \cong F' \subset F$.

(2) Hal ini langsung dari Teorema 7.3.3. ✓

Baru saja telah dibuktikan bahwa $\mathbb{Q}$ adalah lapangan terkecil yang mempunyai karakteristik nol. Dengan kata lain, setiap lapangan berkarakteristik nol memuat suatu sub-lapangan yang isomorpik dengan $\mathbb{Q}$. Dalam hal mempunyai karakteristik p, maka lapangan terkecilnya isomorpik dengan $\mathbb{Z}_p$.

Definisi 7.3.2 Lapangan $\mathbb{Q}$ dan $\mathbb{Z}_p$ dinamakan **lapangan prima**. ●

Dalam pembahasan berikutnya, lapangan prima adalah suatu dasar dari semua lapangan-lapangan yang lainnya dibentuk.

Latihan

Bab 8

Polinomial Ring

Dalam bab ini dibahas polinomial dengan koefisien dalam suatu ring, mengkonstruksi *polinomial ring* $R[x]$ dan membahas sifat-sifatnya. Dalam suatu hal khusus yang penting dimana ring R juga merupakan suatu lapangan $\mathbb{F}$. Polinomial ring $\mathbb{F}[x]$ ternyata memiliki banyak sifat yang sama dengan ring himpunan bilangan bulat $\mathbb{Z}$. Misalkan bahwa diberikan dua daerah integral yang keduanya bukan lapangan. Sebagaimana telah diketahui dalam keduanya berlaku algoritma pembagian. Nantinya ditemukan juga bahwa ada kesamaan penting antara ideal di $\mathbb{F}[x]$ dan di di $\mathbb{Z}$.

8.1 Konsep Dasar dan Notasi

Pada bagian ini dikonstruksi ring polinomial dengan koefisien di suatu ring tetap R dan diberikan beberapa definisi dasar dan sifat. Contoh pertama menggambarkan pentingnya ring R yang mana elemen-elemennya adalah koefisien dari polinomial.

Contoh 8.1.1 Menentukan akar-akar dari suatu polinomial adalah suatu masalah klasik dalam aljabar. Misalnya diberikan polinomial $(x) = x^2 + x + 1$. Jika ditanyakan akar-akar polinomial $f(x)$ pertanyaannya adalah tidak lengkap, sebagai ditujukkan berikut ini:

(1) Bila koefisien dari polinomial adalah di ring himpunan bilangan riil $\mathbb{R}$, maka $f(x)$ tidak memiliki akar riil.

(2) Bila koefisien dari polinomial adalah di ring $\mathbb{Z}_3$, maka $f(x) = x^2 + x + 1 = (x-1)^2$. Jadi, $f(1) = 0$, dengan demikian hanyalah $1 \in \mathbb{Z}_3$ yang merupakan akar dari $f(x)$.

(3) Bila koefisien dari polinomial adalah di ring $\mathbb{Z}_7$, maka $f(x) = x^2 + x + 1 = (x-2)(x-4)$. Jadi, $f(2) = 0$ dan $f(4) = 0$, dengan demikian $2, 4 \in \mathbb{Z}_7$ adalah dua akar yang berbeda dari $f(x)$. ●

Jadi ketika bekerja dengan polinomial, harus selalu diperhatikan ring yang digunakan dalam koefisien suatu polinomial.

Contoh 8.1.2 Diberikan polinomial $f(x) = x^2 + 8$.

(1) Polinomial $f(x)$ tidak mempunyai akar-akar di $\mathbb{R}$ hal ini mudah diselidiki.

(2) Dalam $\mathbb{Z}_{11}$, $f(x) = x^2 + 8 = x^2 - 3 = (x-5)(x-6)$ dengan demikian $f(x)$ mempunyai dua akar $5, 6 \in \mathbb{Z}_{11}$.

(3) Dalam $\mathbb{Z}_{12}$, $f(x) = x^2 + 8 = x^2 - 4 = (x-2)(x-10) = (x-4)(x-8)$ dengan demikian $f(x)$ mempunyai empat akar $2, 10, 4, 8 \in \mathbb{Z}_{12}$.

Berikut ini diberikan definisi polinomial yang berguna untuk pembahasan aksioma ring berikutnya. Namum sebelumnya dibahas suatu pertanyaan mengenai subring himpunan bilangan bulat $\mathbb{Z}$ dari ring himpunan bilangan kompleks $\mathbb{C}$ yang berkaitan dengan pengertian polinomial secara umum. Satu elemen di $\mathbb{C}$ yang bukan di $\mathbb{Z}$ adalah bilangan irrasional $\pi = 3.14159....$ Bila π digabungkan dengan $\mathbb{Z}$, bilangan lain apa yang harus tercakup supaya didapat suatu ring? Pertanyaan ini dijawab sebagai berikut. Misalkan S adalah suatu subring dari $\mathbb{C}$ sebagaimana dinginkan untuk menjawab pertanyaan. Jadi S memuat π dan semua bilangan bulat (subring $\mathbb{R}$ dari ring $\mathbb{C}$ adalah memenuhi yang diharapakan dalam S, tetapi apakah tepat memang $\mathbb{R} = S$?). Karena S tertutup terhadap perkalian, maka pangkat dari π: $\pi, \pi^2, \pi^3, \ldots$ juga berada di S dan juga $a\pi^n$ di S untuk setiap bilangan bulat $a \in \mathbb{Z}$ dan bilangan bulat taknegatif n. Karena S tertutup terhadap penjumlahan, maka S memuat semua bilangan yang berbentuk

$$\alpha = a_0 + a_1\pi + \cdots + a_{n-1}\pi^{n-1} + a_n\pi^n, \quad a_i \in \mathbb{Z}. \tag{8.1}$$

Himpunan yang memuat bentuk (8.1) dinotasikan sebagai $\mathbb{Z}[\pi]$, dengan demikian jelas bahwa $S = \mathbb{Z}[\pi]$ dan dapat ditunjukkan bahwa $\mathbb{Z}[\pi]$ adalah suatu ring.

Definisi 8.1.1 Misalkan R adalah suatu ring. Suatu **polinomial** dengan koefisien di $\mathbb{R}$ dan peubah (indeterminate) x adalah suatu jumlahan berhingga

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0x^0 + a_1x^1 + a_2x^2 + \cdots + a_{n-1}x^{n-1} + a_nx^n,$$

dimana $a_i \in R$ untuk $i \in \mathbb{Z}$ dengan $0 \leq i \leq n$. Nilai-nilai a_i dinamakan **koefisien** dari polinomial. Dalam hal khusus dimana semua koefisien adalah nol, maka polinomial dinamakan **polinomial nol** dan ditulis $f(x) = 0$. Himpunan semua polinomial dengan koefisien di R dan indetermine x dinotasikan oleh $R[x]$

Dua polinomial tepat sama bila koefisien yang bersesuaian sama yaitu

$$\begin{aligned} f(x) &= a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + a_nx^n \\ g(x) &= b_0 + b_1x + \cdots + b_{m-1}x^{m-1} + b_mx^m, \end{aligned}$$

maka $f(x) = g(x)$ bila dan hanya bila $a_i = b_i$ untuk semua $i \geq 0$.

Dalam penulisan polinomial, ditulis a_1x untuk a_1x^1 dan a_0 untuk a_0x^0. Juga, umumnya sebarang a_ix^i yang ada dalam jumlahan dihilangkan bila $a_i = 0$ dan sebarang a_ix^i dengan $a_i = 1$ ditulis x^i begitu juga untuk a_ix^i dengan $a_i = -1$ ditulis $-x^i$. Contoh,

$$f(x) = 1x^3 + (-1)x^2 + 0x^1 + 1x^0 = x^3 - x^2 + 1.$$

Definisi 8.1.2 Misalkan R adalah suatu ring, $f(x) = a_0 + a_1x + \cdots + a_nx^n$ adalah suatu polinomial di $R[x]$ dan b suatu elemen di R. **Nilai** $f(b)$ untuk **argumen** b adalah elemen

$$a_0 + a_1b + \cdots + a_{n-1}b^{n-1} + a_nb^n \in R.$$

Fungsi polinomial ditentukan oleh $f(x)$ adalah fungsi dari R ke R dengan memberikan setiap argumen $b \in R$ ke nilai $f(b)$. Suatu argumen b yang mana nilai $f(b)$ dari polinomial $f(x)$ adalah nol dinamakan suatu **akar** dari polinomial $f(x)$ dan merupakan suatu **penyelesaian** dari **persamaan polinomial** $f(x) = 0$.

Polinomial tidak sama dengan fungsi polinomial. Kususnya dua polinomial tidak sama kecuali semua koefisiennya sama. meskipun bila polinomial-polinomial tersebut adalah fungsi polinomial yang sama. Contoh berikut memberikan gambaran apa yang dibahas.

Contoh 8.1.3 Misalkan $R = \mathbb{Z}_2$. Polinomial $f(x) = x + 1$ dan $g(x) = x^2 + 1$ adalah polinomial yang tidak sama. Sebab, f mempunyai koefisien $a_1 = 1, a_0 = 1$ sedangkan g mempunyai koefisien $b_2 = 1, b_1 = 0, b_0 = 1$. Tetapi, dengan mudah didapat $f(0) = 1 = g(0)$ dan $f(1) = 0 = g(1)$. Jadi, f dan g menentukan fungsi polinomial yang sama dari $\mathbb{Z}_2$ ke $\mathbb{Z}_2$.

Definisi 8.1.3 Misalkan $f(x)$ adalah suatu polinomial dengan indeterminate x dan koefisien a_i di suatu ring R. Untuk bilangan bulat positip n dengan $a_n \neq 0$ dinamakan derajad dari $f(x)$ ditulis $n = \deg(f(x))$ dan koefisien a_n dinamakan koefisien **utama (leading)**. Perlu diperhatikan bahwa pengertian dari derajad dan koefisien utama tidak terdefinisi untuk hal yang kusus polinomial nol. Bila derajad polinomial adalah nol, maka $f(x) = a_0$ adalah polinomial **konstan**. Setiap $a \in R$ dapat diidentifikasi dengan polinomial $f(x) = a$ dalam hal demikian ini R dapat dipandang sebagai subset dari $R[x]$. Masing-masing polinomial berderajad $1, 2, 3, 4$ dan 5 dinamakan polinomial **linier**, **kuadrat**, **kubik**, **kuartik** dan **kuintik**. Bila koefisien utama adalah 1, maka polinomialnya adalah

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$$

dan dinamakan polinomial **monik**.

Ditulis sebagai $R[x]$ untuk himpunan dari semua polinomial dalam indetermine x dengan koefisien di ring R. Dengan operasi tambah dan perkalian yang sesuai di $R[x]$ dibuat ring $R[x]$. Secara umum tidak dibedakan polinomial konstan a_0 di $R[x]$ dengan elemen a_0 di R, juga tidak dibedakan polinomial nol 0 di $R[x]$ dengan elemen nol 0 di R. Operasi penjumlahan dan perkalian pada $R[x]$ didefinisikan sesuai dengan operasi pada R, dengan demikian ring R merupakan subring dari ring $R[x]$.

Definisi 8.1.4 Bila $f(x), g(x) \in R[x]$ dimana $f(x) = \sum_{i=0}^{n} a_ix^i$ dan $g(x) = \sum_{i=0}^{m} b_ix^i$, maka didefinisikan jumlahan dan perkalian sebagai berikut:

(1) $f(x) + g(x) = \sum_{i=0}^{\max\{n,m\}} c_ix^i$, dimana $c_i = a_i + b_i$.

(2) $f(x).g(x) = \sum_{i=0}^{n+m} d_ix^i$, dimana

$$d_i = \sum_{k=0}^{i} a_kb_{i-k} = a_0b_i + a_1b_{i-1} + \cdots + a_{i-1}b_1 + a_ib_0.$$

Contoh 8.1.4 Diberikan $f(x) = x^3 + 2x^2 + 3x + 4$ dan $g(x) = 5x^2 + 6x + 7$ di $\mathbb{Z}[x]$. Maka $f(x).g(x) = \sum_{i=0}^{5} d_i x^i$ dimana
$d_0 = 4(7) = 28$
$d_1 = 3(7) + 4(6) = 45$
$d_2 = 2(7) + 3(6) + 4(5) = 52$
$d_3 = 1(7) + 2(6) + 3(5) = 34$
$d_4 = 1(6) + 2(5) = 16$
$d_5 = 1(5) = 5$.
Jadi, perkalian dari $f(x)g(x)$ adalah

$$f(x)g(x) = 5x^5 + 16x^4 + 34x^3 + 52x^2 + 45x + 28. \quad \bullet$$

Contoh 8.1.5 Misalkan polinomial $f(x)$ dan $g(x)$ seperti diberikan dalam Contoh 8.1.4, tetapi sekarang dalam $\mathbb{Z}_{10}[x]$. Maka

$$f(x)g(x) = 5x^5 + 6x^4 + 4x^3 + 2x^2 + 5x + 8. \quad \bullet$$

Menghitung derajad hasil kali dua polinomial dengan koefisien di $\mathbb{R}$ atau di $\mathbb{C}$ adalah jumlah masing-masing dari derajad polinomial tersebut. Tetapi hal ini tidak selalu benar untuk sebarang polinomial dengan koefisien disebarang ring R. Contoh berikut menjelaskan hal ini.

Contoh 8.1.6 Tinjau polinomial $f(x) = 2x^3$ dan $g(x) = 2x^2$ di $\mathbb{Z}_4[x]$. Maka $f(x)g(x) = 0$ adalah polinomial nol. $\bullet$

Suatu pertanyaan, kapan kita bisa menghitung derajad dari perkalian dua polinomial yang diberikan sama dengan jumlah dari masing-masing derajad dari polinomial tersebut? Dari dua contoh yang baru saja dibahas, dapat diterka jawabannya sebagaimana diberikan dalam bagian terakhir teorema berikut.

Teorema 8.1.1 Misalkan R adalah suatu ring. Maka dengan operasi jumlah dan perkalian sebagaimana telah diberikan dalam Definisi 8.1.4,

(1) $R[x]$ adalah suatu ring yang memuat ring R sebagai suatu subring.

(2) Bila R adalah suatu ring komutatif, maka $R[x]$ adalah ring komutatif.

(3) Bila R mempunyai elemen satuan 1, maka 1 juga merupakan elemen satuan di $R[x]$.

(4) Bila R adalah suatu daerah integral, maka $R[x]$ adalah daerah integral dan hasil perkalian dua polinomial taknol $f(x), g(x) \in R[x]$ memenuhi $\deg(f(x).g(x)) = \deg(f(x)) + \deg(g(x))$.

Bukti

(1) Operasi Penjumlahan Tertutup, sebab $f(x), g(x), h(x) \in R[x]$ didapat

$$f(x) + g(x) = \sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{\max\{m,n\}} c_i x^i,$$

dimana $c_i = a_i + b_i \in R$. Jadi $f(x) + g(x) \in R[x]$. Penjumlahan di $R[x]$ memenuhi asosiatif sebab

$$\begin{aligned}
(f(x) + g(x)) + h(x) &= \sum_{i=0}^{\max\{m,n\}} (a_i + b_i)x^i + \sum_{i=0}^{p} c_i x^i \\
&= \sum_{i=0}^{\max\{m,n,p\}} ((a_i + b_i) + c_i)x^i \\
&= \sum_{i=0}^{\max\{m,n,p\}} (a_i + (b_i + c_i))x^i \\
&= \sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{\max\{n,p\}} (c_i + b_i)x^i \\
&= f(x) + \left(\sum_{i=0}^{n} b_i x^i + \sum_{i=0}^{p} c_i x^i \right) \\
&= f(x) + (g(x) + h(x)).
\end{aligned}$$

Ada polinomial nol yaitu $O(x) = \sum_{i=0}^{m} 0\, x^i = 0$ yang memenuhi

$$\begin{aligned}
f(x) + O(x) &= \sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{m} 0\, x^i \\
&= \sum_{i=0}^{m} (a_i + 0)x^i \\
&= \sum_{i=0}^{m} a_i x^i = f(x),
\end{aligned}$$

juga

$$\begin{aligned}
O(x) + f(x) &= \sum_{i=0}^{m} 0\, x^i + \sum_{i=0}^{m} a_i x^i \\
&= \sum_{i=0}^{m} (0 + a_i)x^i \\
&= \sum_{i=0}^{m} a_i x^i = f(x).
\end{aligned}$$

Untuk setiap $f(x) \in R[x]$ ada invers dari $f(x)$, yaitu $-f(x) = \sum_{i=0}^{m}(-a_i)x^i$ yang memenuhi

$$f(x) + (-f(x)) = \sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{m}(-a_i)x^i = \sum_{i=0}^{m}(a_i - a_i)x^i = \sum_{i=0}^{m} 0\, x^i = O(x) = 0.$$

Penjumlahan polinomial adalah komutatif,

$$\begin{aligned} f(x) + g(x) &= \sum_{i=0}^{m} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{\max\{m,n\}} (a_i + b_i)x^i \\ &= \sum_{i=0}^{\max\{n,m\}} (b_i + a_i)x^i = \sum_{i=0}^{n} b_i x^i + \sum_{i=0}^{m} a_i x^i = g(x) + f(x). \end{aligned}$$

Jadi $R[x]$ terhadap operasi "+" memenuhi aksioma grup komutatif.

Terhadap operasi perkalian di $R[x]$ memenuhi sifat tertutup, sebab

$$f(x).g(x) = \left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{m+n} d_i x^i,$$

dimana $d_i = \sum_{k=0}^{i} a_k b_{i-k} \in R$ sebab $a_i, b_i \in R$. Jadi $f(x).g(x) \in R[x]$. Berikutnya, terhadap perkalian sebagaimana telah didefinisikan di ring $R[x]$ adalah asosiatif. Sifat asosiatif ini ditunjukkan sebagai berikut:

$$\begin{aligned} (f(x).g(x)).h(x) &= \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\ &= \left[\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j b_i - j\right)x^i\right]\left(\sum_{i=0}^{p} c_i x^i\right) \\ &= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i}\left(\sum_{k=0}^{j} a_k b_{j-k}\right)c_{i-j}\right]x^i \\ &= \sum_{i=0}^{m+n+p}\left(\sum_{j+k+l=i} a_j b_k c_l\right)x^i \\ &= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i} a_j\left(\sum_{k=0}^{i-j} b_k c_{i-j-k}\right)\right]x^i \\ &= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\sum_{i=0}^{n+p}\left(\sum_{j=0}^{i} b_j c_{i-j}\right)x^i\right] \\ &= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\left(\sum_{i=0}^{n} b_i x^i\right)\left(\sum_{i=0}^{p} c_i x^i\right)\right] \\ &= f(x)[g(x).h(x)]. \end{aligned}$$

Berlaku sifat distributif di $R[x]$,

$$\begin{aligned} f(x)(g(x)+h(x)) &= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\sum_{i=0}^{n} b_i x^i + \sum_{i=0}^{p} c_i x^i\right] \\ &= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\sum_{i=0}^{\max\{n,p\}} (b_i + c_i) x^i\right] \\ &= \sum_{i=0}^{m+\max\{n,p\}} \left(\sum_{j=0}^{i} a_j (b_{i-j} + c_{i-j})\right) x^i \\ &= \sum_{i=0}^{m+\max\{n,p\}} \left(\sum_{j=0}^{i} a_j b_{i-j} + a_j c_{i-j}\right) x^i \\ &= \sum_{i=0}^{m+n} \left(\sum_{j=0}^{i} a_j b_{i-j}\right) x^i + \sum_{i=0}^{m+p} \left(\sum_{j=0}^{i} a_j c_{i-j}\right) x^i \\ &= f(x).g(x) + f(x)h(x). \end{aligned}$$

Selanjutnya dibuat pemetaan inklusi dar ring R ke ring $R[x]$ yaitu $\iota : R \to R[x]$ didefinisikan oleh $\iota(r) = rx^0,\ \forall r \in R$. Ditunjukkan bahwa ι adalah suatu homomorpisma ring.
1. $\iota(r+q) = (r+q)x^0 = rx^0 + qx^0 = \iota(r) + \iota(q),\ \forall r, q \in R$.
2. $\iota(r.q) = (r.q)x^0 = (r.q)x^{0+0} = (rx^0).(qx^0) = \iota(r).\iota(q),\ \forall r, q \in R$.
Sebagaimana telah diketahui bahwa image $\iota(R)$ adalah subring dari $R[x]$ dan pemetaan ι adalah pemetaan satu-satu sebab bila $\iota(r) = \iota(q)$, maka $rx^0 = qx^0$. Hal ini berakibat $r = q$. Jadi ι adalah satu-satu. Dengan demikian $R \cong \iota(R)$. Karena $\iota(R)$ adalah subring dari $R[x]$ dan $R \cong \iota(R)$, maka R dapat dipandang sebagi subring dari $R[x]$ dengan identifikasi elemen-elemen di R sebagai elemen-elemen di $\iota(R)$ diberikan oleh $r \mapsto rx^0$.

(2) Bila R adalah ring komutatif, maka untuk sebarang $f(x), g(x)$ di $R[x]$ dengan $f(x) = \sum_{i=0}^{m} a_i x^i$ dan $g(x) = \sum_{i=0}^{n} b_i x^i$ didapat

$$\begin{aligned} f(x).g(x) &= \sum_{i=0}^{m+n} \left(\sum_{k=0}^{i} a_k b_{i-k}\right) x^i \\ &= \sum_{i=0}^{n+m} \left(\sum_{k=0}^{i} b_k a_{i-k}\right) x^i \\ &= g(x).f(x). \end{aligned}$$

Jadi $R[x]$ adalah ring komutatif.

(3) Dari hasil (1) R adalah subring dari $R[x]$. Jadi, bila $1 \in R$ adalah elemen satuan di R, maka $1 = 1.x^0$ dan untuk sebarang $f(x) = \sum_{i=0}^{m} a_i x^i \in R[x]$ didapat

$$1.x^0.f(x) = 1.x^0\left(\sum_{i=0}^{m} a_i x^i\right) = \sum_{i=0}^{0+m}(1.a_i)x^i = \sum_{i=0}^{m} a_i x^i = f(x).$$

Juga, didapat

$$f(x).1x^0 = \left(\sum_{i=0}^{m} a_i x^i\right)1.x^0 = \sum_{i=0}^{m+0}(a_i.1)x^i = \sum_{i=0}^{m} a_i x^i = f(x).$$

Jadi, elemen $1 = 1.x^0$ adalah elemen satuan di $R[x]$.

(4) Misalkan R daerah integral. Diberikan sebarang plinomial tak nol di $R[x]$

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{m-1}x^{m-1} + a_m x^m$$

dan

$$g(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_{n-1}x^{n-1} + b_n x^n,$$

dimana a_m dan b_n adalah koefisien utama dari masing-masing $f(x)$ dan $g(x)$. Jadi $a_m \neq 0$ dan $b_n \neq 0$, akibatnya $a_m b_n \neq 0$ (sebab R daerah integral). Sehingga didapat

$$f(x).h(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \cdots + (a_m b_n)x^{m+n},$$

$f(x).g(x) \neq 0$ sebab $a_m b_n \neq 0$. Jadi $R[x]$ adalah daerah integral. Juga, didapat

$$\deg(f(x).g(x)) = m + n = \deg(f(x)) + \deg(g(x)).$$

Contoh 8.1.7 Akan ditentukan semua unit di $\mathbb{Z}_3[x]$. Diberikan sebarang $0 \neq f(x) \in \mathbb{Z}_3[x]$ adalah unit di $\mathbb{Z}_3[x]$. Hal ini berarti dapat dipilih suatu $g(x) \in \mathbb{Z}_3[x]$ yang memenuhi $f(x).g(x) = 1 \in \mathbb{Z}_3[x]$. Dengan menggunakan Teorema 8.1.1 bagian (4), didapat

$$\deg(f(x)) + \deg(g(x)) = \deg(1) = 0.$$

Jadi, $f(x)$ adalah polinomial konstan. Maka dari itu, hanyalah $f(x) = 1$ dan $f(x) = 2$ yang merupakan unit di $\mathbb{Z}_3[x]$.

Proposisi 8.1.1 Misalkan D adalah daerah integral, maka elemen unit di $D[x]$ adalah tepat sama dengan elemen unit di D.

Bukti Misalkan $c \in D$ adalah sebarang unit di D dan $d \in D$ adalah invers dari c terhadap perkalian. Selanjutnya tinjau polinomial konstan $c, d \in D[x]$, maka hasil kali $cd \in D[x]$ adalah sama dengan hasil kali $cd \in D$. Hasil kali c dan d memenuhi $cd = 1$. Hal ini memperlihatkan bahwa $c \in D[x]$ adalah unit di $D[x]$ dan $d \in D[x]$ adalah invers dari c terhadap perkalian. Sebaliknya, bila $f(x)$ adalah sebarang unit di $D[x]$ dan misalkan $g(x) \in D[x]$ adalah invers dari $f(x)$ terhadap perkalian. Maka $f(x).g(x) = 1$, karena 1 berderajad nol, maka menurut Teorema 8.1.1 haruslah $\deg(f(x)) = 0$ dan $\deg(g(x)) = 0$. Jadi $f(x) = c_0$ dan $g(x) = d_0$. Lagipula, c_0 harus merupakan unit di D dengan d_0 adalah invers dari c_0 terhadap perkalian sebab $c_0.d_0 = f(x).g(x) = 1$.

Akibat 8.1.1 Bila $\mathbb{F}$ adalah suatu lapangan, maka $F[x]$ adalah daerah integral dan bukan lapangan.

Bukti Karena $\mathbb{F}$ lapangan, maka $\mathbb{F}$ adalah daerah integral dan berdasarkan Teorema 8.1.1 bagian (4) $F[x]$ adalah daerah integral. Dengan menggunakan Proposisi 8.1.1, semua polinomial konstan taknol di $F[x]$ adalah elemen-elemen taknol yang bukan unit. Jadi $F[x]$ bukan suatu lapangan.

Proposisi 8.1.2 Misalkan R adalah suatu ring. Maka $R[x]$ mempunyai karakteristik sama dengan karakteristik dari R.

Bukti Untuk sebarang bilangan bulat $n > 0$, na adalah $\overbrace{a + a + \cdots + a}^{n}$ dan

$$nf(x) = \overbrace{f(x) + f(x) + \cdots + f(x)}^{n}.$$

Menurut pengertian karakteristik, khar$(R[x])$ adalah bilangan bulat terkecil $n > 0$ yang memenuhi $nf(x) = 0$ untuk semua $f(x) \in R[x]$ dan bila tidak ada n yang demikian, maka $R[x]$ mempunyai karakteristik nol. Karena R termuat (sebagai subring) di $R[x]$, jelas bahwa bila $nf(x) = 0$, maka juga $na = 0$ untuk semua $a \in R$. Selanjutnya bila $na = 0$ untuk semua $a \in R$, maka untuk sebarang

$$f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{m-1} + a_mx^m \in R[x],$$

didapat

$$nf(x) = na_0 + na_1x + \cdots + na_{m-1}x^{m-1} + na_mx^m = 0 + 0x + \cdots + 0x^{m-1} + 0x^m = 0.$$

Contoh berikut menjelaskan pengkonstruksian beberapa daerah integral dari berbagai karakteristik berbeda yang bukan lapangan.

Contoh 8.1.8 (1) Mempunyai karakteristik 0: $\mathbb{Z}[x], \mathbb{Q}[x], \mathbb{R}[x], \mathbb{C}[x]$ adalah daerah integral yang bukan lapangan.

(2) Mempunyai karakterisktik p: untuk sebarang bilangan prima p, ring polinomial $\mathbb{Z}_p[x]$ adalah suatu daerah integral mempunyai karakteristik p yang bukan lapangan.

Pengkonstruksian polinomial ring dapat digeneralisasi pada lebih dari satu indeterminate.

Definisi 8.1.5 Dimulai dari ring R dan ditentukan satu indeterminate x dapat dibentuk ring $R[x]$. Selanjutnya ditentukan indeterminate yang lain yaitu y dapat dilakukan pembentukan ring $R[x][y]$ yang elemen-elemennya polinomial dalam y dengan koefisien di ring $R[x]$, misalnya:
(1) $(x + 2)y^2 + (x^3 + 2x)y + (x^2 + 1)$. Sebagai penggantinya, dapat dilakukan secara general untuk definisi suatu ring $R[x, y]$. Elemen-elemennya adalah jumlahan berhingga $\sum a_{i,j}x^iy^j$, misalnya:
(2) $xy^2 + 2y^2x^3y + 2xy + x^2 + 1$.
Hasil dari dua pengkonstruksian ini adalah ekivalen dan dapat dianggap sebagai **polinomial ring dari dua indeterminate** dengan koefisien di R.

Lebil general, dapat didefinisikan ring polinomial $R[x_1, \ldots, x_n]$ dengan n indeterminate $x_1, \ldots, x_n$. Juga, $R[x_1, \ldots, x_n]$ adalah daerah integral bila R adalah daerah integral.

Proposisi 8.1.3 Misalkan R suatu ring. Maka $R[x][y]$ dan $\mathbb{R}[x, y]$ adalah isomorpik. Selain itu, keduanya adalah daerah integral jika R adalah daerah integral.

Bukti
Misalkan ϕ memetakan elemen $R[x][y]$ ke elemen $R[x, y]$ yang diperoleh dengan "menggandakan" dengan cara mengubah (1) dalam Definisi 8.1.5 sebelumnya menjadi (2). Lebih formal, pertimbangkan elemen h dari $R[x][y]$

$$h = f_n(x)y^n + \cdots + f_1(x)y + f_0(x),$$

dimana $f_i(x) = \left(\sum_{j=0}^{m_i} a_{i,j}x^j\right)$ dan deg $f_i(x) == m_i$. Lalu kita punya

$$\phi(h) = \sum_{i=0}^{n}\sum_{j=0}^{m_i} a_{i,j}x^j y^i.$$

Verifikasi bahwa ini adalah isomorfisme diserahkan kepada pembaca. (Lihat Latihan 8.1 no.25) Dengan Teorema 8.1.1, jika R adalah domain integral, maka $R[x]$ juga demikian. Mengulangi argumen ini, begitu juga $R[x][y]$. Tapi begitu juga $R[x, y]$ karena isomorfik ke $R[x][y]$.

Pada pembahasan terdahulu untuk sebarang daerah integral bisa dikonstruksi lapangan pecahan.

Definisi 8.1.6 Misalkan D adalah suatu daerah integral dan $D[x]$ adalah ring polinomial dengan koefisien di D. Lapangan pecahan dari $D[x]$ dinamakan lapangan dari **fungsi rasional** dengan koefisien di D dan ditulis $D(x)$. Elemen-elemennya adalah pecahan berbentuk $f(x)/g(x)$, dimana $f(x), g(x) \in D[x]$ dan $g(x) \neq 0$. Selanjutnya $f_1(x)/g_1(x) = f_2(x)/g_2(x)$ bila dan hanya bila $f_1(x)g_2(x) = f_2(x)g_1(x)$.

Teorema 8.1.2 Misalkan R adalah suatu ring komutatif yang mempunyai elemen satuan dan sebarang $\alpha \in R$ dengan α tetap. Maka suatu pemetaan $\phi_\alpha : R[x] \to R$ didefinisikan oleh

$$\phi_\alpha(f(x)) = f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0,$$

dengan $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ adalah suatu homomorpisma ring.

Bukti Misalkan $f(x) = \sum_{i=0}^{n} a_i x^i$ dan $g(x) = \sum_{i}^{m} b_i x^i$ di $R[x]$, didapat

$$\begin{aligned}
\phi_\alpha(f(x)+g(x)) &= \phi_\alpha\left(\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{m} b_i x^i\right) \\
&= \phi_\alpha\left(\sum_{i=0}^{\max\{n,m\}} (a_i + b_i)x^i\right) \\
&= \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)\alpha^i \\
&= \sum_{i=0}^{n} a_i\alpha^i + \sum_{i=0}^{m} b_i\alpha^i \\
&= \phi_\alpha(f(x)) + \phi_\alpha(g(x))
\end{aligned}$$

dan

$$\begin{aligned}
\phi_\alpha(f(x).g(x)) &= f(\alpha).g(\alpha) \\
&= \left(\sum_{i=0}^{n} a_i\alpha^i\right)\left(\sum_{i=0}^{m} b_i\alpha^i\right) \\
&= \sum_{i=0}^{n+m}\left(\sum_{k=0}^{i} a_k b_{i-k}\right)\alpha^i \\
&= \phi_\alpha(f(x).g(x)).
\end{aligned}$$

Pemetaan ϕ_α dinamakan **homomorpisma evaluasi** di α.

BARISAN dalam RING

Misalkan R ring komutatif dan barisan $< a_0, a_1, a_2, \ldots >$ dengan $a_i \in R$ dinotasikan oleh $< a_i >$. Bila penjumlahan $(+)$ dan konfolusi $(*)$ dari barisan masing-masing didefinisikan oleh

$$< a_i > + < b_i > = < a_i + b_i >$$

dan

$$\begin{aligned}
< a_i > * < b_i > &= \left\langle \sum_{j+k=i} a_j b_k \right\rangle \\
&= < a_0 b_i + a_1 b_{i-1} + \ldots + a_i b_0 > .
\end{aligned}$$

Maka $(R^{\mathbb{N}}, +, *)$ adalah ring komutatif dan merupakan daerah integral bila R adalah daerah integral.

Bukti Penjumlahan jelas assosiatif dan komutatif. Elemen nol adalah $< 0 >=< 0, 0, \ldots >$ dan invers dari $< a_i >$ adalah $< -a_i >$. Selanjutnya

$$\begin{aligned}(< a_i > * < b_i >) * < c_i > &= \left\langle \sum_{j+k=i} a_j b_k \right\rangle * < c_i > \\ &= \left\langle \sum_{l+m=i} \left(\sum_{j+k=m} a_j b_k \right) c_l \right\rangle = \left\langle \sum_{j+k+l=i} a_j b_k c_l \right\rangle\end{aligned}$$

Dengan cara serupa didapat

$$< a_i > *(< b_i > * < c_i >) = \left\langle \sum_{j+k+l=i} a_j b_k c_l \right\rangle$$

Terlihat bahwa $(< a_i > * < b_i >) * < c_i >=< a_i > *(< b_i > * < c_i >)$ dan

$$\begin{aligned}< a_i > *(< b_i > + < c_i >) &= \left\langle \sum_{j+k=i} a_j (b_k + c_k) \right\rangle \\ &= \left\langle \sum_{j+k=i} a_j b_k \right\rangle + \left\langle \sum_{j+k=i} a_j c_k \right\rangle \\ &= < a_i > * < b_i > + < a_i > * < c_i > .\end{aligned}$$

Konvolusi jelas komutatif sebab R ring komutatif. Identitas adalah $< 1, 0, 0, \ldots >$, sebab

$$\begin{aligned}< 1, 0, 0, \ldots > * < a_0, a_1, a_2, \ldots > &= < 1a_0, 1a_1 + 0a_0, 1a_2 + 0a_1 + 0a_0, \ldots > \\ &= < a_0, a_1, a_2, \ldots >\end{aligned}$$

Jadi $(R^{\mathbb{N}}, +, *)$ adalah ring komutatif. Misalkan masing-masing a_q dan b_r adalah elemen pertama yang tak nol dalam barisan $< a_i >$ dan $< b_i >$, maka posisi elemen ke-$q + r$ dalam barisan konvolusi $< a_i > * < b_i >$ diberikan oleh :

$$\begin{aligned}\sum_{j+k=q+r} &= a_0 b_{q+r} a_1 b_{q+r-1} + \ldots + a_q b_r + a_{q+1} b_{r-1} + \ldots + a_{q+r} b_0 \\ &= 0 + 0 + \ldots + a_q b_r + 0 + \ldots + 0 \\ &= a_q b_r.\end{aligned}$$

Bila R adalah daerah integral, maka $a_q b_r \neq 0$. Oleh karena itu $\sum_{j+k=q+r} a_j b_k \neq 0$. Jadi ring dari barisan tidak memuat pembagi nol.

Ring dari barisan tidak akan mempunyai struktur lapangan, sebab $< 0, 1, 0, 0, \ldots >$ tidak mempunyai invers. Faktanya bahwa, untuk setiap barisan $< b_i >$, didapat

$$< 0, 1, 0, 0, \ldots > * < b_0, b_1, b_2, b_3, \ldots >=< 0, b_0, b_1, b_2, \ldots >$$

terlihat bahwa hasil konvolusi bukan barisan identitas. Suatu **deret formal** dalam x dengan koefisien di ring komutatif R adalah

$$\sum_{i=0}^{\infty} a_i x^i, \text{ dimana } a_i \in R.$$

Berbeda dengan suatu polinomial, deret pangkat ini bisa mempunyai sejumlah takhingga suku-suku yang tak nol.

DERET FORMAL

Himpunan semua deret formal dinotasikan oleh $R[[x]]$. Istilah formal digunakan untuk mengindikasi bahwa kekonvergenan dari deret tidak dipertimbangkan. Termotifasi oleh $\mathbb{R}^{\mathbb{N}}$, penjumlahan dan perkalian dalam $R[[x]]$ didifinisikan oleh

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

dan

$$\left(\sum_{i=0}^{\infty} a_i x^i\right).\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty}\left(\sum_{j+k=i} a_j b_k\right) x^i.$$

Dapat diselidiki bahwa himpunan semua deret formal adalah suatu ring $(R[[x]], +, .)$ dan polinomial ring $R[x]$ dengan sejumlah suku-suku taknol yang berhingga adalah subring dari ring $R[[x]]$. Suatu fakta bahwa barisan ring $(R^{\mathbb{N}}, +, *)$ adalah isomorpik dengan ring deret formal $(R[[x]], +, .)$. Fungsi $f : R^{\mathbb{N}} \to R[[x]]$ yang didifinisikan oleh

$$f(< a_0, a_1, a_2, \ldots >) = a_0 + a_1 x + a_2 x^2 + \ldots$$

jelas f fungsi satu-satu pada. Dari difinisi penjumlahan, perkalian dan konvolusi dalam ring $R^{\mathbb{N}}$ dan $R[[x]]$, maka f adalah isomorpisma ring. □

Latihan

Dalam Latihan 1 sampai 6 hitung jumlah $f(x) + g(x)$ dan hasil perkalian $f(x)g(x)$ untuk polinomial yang diberikan $f(x)$ dan $g(x)$ di ring polinomial yang diberikan $R[x]$.

1. $2x^2 + x + 1$ dan $3x^3 + 2$ di $\mathbb{Z}[x]$.
2. $2x^2 + x + 1$ dan $3x^3 + 2$ di $\mathbb{Z}_6[x]$.
3. $2x^2 + x + 1$ dan $3x^3 + 2$ di $\mathbb{Z}_7[x]$.
4. $6x^2 + 2$ dan $2x^3 + 6x$ di $\mathbb{Z}_4[x]$.
5. $6x^2 + 2x + 1$ dan $2x^2 + 2x + 1$ di $\mathbb{Z}_4[x]$.
6. $3x^3 + 4x^2 + 2x + 1$ dan $4x^3 + 3x + 2$ di $\mathbb{Z}_5[x]$.

7. Dapatkan semua polinomial berderajad ≤ 2 di $\mathbb{Z}_2[x]$.

8. Dapatkan semua polinomial berderajad ≤ 2 di $\mathbb{Z}_3[x]$.

9. Misalkan $\mathbb{F}$ adalah suatu sublapangan dari suatu lapangan $\mathbb{E}$ dan $\alpha \in \mathbb{E}$. Didefinisikan $\phi_\alpha : \mathbb{F}[x] \to \mathbb{E}$ sebagai berikut. Untuk

$$f(x) = a_n x^n + \cdots a_1 x + a_0 \in \mathbb{F}[x],$$

misalkan

$$\phi_\alpha(f(x)) = a_n \alpha^n + \cdots a_1 \alpha + a_0 \in \mathbb{E}.$$

Tunjukkan bahwa ϕ_α adalah suatu homomorpisma ring. Ini disebut **homomorpisma evaluasi**.

Dalam Latihan 10 hingga 14 hitung $\phi_\alpha(f(x))$ untuk lapangan $\mathbb{E}$ dan $\mathbb{F}$ yang diberikan.

10. $\phi_1(x^4 + 1)$ $\mathbb{F} = \mathbb{E} = \mathbb{Z}_2$.

11. $\phi_1(x^2 + x + 1)$ $\mathbb{F} = \mathbb{E} = \mathbb{Z}_2$.

12. $\phi_{\sqrt{2}}(x^2 - 2)$ $\mathbb{F} = \mathbb{Q}, \mathbb{E} = \mathbb{R}$.

13. $\phi_i(x^3)$ $\mathbb{F} = \mathbb{Q}, \mathbb{E} = \mathbb{C}$.

14. $\phi_2[(x^4 + 1)(x^3 + 4x + 2)]$ $\mathbb{F} = \mathbb{E} = \mathbb{Z}_5$.

15. Misalkan $\phi : R \to S$ adalah suatu homomoipisma ring, dan didefinisikan $\phi^* : R[x] \to S[x]$ sebagai berikut. Untuk

$$f(x) = a_n x^n + \cdots a_1 x + a_0 \in R[x],$$

misalkan

$$\phi^*(f(x)) = \phi(a_n)x^n + \cdots + \phi(a_1)x + \phi(a_0) \in S[x].$$

Tunjukkan bahwa ϕ^* adalah suatu homomoipisma ring. Ini disebut **homomorpisma terinduksi**.

16. Misalkan $\phi : \mathbb{Z} \to \mathbb{Z}_5$ adalah sauatu homomorpisma alami dari $\mathbb{Z}$ ke $\mathbb{Z}_5$ yang memetakan $n \in \mathbb{Z}$ ke sisa mod 5 . Tunjukkan bahwa homomorpisma induksi $\phi^* : \mathbb{Z}[x] \to \mathbb{Z}_5[x]$ seperti yang didefinisikan pada soal sebelumnya juga merupakan pemetaan **pada**. Jelaskan kernel dari ϕ^*.

17. Tunjukkan bahwa jika ring R dan S isomorpik, maka $R[x]$ isomorpik dengan $S[x]$.

18. Tunjukkan bahwa jika S adalah subring dari R maka $S[x]$ adalah subring dari $R[x]$.

19. Dapatkan semua unit di
(a) $\mathbb{Z}[x]$ (b) $\mathbb{Q}[x]$ (c) $\mathbb{Z}_5[x]$ (d) $\mathbb{Z}[x, y]$ (e) $\mathbb{Q}(x)$.

20. Berikan contoh bilangan asli $n > 1$ dan polinomial $f(x) \in \mathbb{Z}_n[x]$ derajat > 0 yang merupakan unit di $\mathbb{Z}_n[x]$.

21. Dapatkan pembagi nol, jika mungkin, di setiap berikut. Jika tidak memungkinkan, jelaskan mengapa tidak.
(a) $\mathbb{Z}_4[x]$ (b) $\mathbb{Z}_5[x]$ (c) $\mathbb{Z}_6[x]$.

22. Berikan contoh, jika mungkin, dari dua polinomial $f(x)$ dan $g(x)$ pada ring yang ditunjukkan sehingga derajat $f(x)g(x)$ tidak sama dengan jumlah dari derajat $f(x)$ dan $g(x)$. Jika tidak memungkinkan, jelaskan mengapa tidak.
(a) $\mathbb{Z}_8[x]$ (b) $\mathbb{Z}_7[x]$ (c) $\mathbb{Z}_9[x]$.

23. Buktikan bagian (1) sampai (3) dari Teorema 8.1.1.

24. Misalkan $f(x, y)$ adalah suatu elemen di $\mathbb{Q}[x, y]$ berikut:

$$4x^2y^3 + 5xy^3 - 7x^4 + 3x^3y^2 - 2y^3 + 3x^4y + 2x^2 - x^3y + 10xy^2 + 3.$$

(a) Tulis ulang $f(x, y)$ sebagai suatu elemen dari $(\mathbb{Q}[x])[y]$.
(b) Tulis ulang $f(x, y)$ sebagai suatu elemen dari $(\mathbb{Q}[y])[x]$.

25. Buktikan bahwa pemetaan ϕ yang didefinisikan dalam pembuktian Proposisi 8.1.3 adalah isomorpisma.

8.2 Algorithma Pembagian di $\mathbb{F}[x]$

Sudah ditunjukkan bahwa bila D adalah suatu daerah integral maka $D[x]$ adalah daerah integral dan bukan lapangan. Dalam bagian ini untuk hal $\mathbb{F}$ adalah lapangan, maka daerah integral $\mathbb{F}[x]$ mempunyai beberapa sifat analogi dengan sifat-sifat $\mathbb{Z}$ yang sudah dikenal.

Suatu sifat fundamentaldari $\mathbb{Z}$ adalah berlakunya algoritma pembagian bilangan bulat yaitu, untuk sebarang bilangan bulat a dan b dengan $b \neq 0$, ada dengan tuggal pasangan bilangan bulat q dan r yang memenuhi $a = b.q + r$, $0 \leq r < |b|$. Sifat ini secara intensif sudah banyak digunakan. Sifat analogi untuk $F[x]$, yang akan terlihat memainkan suatu aturan fundamental.

Contoh 8.2.1 Tinjau polinomial $f(x) = 3x$ dan $g(x) = 2x$ di $\mathbb{Z}_7[x]$. Misalkan $f(x)$ dibagi oleh $g(x)$. Dengan kata lain, mendapatkan $q(x) \in \mathbb{Z}_7[x]$ yang memenuhi $f(x) = q(x).g(x)$. Karena $\mathbb{Z}_7[x]$ adalah daerah integral, maka $\deg(f(x)) = \deg(q(x)) + \deg(g(x))$. Jadi, $\deg(q(x)) = 0$ dan $q(x) = c \in \mathbb{Z}_7[x]$ adalah polinomial konstan. Dengan demikian $3x = c(2x)$ dan $c = 3.2^{-1} = 3.4 = 5 \in \mathbb{Z}_7[x]$. Catatan bahwa c ada dan tunggal sebab invers terhadap perkalian 2^{-1} ada dan tunggal di $\mathbb{Z}_7[x]$. ●

Teorema berikut analogi dari algoritma pembagian untuk $\mathbb{Z}$. Yaitu algoritma pembagian untuk polinomial-polinomial di daerah integral $\mathbb{F}[x]$.

Teorema 8.2.1 (**Algoritma Pembagian**) Misalkan $f(x), g(x)$ adalah polinomial di $\mathbb{F}[x]$ dimana $\mathbb{F}$ adalah suatu lapangan dan $g(x)$ polinomial taknol. Maka ada dengan tunggal polinomial $q(x)$ dan $r(x)$ di $\mathbb{F}[x]$ yang memenuhi

$$f(x) = g(x).q(x) + r(x),$$

dengan $\deg(r(x)) < \deg(g(x))$ atau $r(x)$ adalah polinomial nol.

Bukti Ditunjukkan eksistensi dari $q(x)$ dan $r(x)$. Bila $f(x)$ adalah polinomial nol, maka

$$0 = 0.g(x) + 0,$$

terlihat dua-duanya $q(x)$ dan $r(x)$ adalah polinomial nol dan memenuhi $r(x) = 0$ atau $\deg(r(x)) < \deg(g(x))$. Selanjutnya, untuk $f(x)$ bukan polinomial nol dan $\deg(f(x)) = m$, misalkan $\deg(g(x)) = n$. Bila $m < n$, maka $q(x) = 0$, $r(x) = f(x)$ dan memenuhi $f(x) = 0.g(x) + f(x)$ dengan $\deg(f(x)) < \deg(g(x))$. Berikutnya, bila $m \geq n$ dan

$$\begin{aligned} f(x) &= a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \\ g(x) &= b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0. \end{aligned}$$

Dalam kaasus ini bukti dilakukan secara induksi pada m yaitu derajad dari $f(x)$. Bila $m = 0$, maka $n = 0$ dalam hal yang demikian $f(x) = a_0$ dan $g(x) = b_0$ keduanya merupakan polinomial konstan taknol di $\mathbb{F}[x]$. Sehingga didapat

$$f(x) = a_0 = (a_0 b_0^{-1})b_0 + 0 = (a_0 b_0^{-1})g(x) + 0,$$

Terlihat disini $r(x) = 0$. Jadi teorema benar untuk $m = 0$ atau derajad dari $f(x)$ kurang dari satu. Selanjutnya diasumsikan teorema benar untuk polinomial $f(x)$ berderajad kurang dari m dan ditunjukkan bahwa teorema benar untuk $\deg(f(x)) = m$. Dengan demikian teorema terbukti. Untuk hal yang demikian tinjau polinomial

$$f_1(x) = f(x) - (a_m b_n^{-1})x^{m-n}.g(x), \tag{8.2}$$

jelas bahwa $f_1(x)$ mempunyai derajad kurang dari m. Dengan asumsi yang telah diberikan bila $f_1(x)$ dibagi $g(x)$, maka ada $q_1(x)$ dan $r_1(x)$ yang memenuhi

$$f_1(x) = q_1(x).g(x) + r_1(x),$$

dengan $r_1(x) = 0$ atau $\deg(r_1(x)) < \deg(g(x))$. Selanjutnya, misalkan

$$q(x) = q_1(x) + (a_m b_n^{-1})x^{m-n}.$$

Maka

$$f(x) = g(x).q(x) + r(x),$$

dengan $r(x) = r_1(x) = 0$ atau $\deg(r(x)) < \deg(g(x))$. Hasil ini menunjukkan eksistensi dari $q(x)$ dan $r(x)$ yang memenuhi

$$f(x) = q(x).g(x) + r(x),$$

dengan $r(x) = 0$ atau $\deg(r(x)) < \deg(g(x))$. Tinggal menunjukkan bahwa $q(x)$ dan $r(x)$ tunggal. Misalkan ada dua polinomial $q'(x)$ dan $r'(x)$ yang memenuhi

$$f(x) = g(x).q'(x) + r'(x),$$

dengan $r'(x) = 0$ atau $\deg(r'(x)) < \deg(g(x))$. Didapat

$$f(x) = g(x).q(x) + r(x) = g(x).q'(x) + r'(x)$$

dan

$$r'(x) - r(x) = g(x)[q(x) - q'(x)].$$

Untuk $g(x)$ bukan polinomial nol dan andaikan $q(x) - q'(x) \neq 0$ maka

$$\deg(r'(x) - r(x)) = \deg(g(x)[q(x) - q'(x)]) \geq \deg(g(x)).$$

Hal ini tidak mungkin sebab derajad dari masing-masing $r'(x)$ dan $r(x)$ tidak melebihi derajad dari $g(x)$. Jadi haruslah $q(x) - q'(x)$ adalah polinomial nol. Sehingga didapat $q(x) = q'(x)$ dan $r(x) = r'(x)$. ●

Contoh 8.2.2 Cara algoritma pembagian bilangan bulat sudah banyak dilakukan dengan apa yang dinamakan pembagian panjang ("poro gapit"). Misalkan, diberikan dua polinomial $f(x) = 2x^3 - 3x^2 + 4x - 5$ dan $g(x) = x - 1$ di $\mathbb{R}[x]$, maka $f(x)$ dibagi $g(x)$ dilakukan sebagai berikut:

$$\begin{array}{r|l} & 2x^2 - x + 3 \\ \hline x-1 & 2x^3 - 3x^2 + 4x - 5 \\ & -2x^3 + 2x^2 \\ \hline & \quad -x^2 + 4x \\ & \quad x^2 - x \\ \hline & \quad\quad 3x - 5 \\ & \quad\quad -3x + 3 \\ \hline & \quad\quad\quad -2 \end{array}$$

Terlihat bahwa $f(x) = q(x).g(x) + r(x)$, diberikan oleh

$$2x^3 - 3x^2 + 4x - 5 = (2x^2 - x + 3)(x - 1) + (-2).$$

Contoh 8.2.3 Dalam $\mathbb{Z}_5[x]$, diberikan

$$f(x) = 2x^4 + x^3 + 3x^2 + 3x + 1, \quad g(x) = 2x^2 - x + 2,$$

maka dengan melakukan pembagian panjang $f(x)$ dibagi $g(x)$, didapat

$$\begin{array}{r|l} & x^2 + x + 1 \\ \hline 2x^2 - x + 2 & 2x^4 + x^3 + 3x^2 + 3x + 1 \\ & -2x^4 + x^3 - 2x^2 \\ \hline & \quad 2x^3 + x^2 + 3x + 1 \\ & \quad -2x^3 + x^2 - 2x \\ \hline & \quad\quad 2x^2 + x + 1 \\ & \quad\quad -2x^2 + x - 2 \\ \hline & \quad\quad\quad 2x - 1 = 2x + 4 \end{array}$$

Terlihat hasil bagi $q(x) = x^2 + x + 1$ dan sisa pembagian $r(x) = 2x + 4$. Sehingga didapat

$$2x^4 + x^3 + 3x^2 + 3x + 1 = (x^2 + x + 1)(2x^2 - x + 2) + 2x + 4.$$

Suatu aplikasi langsung dari algoritma pembagian pada himpunan bilangan bulat $\mathbb{Z}$ adalah menghitung faktor persekutuan terbesar (fpb) dari dua bilangan bulat a dan b. Dalam pembahasan berikutnyaditunjukkan bahwa hal ini dapat juga dilakukan dalam $\mathbb{F}[x]$. Sebelumnya diberikan analogi definisi yang telah digunakan untuk $\mathbb{Z}$.

Definisi 8.2.1 Untuk sebarang $f(x)$ dan $g(x) \neq 0$ di $\mathbb{F}[x]$, dimana $\mathbb{F}$ adalah suatu lapangan. Polinomial $q(x)$ dan $r(x)$ dalam algoritma pembagian masing-masing dinamakan **hasil bagi** dan **sisa** pada pembagian $f(x)$ dibagi oleh $g(x)$. Bila sisa $r(x) = 0$ atau dengan kata lain bila ada suatu $q(x)$ yang memenuhi $f(x) = q(x).g(x)$, maka $g(x)$ dinamakan suatu **pembagi** dari $f(x)$ atau $g(x)$ **membagi** $f(x)$ dan ditulis $g(x)|f(x)$. Juga, dalam hal ini $f(x)$ dinamakan **kelipatan** dari $g(x)$. Penulisan suatu polinomial menjadi suatu produk $f(x) = g(x).h(x)$ dinamakan **pemfaktoran** polinomial. Pemfaktoran yang demikian dinamakan **taktrivial** bila faktor-faktor $g(x)$ dan $h(x)$ keduanya mempunyai derajad lebih besar dari nol.

Proposisi 8.2.1 Misalkan $\mathbb{F}$ adalah suatu lapangan, polinomial $f(x)$ dan $g(x)$ di $\mathbb{F}[x]$. Maka
(1) Bila $g(x)|f(x)$, maka $cg(x)|f(x)$ untuk sebarang elemen $c \neq 0$ di $\mathbb{F}$.
(2) Bila $g(x)|f(x)$ dan $f(x)|g(x)$, maka $f(x) = cg(x)$ untuk beberapa elemen $c \neq 0$ di $\mathbb{F}$.

Bukti (1) Karena $\mathbb{F}$ adalah lapangan dan $c \neq 0$ di $\mathbb{F}$, maka c adalah unit di $\mathbb{F}$. Bila $f(x) = q(x).g(x)$ (sebab $g(x)|f(x)$), maka juga $f(x) = [c^{-1}q(x)].[cg(x)]$. terlihat bahwa $cg(x)|f(x)$.
(2) Bila $f(x) = q(x).g(x)$ dan $g(x) = p(x).f(x)$, maka $f(x) = [q(x).p(x)].f(x)$. Karena $\mathbb{F}[x]$ daerah integral, maka haruslah $q(x).p(x) = 1$. Jadi, $q(x)$ dan $p(x)$ keduanya polinomial berderajad nol. Dengan demikian $q(x) = c$ dan $p(x) = c^{-1}$ untuk beberapa $c \in \mathbb{F}$.

Definisi 8.2.2 Bila $\mathbb{F}$ adalah suatu lapangan, $f(x)$ dan $g(x)$ di $\mathbb{F}[x]$ suatu **pembagi persekutuan** dari $f(x)$ dan $g(x)$ adalah sebarang polinomial $c(x) \in \mathbb{F}[x]$ yang memenuhi $c(x)|f(x)$ dan $c(x)|g(x)$. Suatu **pembagi persekutuan terbesar** (fpb) dari $f(x)$ dan $g(x)$ adalah suatu pembagi persekutuan $d(x)$ yang memenuhi untuk sebarang pembagi persekutuan yang lain $c(x)$, maka $c(x)|d(x)$. Bila pembagi persekutuan terbesar dari $f(x)$ dan $g(x)$ hanyalah suatu polinomial konstan, maka $f(x)$ dan $g(x)$ dinamakan **prima relatif**. Catatan bahwa dari proposisi sebelumnya, bila $d_1(x)$ dan $d_2(x)$ keduanya adalah pembagi persekutuan terbesar dari $f(x)$ dan $g(x)$, maka $d_1(x) = cd_2(x)$ untuk beberapa $c \neq 0$ di $\mathbb{F}$. Dari hal ini maka hanya terdapat satu monik pembagi persekutuan terbesar yang dinotasikan oleh fpb$(f(x), g(x))$

Contoh 8.2.4 Dalam $\mathbb{C}[x]$, diberikan polinomial

$$f(x) = 2x^4 - x^3 + 4x^2 + 3 \qquad \text{dan} \qquad g(x) = x^3 + 2x + 1.$$

Bila digunakan algoritma pembagian pada $f(x)$ dan $g(x)$ didapat

$$\begin{array}{rl} & 2x - 1 \\ \hline x^3 + 2x + 1 \,\big) & 2x^4 - x^3 + 4x^2 \quad + 3 \\ & -2x^4 \quad - 4x^2 - 2x \\ \hline & \quad -x^3 \quad - 2x + 3 \\ & \quad x^3 \quad + 2x + 1 \\ \hline & \qquad\qquad 4 \end{array}$$

Terlihat bahwa

$$f(x) = (2x - 1)g(x) + 4. \tag{8.3}$$

Selanjutnya, untuk setiap $\alpha \in \mathbb{C}$ yang memenuhi $g(\alpha) = 0$ didapat $f(\alpha) = 4 \neq 0$. Jadi $f(x)$ dan $g(x)$ tidak mempunyai akar-akar yang sama. Perhatikan bahwa Persamaan (8.3) berakibat bahwa fpb$(f(x), g(x)) = 1$, atau dengan kata lain $f(x)$ dan $g(x)$ adalah prima relatif.

Sebagaimana dalam $\mathbb{Z}$ mengenai fpb, berikut ini dibuktikan suatu analogi teorema tentang fpb dalam $F[x]$.

Teorema 8.2.2 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x)$ dan $g(x)$ di $\mathbb{F}[x]$ yang keduanya bukan polinomial nol. Maka ada suatu pembagi persekutuan terbesar $d(x)$ dari $f(x)$ dan $g(x)$ yang bisa ditulis sebagai kombinasi linier dari $f(x)$ dan $g(x)$. Yaitu, ada elemen $u(x)$ dan $v(x)$ di $\mathbb{F}[x]$ yang memenuhi

$$d(x) = u(x).f(x) + v(x).g(x)$$

adalah pembagi persekutuan terbesar dari $f(x)$ dan $g(x)$.

Bukti Pembuktian dilakukan dalam tiga langkah.

(1) Tinjau himpunan

$$I = \{m(x).f(x) + n(x).g(x) \,|\, m(x), n(x) \in \mathbb{F}[x]\}.$$

Catatan bahwa $f(x), g(x) \in I$, dengan demikian I mempunyai elemen yang bukan polinomial nol. Misalkan $d(x)$ adalah suatu elemen di I yang mempunyai derajad paling kecil dari semua elemen-elemen di I. Maka untuk setiap $c \in \mathbb{F}$, $cd(x) \in I$ dan mempunyai derajad sama dengan derajad dari $d(x)$. Dengan demikian dapat ditentukan $d(x)$ adalah monik, sebab bila tidak dapat diganti oleh $a^{-1}d(x)$ dimana a adalah koefisien utama (leading) dari $d(x)$. Karena $d(x) \in I$, didapat

$$d(x) = u(x).f(x) + v(x).g(x),$$

untuk beberapa $u(x), v(x) \in \mathbb{F}[x]$

(2) Berikutnya, ditunjukkan bahwa $d(x)$ adalah pembagi persekutuan dari $f(x)$ dan $g(x)$. Dengan menggunakan algoritma pembagian, didapat $f(x) = q(x).d(x) + r(x)$, dimana $r(x) = 0$ atau $\deg(r(x)) < \deg(d(x))$. Dalam hal ini diinginkan $r(x) = 0$. Selesaikan $r(x)$, didapat

$$r(x) = f(x) - q(x).d(x) = [1 - q(x).u(x)]f(x) - [q(x)v(x)]g(x).$$

Hal ini memperlihatkan bahwa $r(x) \in I$ dan karena $d(x)$ dipilih berderajad paling kecil di I, tidaklah mungkin $\deg(r(x)) < \deg(d(x))$. Jadi $r(x) = 0$, dengan demikian $d(x)|f(x)$. Dengan argumentasi yang sama, berdasarkan algoritma pembagian didapat $g(x) = h(x)d(x)+r(x)$ dimana $r(x) = 0$ atau $\deg(r(x)) < \deg(d(x))$. Selesaikan $r(x)$, didapat

$$r(x) = g(x) - h(x).d(x) = [1 - h(x).v(x)]g(x) - [h(x)u(x)]f(x).$$

Hal ini memperlihatkan bahwa $r(x) \in I$ dan karena $d(x)$ dipilih berderajad paling kecil di I, tidaklah mungkin $\deg(r(x)) < \deg(d(x))$. Jadi $r(x) = 0$, dengan demikian $d(x)|g(x)$.

(3) Untuk melengkapi bukti, ditunjukkan bahwa sebarang pembagi pesekutuan $c(x)$ dari $f(x)$ dan $g(x)$ membagi $d(x)$. Tetapi, bila $f(x) = q(x).c(x)$ dan $g(x) = p(x).c(x)$, maka

$$d(x) = u(x).f(x) + v(x).g(x) = [u(x).q(x) + v(x).p(x)]c(x).$$

Terlihat bahwa $c(x)|d(x)$ sebagaimana yang dikehendaki. ◪

Algoritma pembagian dapat digunakan untuk mendapatkan fpb di $\mathbb{F}[x]$ sebagaimana di $\mathbb{Z}$.

Teorema 8.2.3 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x)$ dan $g(x)$ di $\mathbb{F}[x]$, bila secara berulang digunakan algoritma pembagian didapat
(1) $f(x) = q_1(x).g(x) + r_1(x)$
(2) $g(x) = q_2(x).r_1(x) + r_2(x)$
(3) $r_1(x) = q_3(x).r_2(x) + r_3(x)$
$\vdots$
maka akan sampai n berhingga didapat
(n) $r_{n-2}(x) = q_n(x).r_{n-1}(x) + r_n(x)$
(n+1) $r_{n-1}(x) = q_{n+1}(x).r_n(x) + r_{n+1}(x)$,
dimana $r_{n+1}(x) = 0$. Maka $r(x) = r_n(x)$ adalah suatu fpb dari $f(x)$ dan $g(x)$, pembagian tidak akan terus berlangsung, sebab

$$\deg(g(x)) > \deg(r_1(x)) > \deg(r_2(x)) > \deg(r_3(x)) > \cdots > 0,$$

jadi akan sampai pada suatu n sebagaimana telah disebutkan. Untuk n yang demikian, dari Persamaan (n+1) terlihat bahwa $r_n(x)|r_{n-1}(x)$, maka dari Persamaan (n) didapat $r_n(x)|r_{n-2}(x)$ dan seterusnya sampai ke Persamaan (2) dan (1) menunjukkan bahwa $r_n(x)|g(x)$ dan $r_n(x)|f(x)$. Lagipula, bila $c(x)$ adalah sebarang pembagi persekutuan dari $f(x)$ dan $g(x)$, maka dari Persamaan (1) didapat $c(x)|r_1(x)$ dan, juga dari Persamaan (2) didapat $c(x)|r_2(x)$ dan terus kebawah sampai ke Persamaan (n+1) didapat $c(x)|r_n(x)$. Hal ini menunjukkan bahwa $r_n(x)$ adalah suatu fpb dari $f(x)$ dan $g(x)$. ✓

Definisi 8.2.3 Barisan dari penghitungan (1), (2), (3), ... dalam Teorema 8.2.3 dinamakan **algoritma Eulcide**. ✓

Contoh 8.2.5 Tinjau polinomial

$$f(x) = x^4 + 2x^2 + 1 \quad \text{dan} \quad g(x) = x^2 + x + 2$$

di $\mathbb{Z}_3[x]$. Gunakan algoritma Euclide, didapat
(1) $x^4 + 2x^2 + 1 = (x^2 - x + 1)(x^2 + x + 2) + (x + 2)$
(2) $x^2 + x + 2 = (x + 2)(x + 2) + 1$.
Jadi, fpb$(f(x), g(x)) = 1$ dan; $f(x)$ dan $g(x)$ adalah prima relatif. Juga, didapat

$$\begin{aligned} 1 &= (x^2 + x + 2) - (x + 2)(x + 2) \\ &= (x^2 + x + 2) - (x + 2)[(x^4 + 2x^2 + 1) - (x^2 - x + 1)(x^2 + x + 2)] \\ &= [-x - 2](x^4 + 2x^2 + 1) + [1 - (x + 2)(x^2 - x + 1)](x^2 + x + 2) \\ \text{fpb}(f(x), g(x)) &= u(x).f(x) + v(x).g(x). \end{aligned}$$

Perhitungan yang dilakukan ini akan berguna ketika mencari invers terhadap perkalian dalam ring kuasi $F[x]$. ●

Latihan

8.3 Aplikasi Algorithma Pembagian

Telah dibahas bagaimana menggunakan algoritma pembagian untuk menemukan FPB dari dua polinomial. Pada bagian ini digunakan algoritma pembagian untuk membangun beberapa sifat dasar polinomial dan menentukan akar dari polinomial. (Gagasan akar dari suatu polinomial telah didefinisikan dalam bagian sebelumnya.)

Contoh 8.3.1 (1) Sebagaimana telah dibahas dalam $\mathbb{Z}_3[x]$, $f(x) = x^2 + x + 1$ mempuyai tepat satu akar, $f(1) = 0$ dan $f(x)$ dapat difaktorkan sebagai $x^2 + x + 1 = (x-1)^2$ di $\mathbb{Z}_3[x]$.
(2) Berbeda dalam $\mathbb{Z}_7[x]$, $f(x) = x^2 + x + 1$ mempunyai tepat dua akar, yaitu $f(2) = f(4) = 0$ dan dalam $\mathbb{Z}_7[x]$, $f(x)$ dapat difaktorkan sebagai $x^2 + x + 1 = (x-2)(x-4)$.
(3) Dalam $\mathbb{Q}[x]$, $f(x) = x^3 + x^2 + x + 1$ mempunyai suatu akar di $\mathbb{Q}$, $f(-1) = 0$ dan dalam $\mathbb{Q}[x]$, $f(x)$ dapat difaktorkan sebagai $x^3 + x^2 + x = 1 = (x+1)(x^2+1)$.
(4) Berbeda di $\mathbb{C}[x]$, $f(x) = x^3 + x^2 + x + 1 = (x+1)(x-i)(x+i)$, jadi $-1, \pm i$ adalah tiga akar dari $f(x)$ di $\mathbb{C}[x]$. ●

Contoh yang dibahas ini menggambarkan konsekuensi yang sangat penting dari algoritma pembagian, yang dibuktikan sebagai berikut.

Teorema 8.3.1 (**Teori Faktor**) Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x)$ suatu polinomial di $\mathbb{F}[x]$ dan a suatu elemen di $\mathbb{F}$. Maka a adalah suatu akar dari $f(x)$ bila dan hanya bila $(x-a)$ adalah suatu pembagi dari $f(x)$ dalam $\mathbb{F}[x]$.

Bukti ($\Rightarrow$) Pertama asumsikan bahwa a adalah suatu akar dari $f(x)$. Gunakan algoritma pembagian, dapat ditulis $f(x) = q(x)(x-a) + r(x)$, dimana salah satu $r(x) = 0$ atau $\deg(r(x)) < \deg(x-a) = 1$. Jadi $r(x)$ adalah suatu konstan $c \in \mathbb{F}$ dan $f(x) = q(x)(x-a) + c$. Dengan demikian $0 = f(a) = q(a)(a-a) + c = c$, jadi $f(x) = q(x)(x-a)$, dengan demikian $(x-a)$ adalah suatu pembagi dari $f(x)$ sebagaimana diharapkan.
($\Leftarrow$) Asumsikan $(x-a)$ adalah suatu pembagi dari $f(x)$, jadi $f(x) = p(x)(x-a)$ untuk beberapa $p(x)$ di $\mathbb{F}[x]$. Maka, didapat $f(a) = p(a)(a-a) = 0$. Terlihat bahwa a adalah suatu akar dari $f(x)$ di $\mathbb{F}[x]$. ✓

Contoh 8.3.2 Dalam $\mathbb{Z}_5[x]$, tinjau polinomial $f(x) = x^4 + x^3 + x - 1$. Perhatikan bahwa $f(2) = 0$, jadi $(x-2)$ harus merupakan suatu pembagi dari $f(x)$ dalam $\mathbb{Z}_5[x]$. Selanjutnya dihitung pembagian berikut.

$$
\begin{array}{r|l}
 & x^3 + 3x^2 + x + 3 \\
\hline
x - 2 & x^4 + x^3 + \quad x - 1 \\
 & -(x^4 - 2x^3) \\
\hline
 & \quad 3x^3 + \quad x - 1 \\
 & -(3x^3 - x^2) \\
\hline
 & \quad x^2 + x - 1 \\
 & -(x^2 - 2x) \\
\hline
 & \quad 3x - 1 \\
 & -(3x - 1) \\
\hline
 & \quad 0
\end{array}
$$

Jadi dalam $\mathbb{Z}_5[x]$, maka $f(x) = (x^3 + 3x^2 + x + 3)(x-2)$. Karena 2 juga akar dari $g(x) = x^3 + 3x^2 + x + 3$, maka $x - 2$ juga merupakan suatu pembagi dari $g(x)$ dalam $\mathbb{Z}_5[x]$. Lagi, lakukan perhitungan pembagian berikut.

$$
\begin{array}{r|l}
 & x^2+1 \\
\hline
x-2 & x^3+3x^2+x+3 \\
 & \underline{x^3+3x^2} \\
 & \quad x+3 \\
 & \quad \underline{x+3} \\
 & \quad\quad 0
\end{array}
$$

Maka dalam $\mathbb{Z}_5[x]$ didapat

$$(x^2+1)(x-2)^2 = (x^2-4)(x-2)^2 = (x+2)(x-2)(x-2)^2 = (x+2)(x-2)^3,$$

sehingga menghasilkan pemfaktoran $f(x) = (x+2)(x-2)^3$. ●

Teorema 8.3.2 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x)$ suatu polinomial di $F[x]$ dan a suatu elemen di $\mathbb{F}$. Maka $f(a)$ adalah sisa atas pembagian $f(x)$ oleh $(x-a)$ dalam $\mathbb{F}[x]$.

Bukti
Diberikan $f(x)$ dan $(x-a)$ di $\mathbb{F}[x]$, maka dengan menggunakan Teorema Pembagian dapat dipilih $q(x)$ dan $r(x)$ yang memenuhi

$$f(x) = q(x)(x-a) + r(x), \quad \text{denga } r(x) = 0 \text{ atau } \deg(r(x)) < \deg(x-a).$$

Sehingga didapat

$$f(a) = q(a)(a-a) + r(a) = q(a)\,0 + r(a) = r(a) = 0 + r(a) = r(a).$$ ✓●

Definisi 8.3.1 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $f(x) \in F[x]$, $\alpha \in \mathbb{F}$ memenuhi $f(\alpha) = 0$. Maka dikatakan bahwa α adalah akar dari $f(x)$ **rangkap** s bila

$$f(x) = q(x)(x-\alpha)^s,$$

dimana $q(x) \in \mathbb{F}[x]$ dan $q(\alpha) \neq 0$. ✓●

Contoh 8.3.3
(1) Sebagaimana telah dibahas, dalam $\mathbb{Z}_5[x]$, polinomial $f(x) = x^4+x^3+x-1 = (x+2)(x-2)^3$. Jadi $2 \in \mathbb{Z}_5$ adalah akar dari $f(x)$ mrangkap 3.
(2) Dalam $\mathbb{Z}_5[x]$, polinomial $g(x) = x^5-1 = (x-1)^5$, jadi $1 \in \mathbb{Z}_5$ adalah akar dari $g(x)$ rangkat 5.
(3) Dalam $\mathbb{Q}[x]$, polinomial $h(x) = x^5-1 = (x-1)(x^4+x^3+x+1)$, maka $1 \in \mathbb{Q}$ adalah akar dari $h(x)$ rangkap 1. ●

Teorema 8.3.3 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x)$ suatu polinomial taknol di $\mathbb{F}[x]$ mempunyai derajad n. Maka $f(x)$ mempunyai akar di $\mathbb{F}$ tidak lebih dari n.

Bukti

Digunakan induksi pada n. Jika $n = 0$, maka $f(x)$ adalah konstan taknol, sehingga tidak memiliki akar. Selanjutnya diasumsikan teorema ini berlaku untuk semua polinomial di $\mathbb{F}[x]$ dengan derajat $n-1$. Jika $f(x)$ tidak memiliki akar di $\mathbb{F}$, maka teorema tersebut berlaku.

Jika $f(x)$ memiliki akar suatu akar $a \in F$, maka menurut terema faktor didapat $f(x) = q(x)(x-a)$ dimana $q(x)$ memiliki derajat $n-1$. Jika $b \neq a$ adalah akar dari $f(x)$, maka $0 = f(b) = q(b)(b-a)$ dan karena $\mathbb{F}$ adalah lapangan, tidak memiliki pembagi nol, maka haruslah $0 = q(b)$. Hal ini menjelaskan bahwa suatu akar dari $f(x)$ adalah a atau suatu akar dari $q(x)$ dengan hipotesis induksi banyaknya akar dari $q(x)$ di $\mathbb{F}$ tidak lebih dari $n-1$. Hal ini menunjukkan bahwa $f(x)$ tidak mempunyai akar lebih banyak dari n sebagaimana diharapkan.

Dalam teori yang baru saja dibahas, asumsi bahwa $\mathbb{F}$ adalah suatu lapangan sangat penting, sebagaimana terlihat dalam contoh berikut.

Contoh 8.3.4 Misalkan $f(x) = x^2 - 4 \in \mathbb{Z}_{12}$. Maka, dua pemfaktoran dari $f(x)$ diberikan oleh:

$$f(x) = (x-2)(x+2) = (x-2)(x-10)$$
$$f(x) = (x-4)(x+4) = (x-4)(x-8),$$

dalam $\mathbb{Z}_{12}$, terlihat empat akar $f(2) = f(4) = f(8) = f(10) = 0$. Jadi dalam ring $\mathbb{Z}_{12}$ yang bukan lapangan, ada polinomial berderajat dua mempunyai empat akar.

Contoh 8.3.5 Misalkan $f(x) \in \mathbb{R}[x]$ adalah suatu polinomial derajat 3 dan $g(x) \in \mathbb{R}[x]$ suatu polinomial derajat 1. Tinjau $f(x)$ dan $g(x)$ sebagai fungsi polinomial dan digambar grafiknya dalam $\mathbb{R}^2$ bidang-xy. Maka Teorema 8.3.3 menjelaskan bahwa banyaknya titik potong kedua grafik tersebut tidak melebihi 3. Sebab selisih dari $f(x) - g(x) \in \mathbb{R}[x]$ adalah polinomial berderajat 3, maka dari itu ada setidaknya tiga bilangan reall $\alpha \in \mathbb{R}$ yang memenuhi $f(\alpha) - g(\alpha) = 0$.

Dalam teorema berikut ini dengan menggunakan Teorema 8.3.3 ditunjukkan bahwa suatu sifat penting dari lapangan berhingga yang akan bermanfaat kelak.

Teorema 8.3.4 Misalkan $\mathbb{F}$ adalah sebarang lapangan berhingga dan G adalah subrup dari grup perkalian $\mathbb{F}^* = \mathbb{F} - \{0\}$, maka G adalah grup siklik.

Bukti

Grup G adalah suatu grup komutatif berhingga. Dengan menggunakan teorema fundamental untuk grup komutatif berhingga, Teorema 4.4.1 didapat

$$G \cong G_{d_1} \times G_{d_2} \times \cdots \times G_{d_n},$$

dimana pangkat d_i adalah prima dan G_{d_i} adalah suatu grup siklik terhadap perkalian berorder d_i. Selanjutnya, misalkan

$$N = \prod_{i=1}^{n} d_i \quad \text{dan} \quad M = \text{kpk}\{d_1, d_2, \ldots, d_n\}.$$

Jadi $M \leq N$. Dengan menggunakan Teorema Lagrange, untuk setiap $b_i \in G_{d_i}$ didapat $b_i^{d_i} = 1$, jadi $b_i^M = 1$. Maka dari itu, untuk setiap $a \in G$ didapat $a^M = 1$ atau dengan kata lain, setiap elemen dari G adalah suatu akar dari polinomial $f(x) = x^M - 1$ dalam $F[x]$. Sehingga berdasarkan Teorema 8.3.3 maka $|G| \leq M$. Tetapi diketahui bahwa $|G| = N$. Dengan demikian $M = N$ yang hanya mungkin bila d_i dan d_j adalah prima relatif untuk $d_i \neq d_j$. Sehingga berdasarkan Teorema 4.2.2 didapat $G \cong G_N$ adalah grup siklik berorder N.

Pembahasan bagian ini diakhiri oleh beberapa fakta yang berguna tentang akar-akar dari suatu polinomial dalam $\mathbb{R}[x]$.

Contoh 8.3.6 Akar-akar polinomial x^n-1 dinamakan **akar-akar tingkat-n dari satuan**. Bekerja dalam $\mathbb{C}$, bila $\omega = \cos(2\pi/n)+i\sin(2\pi/n)$, maka dengan menggunakan teorema DeMoivre, didapat $\omega^n = 1$ dan $\omega^k \neq 1$ untuk $1 \leq k < n$. Lagipula, dengan mudah terlihat bahwa $1, \omega, \omega^2, \ldots, \omega^{n-1}$ adalah akar-akar dari $f(x) = x^n - 1$ yang berbeda satu dengan yang lainnya. Karena $f(x)$ hanya bisa mempunyai akar-akar tidak melebihi n, maka semua dari ω^k, $0 \leq k \leq n-1$ adalah akar-akar tingkat-n dari satuan.

Teorema 8.3.5 Misalkan $f(x)$ adalah suatu polinomial di $\mathbb{R}[x]$. Bila $z = a + bi \in \mathbb{C}$ adalah suatu akar dari $f(x)$, maka konjuget kompleks $\bar{z} = a - bi$ juga merupakan akar dari $f(x)$.

Bukti

Tinjau polinomial

$$p(x) = x - (a+bi))(x-(a-bi)) = x^2 - 2ax + (a^2+b^2) \in \mathbb{R}[x].$$

Gunakan algoritma pembagian, didapat $q(x), r(x) \in \mathbb{R}[x]$ yang memenuhi

$$f(x) = q(x)p(x) + r(x),$$

dimana $r(x) = 0$ atau $\deg(r(x)) < \deg(p(x))$ yaitu derajat dari $r(x)$ adalah 0 atau 1. Jadi $r(x) = cx + d$ untuk beberapa $c, d \in \mathbb{R}$. Karena $0 = f(a+bi) = q(a+bi).0 + r(a+bi)$, maka $0 = r(a+bi) = c(a+bi) + d = (ca+d) + cbi$. Jadi $ca + d = cb = 0$. Tetapi juga $r(a-bi) = c(a-bi) + d = ca + d - cbi = 0 - 0.i = 0$. Jadi $a - bi$ adalah akar dari $r(x)$ dan juga akar dari $p(x)$, akibatnya juga merupakan akar dari $f(x)$ sebagaimana yang telah diharapkan.

Teorema 8.3.6 Misalkan $f(x)$ adalah suatu polinomial di $\mathbb{Q}[x]$. Bila $\alpha = a + b\sqrt{c}$ adalah suatu akar dari $f(x)$, dimana $a, b \in Q$ dan $\sqrt{c} \notin \mathbb{Q}$, maka $\bar{\alpha} = a - b\sqrt{c}$ juga merupakan akar dari $f(x)$.

Bukti

Tinjau polinomial

$$p(x) = x - (a+b\sqrt{c}))(x-(a-b\sqrt{c})) = x^2 - 2ax + (a^2 - b^2c) \in \mathbb{R}[x].$$

Gunakan algoritma pembagian, didapat $q(x), r(x) \in \mathbb{R}[x]$ yang memenuhi $f(x) = q(x)p(x) + r(x)$, dimana $r(x) = 0$ atau $\deg(r(x)) < \deg(p(x))$ yaitu derajat dari $r(x)$ adalah 0 atau 1. Jadi $r(x) = dx + e$ untuk beberapa $d, e \in \mathbb{R}$. Karena $0 = f(a+b\sqrt{c}) = q(a+b\sqrt{c}).0 + r(a+b\sqrt{c})$, maka $0 = r(a+b\sqrt{c}) = d(a+b\sqrt{c}) + e = (da+e) + db\sqrt{c}$. Jadi $da + e = db = 0$. Tetapi juga $r(a-b\sqrt{c}) = d(a-b\sqrt{c}) + e = da + e - db\sqrt{c} = 0 - 0.\sqrt{c} = 0$. Jadi $a - b\sqrt{c}$ adalah akar dari $r(x)$ dan juga akar dari $p(x)$, akibatnya juga merupakan akar dari $f(x)$ sebagaimana yang telah diharapkan.

Latihan

Latihan 8.3.1 Dapatkan semua zeros dari $f(x)$ dalam lapangan yang diberikan.

1. $f(x) = x^2 + x + 1$ dalam $\mathbb{Z}_3$.
2. $f(x) = x^3 + x^2 + x + 1$ dalam $\mathbb{R}$.
3. $f(x) = x^3 + x^2 + x + 1$ dalam $\mathbb{C}$.
4. $f(x) = x^8 - 1$ dalam $\mathbb{R}$.
5. $f(x) = x^4 - 4x^2 + 4$ dalam $\mathbb{R}$.
6. $f(x) = x^3 + 3x + 5$ dalam $\mathbb{Z}_7$.
7. $f(x) = x^4 + 4$ dalam $\mathbb{Z}_5$.

Latihan 8.3.2 Dalam lapangan $\mathbb{C}$, dapatkan semua akar tingkat-n dari satuan untuk $n = 2, n = 4$ dan $n = 6$. Selanjutnya tunukkan bahwa untuk masing-masing nilai n tersebut memebentuk subgrup siklik dari $\mathbb{C}^*$ berorder n.

Latihan 8.3.3 Dapatkan semua akar dari $x^2 - 1$ di $\mathbb{Z}_{15}$. Apakah hasilnya kontradiksi dengan Teorema 8.3.3?

Latihan 8.3.4 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $f(x)$ suatu polinomial di $\mathbb{F}[x]$. Tunjukkan bahwa bila $f(a) = 0$ untuk sebanyak takhingga elemen a di $\mathbb{F}$, maka $f(x)$ harus merupakan polinomial nol.

Latihan 8.3.5 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $f(x)$ dan $g(x)$ polinomial di $\mathbb{F}[x]$. Tunjukkan bahwa bila $f(x) \neq g(x)$, maka $f(a) = g(a)$ untuk setidaknya sebanyak berhingga a di $\mathbb{F}$.

Latihan 8.3.6 Dapatkan sisa pembagian $f(x) \in F[x]$ oleh $x - a$ dengan $a \in \mathbb{F}$ sebagaimana berikut.

1. $f(x) = x^3 + 3x^2 + 5x + 1, \quad a = 1, \quad F = \mathbb{Z}_7$.
2. $f(x) = x^5 + 4x^3 + 2x + 3, \quad a = 1, \quad F = \mathbb{Z}_5$.
3. $f(x) = x^3 + x^2 + 1, \quad a = -1, \quad F = \mathbb{Z}_3$.
4. $f(x) = x^5 + x^3 + x^2 + 1, \quad a = -1, \quad F = \mathbb{Q}$.
5. $f(x) = x^3 + x^2 - 1, \quad a = 2, \quad F = \mathbb{Z}_5$.

Latihan 8.3.7 Misalkan $\mathbb{F}$ suatu lapangan, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ suatu polinomial di $\mathbb{F}[x]$ dan misalkan a adalah suatu elemen taknol di $\mathbb{F}$. Tunjukkan bahwa bila $f(a) = 0$, maka a^{-1} adalah akar dari polinomial $g(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n$.

Latihan 8.3.8 Misalkan $a_1, \ldots, a_{n+1}$ elemen-elemen dari suatu daerah integral D yang semuanya berbeda dan $b_1, \ldots, b_{n+1}$ beberapa elemen di D. Tunjukkan bahwa ada setidaknya satu polinomial $f(x) \in D[x]$ yang berderajad $\leq n$ dengan $f(a_i) = b_i$ untuk $i = 1, \ldots, n + 1$.

Latihan 8.3.9 (**Interpolasi Langrange**) Misalkan $\mathbb{F}$ adalah suatu lapangan , $a_1, \ldots, a_{n+1}$ elemen-elemen di $\mathbb{F}$ yang semuanya berbeda dan $b_1, \ldots, b_{n+1}$ beberapa elemen di $\mathbb{F}$. Misalkan polinomial:

$$f(x) = \sum_{i=1}^{n+1} \frac{b_i(x-a_1)\cdots(x-a_{i-1})(x-a_{i+1})\cdots(x-a_{n+1})}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_{n+1})} .$$

Tunjukkan bahwa $f(x) \in \mathbb{F}[x]$ adalah polinomial tunggal berderajad n yang memenuhi $f(a_i) = b_i$ untuk semua $i = 1, \ldots, n+1$.

Latihan 8.3.10 Gunakan interpolasi Langrange untuk mendapatkan polinomial tunggal $f(x) \in \mathbb{R}[x]$ yang berderajad n sedemikian hingga graf dari $f(x)$ melalui titik dalam $\mathbb{R}^2$ sebagaimana berikut.

1. $n = 2$ titik: $(1,2), (2,4), (3,2)$
2. $n = 3$ titik: $(1,0), (2,-1), (3,0), (4,1)$
3. $n = 2$ titik: $(0,2), (1,0), (2,0)$.

8.4 Polinomial Tak-Tereduksi

Mendapatkan dan mempelajari akar dari suatu polinomial $f(x)$, atau solusi dari persamaan polinomial $f(x) = 0$, selalu menjadi bagian dasar aljabar. Teorema Pemfaktoran (Teorema 8.3.1) menunjukkan bahwa pemfaktoran suatu polinomial dan mendapatkan akar dari suatu polinomial merupakan masalah terkait erat. Pada bagian ini ditekankan pada faktorisasi dari suatu polinomial dengan koefisien di suatu lapangan $\mathbb{F}$. Pertama didefinisikan gagasan untuk $\mathbb{F}[x]$ yang sesuai dengan gagasan utama untuk $\mathbb{Z}$ dan ditunjukkan bahwa teorema faktorisasi tunggal berlaku di $\mathbb{F}[x]$ analog dengan teorema dasar aritmatika untuk $\mathbb{Z}$.

Definisi 8.4.1 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $f(x)$ polinomial di $\mathbb{F}[x]$ bukan konstan. Maka $f(x)$ adalah ***tak-tereduksi*** atas $\mathbb{F}$ bila $f(x)$ tidak bisa diungkapkan sebagai hasil perkalian $f(x) = g(x)h(x)$ dengan $g(x), h(x) \in \mathbb{F}[x]$ dan keduanya derajadnya kurang dari derajad $f(x)$. Bila tidak demikian maka $f(x)$ adalah ***tereduksi*** atas $\mathbb{F}$.

Ketak-tereduksian dari suatu polinomial atas suatu lapangan $\mathbb{F}$ bergantung pada macam lapangan $\mathbb{F}$, hal ini bisa terlihat dalam contoh-contoh berikut.

Contoh 8.4.1 Polinomial $f(x) = x^2 - 2$ tak-tereduksi atas lapangan $\mathbb{Q}$, tetapi $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ tereduksi atas lapangan $\mathbb{R}$.

Contoh 8.4.2 Polinomial $f(x) = x^2 + 1$ tak-terduksi atas lapangan $\mathbb{Q}$ dan $\mathbb{R}$, tetapi $f(x) = x^2 + 1 = (x - i)(x + i)$ tereduksi atas lapangan $\mathbb{C}$.

Teorema Dasar Aritmatika (Teorema 1.3.7), sebagaimana yang yelah dibahas dalam Bagian 1.3, merupakan konsekuensi penting dari algoritma pembagian untuk $\mathbb{Z}$. Karena telah dibuktikan algoritma pembagian untuk ring polinomial $\mathbb{F}[x]$ dimana $\mathbb{F}$ adalah suatu lapangan. Hal ini seharusnya tidak datang sebagai hal mengejutkan yang mana analog dengan adanya teorema dasar aritmatika untuk $F[x]$.

Teorema 8.4.1 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $f(x) \in \mathbb{F}[x]$ adalah tak-tereduksi atas $\mathbb{F}$. Bila $g(x), h(x) \in \mathbb{F}[x]$ dan $f(x) \mid g(x)h(x)$, maka $f(x) \mid g(x)$ atau $f(x) \mid h(x)$.

Bukti Misalkan $d(x) = \text{fpb}(f(x), g(x))$ yang mana keberadaannya dijamin oleh Teorema 8.2.2. Karena $d(x) \mid f(x)$ dan polinomial $f(x)$ tak-tereduksi, maka

(1) $\deg(d(x)) = \deg(f(x))$ dan $d(x) = af(x)$, dimana $a \in F$ dan $a \neq 0$, atau

(2) $\deg(d(x)) = 0$ dan $d(x) = c \in F$ dan $c \neq 0$.

Dalam kasus (1), karena $\text{fpb}(f(x), g(x)) = d(x)$, maka dapat dipilih $b(x) \in F[x]$ yang memenuhi $g(x) = b(x)d(x)$. Sehingga didapat $g(x) = (ab(x))f(x)$. Jadi $f(x) \mid g(x)$. Dalam kasus (2), gunakan Teorema 8.2.2, maka dapat dipilih $u(x), v(x) \in \mathbb{F}[x]$ yang memenuhi

$$c = u(x)f(x) + v(x)g(x)$$

Kedua ruas persamaan kalikan dengan $h(x)$ dan karena $c \neq 0$, maka didapat

$$h(x) = c^{-1}u(x)f(x)h(x) + c^{-1}v(x)g(x)h(x). \tag{8.4}$$

Tetapi $f(x) \mid g(x)h(x)$, maka dapat dipilih $q(x) \in \mathbb{F}[x]$ yang memenuhi

$$g(x)h(x) = q(x)f(x).$$

Substitusikan $g(x)h(x) = q(x)f(x)$ pada Persamaan (8.4) didapat

$$\begin{aligned} h(x) &= c^{-1}u(x)f(x)h(x) + c^{-1}v(x)g(x)h(x) \\ &= c^{-1}u(x)f(x)h(x) + c^{-1}v(x)q(x)f(x) \\ &= [c^{-1}u(x)h(x) + c^{-1}v(x)q(x)]f(x). \end{aligned}$$

Terlihat bahwa $f(x)$ adalah pembagi dari $h(x)$ atau $f(x) \mid h(x)$. ◪

Dari Teorema 8.4.1 yang baru saja dibahas dan bila digunakan secara berulang didapat kesimpulan berikut.

Akibat 8.4.1 Bila polinomial tak-terduksi $f(x)$ di $\mathbb{F}[x]$ dengan $\mathbb{F}$ adalah suatu lapangan dan $f(x)$ membagi hasil perkalian $g_1(x)g_2(x)\cdots g_n(x)$ dengan $g_i(x) \in F[x]$, $1 \leq i \leq n$, maka $f(x)$ membagi $g_i(x)$ untuk beberapa i, $1 \leq i \leq n$. ◪

Berikut ini diberikan teorema tentang daerah faktorisasi tunggal dari $\mathbb{F}[x]$ dimana $\mathbb{F}$ adalah suatu lapangan.

Teorema 8.4.2 (**Teorema Faktorisasi Tunggal**) Misalkan $f(x)$ polinomial taknol di $\mathbb{F}[x]$ dengan $\mathbb{F}$ adalah suatu lapangan. Maka $f(x)$ adalah suatu unit di $F[x]$ atau

$$f(x) = ap_1(x)p_2(x)\cdots p_m(x),$$

dimana masing-masing $p_i(x)$, $1 \leq i \leq m$ suatu polinomial monik tak-tereduksi di $\mathbb{F}[x]$ dan $a \in F$ adalah koefisien utama dari $f(x)$. Lagipula faktor-faktor $p_1(x), p_2(x), \ldots, p_m(x)$ adalah

tunggal kecuali urutan-urutannya.

Bukti :
Pertama ditunjukkan bahwa $f(x)$ dapat difaktorkan sebagaimana yang dikehendaki. Kedua ditunjukkan bahwa faktor-faktor tersebut tunggal.

Misalkan $f(x)$ polinomial tak-nol di $\mathbb{F}[x]$. Maka polinomial $f(x)$ adalah suatu unit yaitu $\deg(f(x)) = 0$ atau $\deg(f(x)) > 0$. Bila $\deg(f(x)) > 0$ dan koefisien utama dari $f(x)$ adalah a, maka dibuktikan bahwa $f(x)$ merupakan produk (hasil kali) dari a dengan sebanyak berhingga polinomial monik taktereduksi dari $\mathbb{F}[x]$. Bukti menggunakan induksi pada derajad dari $f(x)$.

Misalkan bahwa $\deg(f(x)) = 1$, maka $f(x) = b + ax$ untuk $a, b \in F$ dan $a \neq 0_F$. Sehingga didapat $f(x) = a(a^{-1}b + x)$, dimana $a^{-1}b + x$ adalah tak-terduksi di $\mathbb{F}[x]$. Dengan demikain untuk $\deg(f(x)) = 1$, teorema dipenuhi.

Selanjutnya asumsikan sebagai hipotisis induksi bahwa setiap polinomial di $\mathbb{F}[x]$ berderajad kurang dari n dapat difaktorkan sebagaimana dinyatakan dalam teorema. Diberikan sebarang polinomial $f(x)$ berderajad n dengan koefisien utamanya adalah a. Maka $f(x) = af_1(x)$ dimana $f_1(x) \in F[x]$ adalah monik. Bila $f(x)$ tak-tereduksi, maka $f_1(x)$ juga tak-tereduksi. Jadi teorema dipenuhi. Bila $f(x)$ tereduksi, maka dapat difaktorkan sebagai $f(x) = g(x)h(x)$ dimana $g(x)$ atau $h(x)$ bukan unit di $\mathbb{F}[x]$. Dalam hal ini $\deg(f(x)) = \deg(g(x)) + \deg(h(x))$ dan $g(x), h(x)$ bukan unit di $\mathbb{F}[x]$, maka masing-masing dari $g(x)$ dan $h(x)$ mempunyai derajad 1 atau lebih besar dari 1. Dengan demikan $g(x)$ dan $h(x)$ berderajad kurang dari n. Oleh karena itu, dengan hipotesis induksi didapat

$$g(x) = c\alpha_1(x)\alpha_2(x)\cdots\alpha_s(x) \quad \text{dan} \quad h(x) = d\beta_1(x)\beta_2(x)\cdots\beta_t(x),$$

dimana masing-masing $\alpha_i(x)$ adalah polinomial monik tak-terduksi, masing-masing $\beta_j(x)$ adalah polinomial monik tak-terduksi di $\mathbb{F}[x]$ dan masing-masing c dan d adalah koefisien utama dari $g(x)$ dan $h(x)$. Sehingga didapat

$$f(x) = cd\alpha_1(x)\alpha_2(x)\cdots\alpha_s(x)\beta_1(x)\beta_2(x)\cdots\beta_t(x).$$

Karena koefisien utama dari $f(x)$ adalah a dan masing-masing $\alpha_i(x)$ dan masing-masing $\beta_j(x)$ adalah polinonomial monik, maka haruslah $cd = a$. Jadi

$$f(x) = a\alpha_1(x)\alpha_2(x)\cdots\alpha_s(x)\beta_1(x)\beta_2(x)\cdots\beta_t(x).$$

Terlihat bahwa pemfaktoran dari $f(x)$ memenuhi persyaratan dalam teorema. Jadi teorema dipenuhi untuk semua polinomial di $\mathbb{F}[x]$ berderajad n dengan mengunakan prinsip induksi berlaku untuk semua polinomial berderajad sebarang.

Selanjutnya ditunjukkan bahwa pemfaktorannya adalah tunggal. Misalkan $f(x)$ diberikan oleh dua dekomposisi berikut.

$$f(x) = ap_1(x)p_2(x)\cdots p_m(x) = aq_1(x)q_2(x)\cdots q_n(x),$$

dimana masing-masing $p_i(x)$, $1 \leq i \leq m$ dan $q_j(x)$, $1 \leq j \leq n$ adalah polinomial monik takterduksi. Maka ditunjukkan bahwa $m = n$ dan masing-masing $p_i(x)$ sama dengan beberapa $q_j(x)$ dan sebaliknya. Dari dua dekomposisi $f(x)$ didapat

$$ap_1(x)p_2(x)\cdots p_m(x) = aq_1(x)q_2(x)\cdots q_n(x).$$

Perhatikan bahwa

$$p_i(x)|p_1(x)p_2(x)\cdots p_i(x)\cdots p_m(x).$$

Didapat

$$p_i(x)|q_1(x)q_2(x)\cdots q_j(x)\cdots q_n(x).$$

Berdasarkan Akibat 8.4.1, maka $p_i(x)$ membagi setidaknya satu dari

$$q_1(x), q_2(x), \ldots, q_j(x), \ldots, q_n(x).$$

Misalnya $p_i(x)|q_j(x)$, karena kedua dari $p_i(x)$ dan $q_j(x)$ adalah tak-tereduksi, maka $q_j(x) = up_i(x)$ dengan u adalah unit di $\mathbb{F}[x]$, yaitu u adalah elemen tak-nol di $\mathbb{F}$. Karena kedua dari $q_j(x)$ dan $p_i(x)$ adalah polinomial monik di $\mathbb{F}[x]$, maka haruslah $u = 1_F$. Jadi $p_i(x) = 1_F\, q_j(x) = q_j(x)$ dan karena $\mathbb{F}[x]$ adalah daerah integral serta komutatif didapat persamaan

$$p_1(x)p_2(x)\cdots p_{i-1}(x)p_{i+j}(x)\cdots p_m(x) = q_1(x)q_2(x)\cdots q_{j-1}(x)q_{j+1}(x)\cdots, q_n(x)$$

Proses dapat dilakukan secara berulang untuk $p_{i-1}(x)$ sehingga didapat $p_{i-1}(x) = q_{j-1}(x)$. Bila dalam hal ini andaikan $n > m$, maka setelah langkah pengulangan ke-m, sebelah kiri persamaan bernilai 1_F dan sebelah kanan persamaan adalah perkalian sebanyak $m - n$ dari polinomial monik $q_k(x)$ dan tak-tereduksi, maka $q_k(x)$ bukan unit di $\mathbb{F}[x]$. Jadi $q_k(x)$ bukan polinomial berderajad nol, dengan demikian hasil perkalian dari plonomial $q_k(x)$ adalah polinomial berderajad lebih besar dari 1. Karena

$$1_F \neq \prod_k q_k(x),$$

maka haruslah $n \not> m$ atau $n \leq m$. Untuk hal ini, lakukan hal yang sama pada

$$q_j(x)|q_1(x)q_2(x)\cdots q_j(x)\cdots q_n(x),$$

sehingga didapat $m \leq n$, jadi $n = m$. Juga dalam proses yang telah dilakukan $p_i(x)$ sama dengan beberapa $q_j(x)$ dan sebaliknya. Dengan begitu lengkap sudah bukti. ✓

Menentukan apakah suatu polinomial yang diberikan adalah tak-tereduksi atau bukan atas suatu lapangan bisa merupakan suatu pekerjaan yang sulit. Berikut ini diperkenalkan beberapa cara yang dapat digunakan untuk menunjukkan bahwa suatu polinomial adalah tak-tereduksi. Untuk mengawalinya, teorema pemfaktoran memberikan suatu kriteria yang berguna untuk ketak-tereduksian dari polinomial berderajad dua atau tiga.

Teorema 8.4.3 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x)$ polinomial di $\mathbb{F}[x]$ berderajad 2 atau 3. Maka $f(x)$ tereduksi atas $\mathbb{F}$ bila dan hanya bila $f(x)$ mempunyai akar di $\mathbb{F}$.

Bukti ($\Rightarrow$) Misalkan $f(x)$ tereduksi atas $\mathbb{F}$, sehingga didapat $f(x) = g(x)h(x)$ untuk beberepa polinomial $g(x)$ dan $h(x)$ keduanya berderajad lebih kecil dari derajad $f(x)$. Maka setidaknya satu dari $g(x)$ atau $h(x)$ berderajad 1 dengan kata lain mempunyai bentuk $a_1x + a_0$ untuk beberapa $a_0, a_1 \in F$ dengan $a_1 \neq 0_F$. Dengan demikian didapat $\alpha = -a_1^{-1}a_0 \in F$ adalah suatu akar dari $f(x)$.

($\Leftarrow$) Sebaliknya, bila $\alpha \in F$ adalah suatu akar dari $f(x)$, maka berdasarkan teorema pemfaktoran $f(x)$ dapat difaktorkan sebagai $f(x) = (x - \alpha)q(x)$ untuk beberapa polinomial $q(x) \in F[x]$ yang mempunyai derajad lebih kecil dari derajad $f(x)$. Jadi $f(x)$ adalah tereduksi. ✓

Contoh 8.4.3 Polinomial $f(x) = 2x^3 + x + 1$ tak-tereduksi atas lapangan $\mathbb{Z}_5$. Sebab, dengan cara yang mudah untuk semua $a \in \mathbb{Z}_5$ nilai $f(a)$ sebagai berikut:

$$f(0) = 1, f(1) = 4, f(2) = 4, f(3) = 3 \text{ dan } f(4) = 3.$$

Terlihat bahwa untuk semua $a \in \mathbb{Z}_5$ nilai $f(a) \neq 0$. Jadi $f(x) = 2x^3 + x + 1$ tak-tereduksi atas lapangan $\mathbb{Z}_5$. ●

Contoh 8.4.4 Polinomial $f(x) = x^2+x+1$ tereduksi atas lapangan $\mathbb{Z}_3$. Sebab $f(x) = (x+2)(x+1)$ dan $f(1) = (1 + 2)(1 + 1) = 0$. Tetapi $f(x) = x^2 + x + 1$ tak-tereduksi atas lapangan $\mathbb{Q}$, sebab hal ini bisa ditunjukkan bahwa $f(x) = x^2 + x + 1$ tidak mempunyai akar-akar di $\mathbb{Q}$ sebagai berikut. Karena akar-akar di $\mathbb{C}$ dari

$$x^3 - 1 = (x - 1)(x^2 + x + 1),$$

adalah $1, -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ dan $-\frac{1}{2} - \frac{\sqrt{3}}{2}i$. Terlihat bahwa $f(x) = x^2 + x + 1$ tidak mempunyai akar di $\mathbb{Q}$. Jadi $f(x) = x^2 + x + 1$ tak-tereduksi atas lapangan $\mathbb{Q}$. ●

Contoh berikut menunjukkan bahwa Teorema 8.4.3 hanya berlaku untuk polinomial $f(x)$ berderajad 2 atau 3 atas suatu lapangan $\mathbb{F}$. Sedangkan untuk derajad yang lebih besar walaupun $f(x)$ tidak memiliki akar di $\mathbb{F}$, polinomial $f(x)$ tereduksi.

Contoh 8.4.5 Diberikan polinomial $f(x) = x^4 + 2x^2 + 1 \in \mathbb{Q}$ adalah tereduksi, sebab

$$f(x) = x^4 + 2x^2 + 1 = (x^2 + 1)^2 = (x^2 + 1)(x^2 + 1),$$

semua akar yang mungkin adalah $a = \pm i \in \mathbb{C}$ dan jelas bahwa $a = \pm i \notin \mathbb{Q}$. ●

Catatan Untuk Polinomial di $\mathbb{F}[x]$ tak-tereduksi, dimana $\mathbb{F}$ adalah lapangan

1. Suatu elemen $p(x)$ di $\mathbb{F}[x]$ adalah ***tak-tereduksi*** bila $p(x)$ bukan elemen nol dan bukan suatu unit, dan bila $p(x) = a(x)b(x)$, maka $a(x)$ adalah unit atau $b(x)$ adalah unit. Karena unit di $\mathbb{F}[x]$ adalah semua polinomial taknol yang berderajad nol, maka $u \in \mathbb{F}$ dengan $u \neq 0_{\mathbb{F}}$ adalah suatu unit di $\mathbb{F}[x]$. Dengan demikian bila $\deg(p(x)) = n$, $n \geq 1$, maka salah satu dari berikut yang memenuhi $\deg(a(x)) = n$ atau $\deg(b(x)) = n$. Bila $\deg(a(x)) = n$, maka $\deg(b(x)) = 0$ dengan demikian $b(x)$ adalah unit di $\mathbb{F}[x]$ dan $b(x) = b \in \mathbb{F}$. Begitu juga sebaliknya, bila $\deg(b(x)) = n$, maka $\deg(a(x)) = 0$. Jadi $a(x)$ adalah unit di $\mathbb{F}[x]$ dan $a(x) = a \in \mathbb{F}$.

2. Sebarang polinomial $p(x) = ax + b \in F[x]$ dimana $a, b \in \mathbb{F}$ dan $a \neq 0_{\mathbb{F}}$. Maka

   $$ax + b = a(x + a^{-1}b),$$

   jelas a adalah unit di $\mathbb{F}[x]$ dan $\deg(ax + b) = \deg(x + a^{-1}b)$. Jadi $p(x) = ax + b$ adalah tak-tereduksi dan $ax + b$ berasosiasi dengan $x + a^{-1}b$.

3. Bila $p(x) = ax^2 + bx + c \in F[x]$, dimana $a, b, c \in F$ dan $a \neq 0_{\mathbb{F}}$. Jika $p(x)$ tak-tereduksi, maka

   $$p(x) = ax^2 + bx + c = a(x^2 + \frac{b}{a}x + \frac{c}{a}) = aq(x),$$

dimana $q(x) = x^2 + \frac{b}{a}x + \frac{c}{a}$ adalah polinomial monik (koefisien pangkat tertingginya sama dengan satu) dan $q(x)$ tidak bisa difaktorkan dalam $\mathbb{F}[x]$. Bila $q(x)$ bisa difaktorkan, maka

$$q(x) = (x - x_1)(x - x_2),\ x_1, x_2 \in \mathbb{F}.$$

Didapat $q(x_1) = q(x_2) = 0_F$, jadi x_1 dan x_2 adalah akar dari $q(x)$ dan masing-masing polinomial $x - x_1$ dan $x - x_1$ bukan unit di $\mathbb{F}[x]$. Sehinggaa didapat

$$p(x) = aq(x) = a(x - x_1)(x - x_2) = (ax - ax_1)(x - x_2),$$

dengan masing-masing polinomial $ax - ax_1$ dan $x - x_2$ bukan unit di $\mathbb{F}[x]$. Jadi $p(x)$ tereduksi hal ini bertentangan dengan kenyataan $p(x)$ tak-tereduksi. Jadi $p(x) = ax^2 + bx + c \in F[x]$ tak-tereduksi bila dan hanya bila $p(x)$ tidak mempunyai akar di $\mathbb{F}$. Akibatnya $p(x) = ax^2 + bx + c$ tereduksi di $\mathbb{F}[x]$ bila dan hanya bila $p(x)$ mempunyai akar di $\mathbb{F}$. Bila $\mathbb{F} = \mathbb{R}$, maka $p(x) = ax^2 + bx + c \in \mathbb{R}[x]$ tak-tereduksi bila dan hanya bila $D = b^2 - 4ac < 0$ dan tereduksi bila dan hanya bila $D = b^2 - 4ac \geq 0$.

4. Bila $p(x) \in \mathbb{F}[x]$ dengan $\deg(p(x)) = 3$, maka pernyataan $p(x)$ tereduksi bila dan hanya bila $p(x)$ mempunyai akar di $\mathbb{F}$ masih berlaku. Pembahasan ini sebagaimana telah dibuktikan dalam Teorema 8.4.3. Tetapi bila $\deg(p(x)) \geq 4$ pernyataan tersebut bisa tidak benar, hal ini telah diberikan dalam Contoh 8.4.5. Juga, misalnya, diberikan polinomial $p(x) = (x^2 - 3)^2 = (x^2 - 3)(x^2 - 3) \in \mathbb{Q}[x]$ tereduksi, sebab $x^2 - 3$ bukan unit di $\mathbb{Q}[x]$, dan $p(x)$ tidak mempunyai akar di $\mathbb{Q}$. Begitu juga polinomial $p(x) = (x^2 - 3)(x^2 - 5) \in \mathbb{Q}[x]$ tereduksi sebab masing-masing $x^2 - 3$ dan $x^2 - 5$ bukan unit di $\mathbb{Q}[x]$, juga $p(x)$ tidak mempunyai akar di $\mathbb{Q}$.

5. Pernyataan bahwa $p(x) \in F[x]$ tak-tereduksi bergantung pada lapangan $\mathbb{F}$. Hal ini bukan merupakan sifat yang mutlak. Misalnya polinomial $p(x) = x^2 - 6 \in \mathbb{Q}[x]$ tak-tereduksi di $\mathbb{Q}[x]$ sebab aka-akar dari $p(x) = x^2 - 6$ adalah $\pm\sqrt{6} \notin \mathbb{Q}$. Tetapi $p(x) = x^2 - 6 = (x - \sqrt{6})(x + \sqrt{6})$ tereduksi di $\mathbb{R}[x]$.

Berikut ini diberikan teorema tentang akar pecahan dari polinomial dengan koefisien di $\mathbb{Z}$.

Teorema 8.4.4 Misalkan $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 \in \mathbb{Z}[x]$. Bila $a = \frac{p}{q}$, dengan FPB$(p, q) = 1$ adalah akar pecahan dari $f(x)$, maka $p|a_0$ dan $q|a_n$.

Bukti
Karena $a = \frac{p}{q}$ akar dari $f(x)$ didapat

$$f(a) = a_n\left(\frac{p}{q}\right)^n + a_{n-1}\left(\frac{p}{q}\right)^{n-1} + \cdots + a_1\frac{p}{q} + a_0 = 0$$

Sehingga didapat

$$a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n = 0$$

Karena

$$p|a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} \quad \text{dan} \quad p|0,$$

maka $p|a_0 q^n$. Karena FPB$(p, q) = 1$, maka FPB$(p, q^n) = 1$. Akibatnya $p|a_0$. Juga karena

$$q|a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n \quad \text{dan} \quad q|0,$$

maka $q|a_n p^n$ dan karena FPB$(p, q) = 1$, maka FPB$(p^n, q) = 1$.Akibatnya $q|a_n$.

Kebalikan dari Teorema 8.4.4 yang baru saja dibahas tidak berlaku. Sebagaimana ditunjukkan dalam contoh berikut.

Contoh 8.4.6 Misalnya diberikan polinomial

$$f(x) = 2x^3 + 2x^2 + 5 \in \mathbb{Q}[x].$$

Bila $f(x)$ mempunyai akar $a = \frac{p}{q}$, maka $p|5$ dan $q|2$. Sehingga didapat:

$$p = \pm 1, \pm 5 \quad \text{dan} \quad q = \pm 1, \pm 2.$$

Dengan demikian semua akar dari $f(x)$ yang mungkin adalah

$$\pm 1, \pm 5, \pm \frac{1}{2} \text{ dan } \pm \frac{5}{2}.$$

Diselidiki apakah semua akar yang mungkin merupakan akar dari polinomial $f(x)$ sebagai berikut:
$f(1) = 2 + 2 + 5 = 9 \neq 0, \quad f(-1) = -2 + 2 + 5 = 5 \neq 0,$
$f(5) = 250 + 50 + 5 = 305 \neq 0, \quad f(-5) = -250 + 50 + 5 = -195 \neq 0,$
$f(1/2) = 2/8 + 2/4 + 5 = 23/4 \neq 0, \quad f(-1/2) = -2/8 + 2/4 + 5 = 21/4 \neq 0$
dan
$f(1/5) = 2(125/8) + 2(25/4) + 5 = 195/4 \neq 0,$
$f(-1/5) = -2(125/8) + 2(25/4) + 5 = -55/4 \neq 0.$

Terlihat bahwa semua akar yang mungkin dari $f(x)$ bukan merupakan akar dari $f(x)$. Jadi $f(x) = 2x^3 + 2x^2 + 5 \in \mathbb{Q}[x]$ tidak mempunyai akar di $\mathbb{Q}$, dengan demikian $f(x) = 2x^3 + 2x^2 + 5$ adalah tak-tereduksi di $\mathbb{Q}[x]$. ●

Definisi 8.4.2 Misalkan $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Maka $k = \text{FPB}(a_n, \ldots, a_0)$ dinamakan ***konten*** dari $f(x)$ dan bila $k = 1$, maka $f(x)$ dinamakan polinomial ***primitif***. Perluh diperhatikan bahwa bila $g(x)$ mempunyai konten k, maka $g(x) = kg_1(x)$ dimana $g_1(x)$ adalah polinomial primitif. ✓

Lemma 8.4.1 (**Gauss**) Misalkan $f(x)$ dan $g(x)$ adalah polinomial primitif di $\mathbb{Z}[x]$. Maka hasil kali $f(x)g(x)$ juga polinomial primitif.

Bukti Dibuktikan lemma melalui kontradiksi. Andaikan $f(x)g(x)$ bukan polinomial primitif dan misalkan p suatu bilangan prima yang membagi konten dari $f(x)g(x)$. Digunakan homomorpisma $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ dimana $\phi(f(x)) = \overline{f(x)} \in \mathbb{Z}_p[x]$, untuk semua $f(x) \in \mathbb{Z}[x]$. Karena $p|k$, dimana k adalah konten dari $f(x)g(x)$, maka didapat $\overline{f(x)g(x)} = \overline{0}$. Tetapi $\overline{f(x)g(x)} = \overline{f(x)}\ \overline{g(x)}$, sehingga didapat $\overline{f(x)}\ \overline{g(x)} = \overline{0}$ dan karena $\mathbb{Z}_p[x]$ adalah daerah integral, maka $\overline{f(x)} = \overline{0}$ atau $\overline{g(x)} = \overline{0}$. Hal ini berakibat semua koefisien dari $f(x)$ atau $g(x)$ bisa dibagi oleh p. Hal ini menunjukkan $f(x)$ atau $g(x)$ adalah bukan primitif. Hal ini bertentangan dengan kenyataan bahwa $f(x)$ dan $g(x)$ adalah primitif. Jadi haruslah $f(x)g(x)$ adalah primitfif. ✓

Teorema 8.4.5 Misalkan $f(x)$ suatu polinomial taknol di $\mathbb{Z}[x]$. Maka $f(x)$ dapat difaktorkan menjadi perkalian dua polinomial berderajad r dan s di $\mathbb{Q}[x]$ bila dan hanya bila $f(x)$ juga bisa difaktorkan kedalam hasil kali dua polinomial yang mempunyai derajad sama r dan s di $\mathbb{Z}[x]$.

Bukti Dibuktikan bahwa bila $f(x) = g(x)h(x)$ dengan masing-masing $\deg(g(x)) = r$ dan $\deg(h(x)) = s$ di $\mathbb{Q}[x]$, maka dapat dipilih polinomial $g_1(x), h_1(x) \in \mathbb{Z}[x]$ dengan $\deg(g_1(x)) = r$ dan $\deg(h_1(x)) = s$ yang memenuhi $f(x) = g_1(s)h_1(x)$. Cukup dibuktikan untuk polinomial primitif. Maka bila $f(x)$ sebarang polinomial taknol dapat ditulis $f(x) = kf_1(x)$ dimana k adalah konten dari $f(x)$ dan $f_1(x)$ adalah polinomial primitif dan sebarang pemfaktoran dari $f(x)$ menjadi $f(x) = g(x)h(x)$ di $\mathbb{Q}[x]$ akan memberikan

$$f_1(x) = (k^{-1}g(x))h(x) \quad \text{di} \quad \mathbb{Q}[x].$$

Gunakan teorema pada $f_1(x)$ untuk memperoleh suatu pemfaktoran $f_1(x) = g_1(x)h_1(x)$ di $\mathbb{Z}[x]$ sehingga didapat suatu pemfaktoran $f(x) = (kg_1(x))h_1(x)$ di $\mathbb{Z}[x]$. Jadi bila diberikan pemfaktoran $f(x) = g(x)h(x)$ di $\mathbb{Q}[x]$ dengan $f(x)$ adalah suatu polinomial primitif di $\mathbb{Z}[x]$, misalkan a adalah KPK dari semua penyebut koefisien $g(x)$ yang ditulis dalam suku-suku terkecil dan b juga sama merupakan KPK dari semua penyebut koefisien $h(x)$. Maka $ag(x)$ dan $bh(x)$ adalah polinomial di $\mathbb{Z}[x]$, jadi $abf(x) = (ag(x))(bh(x))$. Selanjutnya tulis $ag(x) = kg_1(x)$ dan $bh(x) = dh_1(x)$ dimana masing-masing k dan d adalah konten dari $ag(x)$ dan $bh(x)$ dan $g_1(x), h_1(x)$ adalah polinomial primitif di $\mathbb{Z}[x]$. Karena $f(x)$ polinomial primitif, konten dari $abf(x)$ adalah ab, maka dengan menggunakan Lemma Gauss 8.4.1, $g_1(x)h_1(x)$ adalah primitif. Dengan demikian kd adalah konten dari $(kg_1(x))(dh_1(x)) = abf(x)$.Sehingga didapat $ab = kd$ dan karena$abf(x) = kdg_1(x)h_1(x)$ maka didapat $f(x) = g_1(x)h_1(x)$ adalah pemfaktoran dari $f(x)$ di $\mathbb{Z}[x]$, dimana derajad dari $g_1(x)$ sama dengan derajad dari $kg_1(x) = ag(x)$ akibatnya sama dengan derajad dari $g(x)$. Begitu juga halnya derajad dari $h_1(x)$ sama dengan derajad dari $h(x)$. Bukti sebaliknya didapat secara langsung. ✓

Contoh 8.4.7 Diberikan polinomial $f(x) = 6x^3 + 4x^2 - 3x - 2 \in \mathbb{Z}[x]$. Maka FPB$(6, 4, 3, 2) = 1$, jadi $f(x)$ adalah primitif. Selanjutnya pemfaktoran dari $f(x)$ di $\mathbb{Q}[x]$ diberikan oleh

$$f(x) = \left(\frac{9}{2}x + 3\right)\left(\frac{4}{3}x^2 - \frac{2}{3}\right),$$

dengan menggunakan notasi bukti Teorema 8.4.5 didapat

$$r = 1, s = 2, a = 2, b = 3, k = 3, d = 2.$$

Jadi

$$ag(x) = 9x + 6 = 3(3x + 2) = kg_1(x)$$

dan

$$bh(x) = 4x^2 - 2 = 2(2x^2 - 1) = dh_1(x).$$

Sehingga didapat pemfaktoran dari $f(x)$ di $\mathbb{Z}[x]$ adalah

$$f(x) = g_1(x)h_1(x) = (3x + 2)(2x^2 - 1). \quad ●$$

Contoh berikut menggunakan Teorema 8.4.5 untuk menjukkan bahwa suatu polinomial adalah tak-tereduksi.

Contoh 8.4.8 Tunjukkan bahwa polinomial $f(x) = x^4 - 5x^2 + 6x + 1 \in \mathbb{Q}[x]$ adalah tak-tereduksi.

Jawab
Bila $f(x)$ mempunyai akar, maka kemungkinan akar-akarnya adalah ± 1. Tetapi hal ini menghasilkan $f(1) = 3 \neq 0$ dan $f(-1) = -9 \neq 0$. Jadi ± 1 bukan akar dari $f(x)$. Selanjutnya bila $f(x)$ mempunyai pembagi yang berderajad 2, maka

$$f(x) = x^4 - 5x^2 + 6x + 1 = (x^2 + ax + b)(x^2 + cx + d),$$

maka menurut teorema yang telah dibahas maka a, b, c, d dapat merupakan bilangan bulat. Selanjutnya

$$(x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (bc + ad)x + bd.$$

Dengan menyamakan koefisien dari polinomial didapat

$$a + c = 0,\ b + d + ac = -5,\ bc + ad = 6 \quad \text{dan} \quad bd = 1.$$

Karena $a, b, c, d \in \mathbb{Z}$, maka dari $bd = 1$ didapat $b = d = \pm 1$ dan dari $bc + ad = 6$ didapat $a + c = \pm 6$. Hal ini bertentangan dengan kenyataan $a + c = 0$ Hal ini menunjukkan $f(x)$ tidak bisa difaktorkan di $\mathbb{Z}[x]$ dengan demikian juga tidak bisa difaktorkan dalam $\mathbb{Q}[x]$. Jadi $f(x)$ adalah tak-tereduksi di $\mathbb{Q}[x]$. ●

Teorema berikut menjelaskan kriteria suatu polinomial di $\mathbb{Z}[x]$ tak-tereduksi di $\mathbb{Q}[x]$.

Teorema 8.4.6 (**Kriteria Eisenstein**) Misalkan

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0 \in \mathbb{Z}[x].$$

Misalkan ada suatu bilangan prima p yang memenuhi

(1) p tidak membagi a_n,

(2) p membagi a_i untuk semua $i < n$,

(3) p^2 tidak membagi a_0.

Maka $f(x)$ tak-tereduksi di $\mathbb{Q}[x]$.

Bukti
Andaikan $f(x)$ tereduksi di $\mathbb{Q}[x]$. Berdasarkan pembahasan teorema yang terdahulu, maka $f(x)$ tereduksi di $\mathbb{Z}[x]$, yaitu

$$f(x) = (b_r x^r + \cdots + b_0)(c_s x^2 + \cdots + c_0),$$

dimana b_i dan c_i adalah bilangan bulat, r dan s bilangan bulat taknol dan $r + s = n$. Suku konstan a_0 dari $f(x)$ harus sama dengan $b_0 c_0$, jadi $a_0 = b_0 c_0$. Dari kondisi (3) diketahui bahwa p^2 tidak membagi a_0, akibatnya p tidak membagi b_0 dan c_0. Sedangkan dari kondisi (2) p membagi $a_0 = b_0 c_0$, maka p membagi salah satu b_0 atau c_0. Misalkan dalam hal ini p membagi b_0 dan tidak membagi c_0. Koefisien utama a_n dari $f(x)$ harus sama dengan $b_r c_s$. Dari kondisi (1) p tidak membagi $a_n = b_r c_s$. Jadi p tidak membagi b_r atau c_s. Misalkan m adalah bilangan bulat terkecil yang mana p tidak membagi b_m, dengan kata lain, p membagi b_i untuk $i < m$,

tetapi p tidak membagi b_m. Tentunya dalam hal ini $1 \leq m \leq r < n$. Selanjutnya ditinjau koefisien a_m dalam $f(x)$ yang diberikan oleh

$$a_m = b_m c_0 + b_{m-1}c_1 + \cdots + b_1 c_{m-1} b_0 c_m.$$

Disini p membagi semua b_i untuk $i < n$, tetapi p tidak membagi b_m atau c_0. Hal ini menunjukkan bahwa p tidak membagi a_m, dimana $m < n$. Hal ini bertentangan dengan kenyataan kondisi (2). Jadi haruslah $f(x)$ tak-tereduksi di $\mathbb{Q}[x]$. ✓

Contoh 8.4.9 Misalkan $f(x) = 10x^7 - 6x^3 + 27x + 12 \in \mathbb{Z}[x]$. Untuk $p = 3$ dan $p^2 = 9$. Jelas bahwa $p = 3$ membagi semua $12, 27, 6$ dan $p = 3$ tidak membagi 10, juga $p^2 = 9$ tidak membagi 12. Sehingga dengan menggunakan kriteria Eisenstein, $f(x)$ tak-terduksi di $\mathbb{Q}[x]$. ●

Kriteria Eisenstein dapat digunakan pada polinomial ***siklotomik***.

Definisi 8.4.3 Diberikan polinomial $x^n - 1$ yang mempunyai n akar-akar dari satuan. Sebab 1 jelas akar dari $x^n - 1$, jadi $x - 1$ adalah suatu pembagi dari $x^n - 1$. Kenyataannya, hasil bagi dapat dihitung:

$$(x^n - 1) = (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1).$$

Bila p adalah suatu bilangan prima, maka polinomial $\Phi_p(x)$ didefinisikan oleh

$$\Phi_p(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \cdots + x + 1,$$

dinamakan polinomial ***siklotomik*** untuk p. ✓

Akibat 8.4.2 Untuk sebarang p prima, polinomial siklotomik $\Phi_p(x)$ adalah tak-tereduksi di $\mathbb{Q}[x]$.

Bukti Disini kriteria Eisenstein tidak bisa langsung digunakan. Tetapi, tinjau $f(x) = \Phi_p(x + 1)$. Sebarang faktorisasi $\Phi_p(x) = g(x)h(x)$ akan juga memberikan suatu faktorisasi $f(x) = g_1(x)h_1(x)$, dimana $g_1(x) = g(x+1)$ dan $h_1(x) = h(x+1)$. Jadi bila $\Phi_p(x)$ tereduksi di $\mathbb{Q}[x]$, maka $f(x)$ juga tereduksi di $\mathbb{Q}[x]$. Dengan menggunakan Teorema binomial didapat

$$f(x) = ((x + 1)^{p-1} - 1)/((x + 1) - 1) = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \cdots + \binom{p}{2}x + p,$$

dimana $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ dan jelas bahwa p membagi $\binom{p}{k}$ juga p^2 tidak membagi p dan p tidak membagi 1. Maka menurut kriteria Einsenstein $f(x)$ tak-tereduksi di $\mathbb{Q}[x]$. Dengan demikian $\Phi_p(x)$ tak-tereduksi di $\mathbb{Q}[x]$. ✓

Contoh 8.4.10 Dari pembahasan kesimpulan, maka $f(x) = \Phi_5(x) = x^4 + x^3 + x^2 + x + 1$ adalah tak-tereduksi di $\mathbb{Q}[x]$. Tetapi $g(x) = x^3 + x^2 + x + 1$ tereduksi di $\mathbb{Q}[x]$, sebab $g(-1) = 0$. Sehingga didapat pemfaktoran

$$g(x) = (x + 1)(x^2 + 1). \quad ●$$

Teorema berikut juga dapat digunakan untuk menentukan suatu polinomial tak-tereduksi di $\mathbb{Q}[x]$.

Teorema 8.4.7 Misalkan $f(x) \in \mathbb{Z}[x]$ dengan $\deg(f(x)) \geq 1$. Untuk suatu bilangan prima p, polininomial $\overline{f(x)} \in \mathbb{Z}_p[x]$ diperoleh dari $f(x) \in \mathbb{Z}[x]$ dengan melakukan semua koefisien menjadi modulo p. Bila $\deg(f(x)) = \deg(\overline{f(x)})$ dan $\overline{f(x)}$ tak-tereduksi di $\mathbb{Z}_p[x]$, maka $f(x)$ tak-tereduksi di $\mathbb{Z}[x]$.

Bukti
Pemetaan $\phi : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, yang diberikan oleh $\phi(f(x)) = \overline{(f(x))}, \forall f(x) \in \mathbb{Z}[x]$ adalah suatu homomorpisma ring. Andaikan $f(x)$ tereduksi di $\mathbb{Q}[x]$, maka $f(x)$ dapat difaktorkan $f(x) = g(x)h(x)$ di $\mathbb{Z}[x]$ dimana $\deg(g(x)) < \deg(f(x))$ dan $\deg(h(x)) < \deg(f(x))$. Sehingga didapat

$$\overline{f(x)} = \overline{g(x)h(x)} = \overline{g(x)}\,\overline{h(x)},$$

dimana $\deg(\overline{g(x)}) \leq \deg(g(x)) < \deg(\overline{f(x)})$ dan juga $\deg(\overline{h(x)}) < \deg(\overline{f(x)})$. Dengan demikian $\overline{f(x)}$ tereduksi di $\mathbb{Z}_p[x]$. Hal ini bertentangan dengan kenyataan bahwa $\overline{f(x)}$ tak-tereduksi di $\mathbb{Z}_p[x]$. Jadi haruslah $f(x)$ tak-tereduksi di $\mathbb{Q}[x]$. ✓

Contoh 8.4.11 Misalkan $f(x) = 7x^3 - 6x^2 + 3x + 9 \in \mathbb{Z}[x]$, maka $\overline{f(x)} = x^3 + x + 1 \in \mathbb{Z}_2[x]$ tetap mempunyai derajad 3 dan tak-tereduksi. Sebab $\overline{f(0)} = \overline{f(1)} = \overline{1}$. Jadi $f(x)$ tak-tereduksi di $\mathbb{Q}[x]$. Perluh diperhatikan bahwa bilangan prima $p = 2$ suatu hal yang penting untuk menentukan bahwa $\overline{f(x)}$ tak-tereduksi di $\mathbb{Z}_2[x]$. Bila $p = 2$ diganti dengan nilai prima yang lain, misal $p = 3$, maka didapat $\overline{f(x)} = x^3 \in \mathbb{Z}_3[x]$. Jelas bahwa $\overline{f(x)} = x^3$ tereduksi di $\mathbb{Z}_3[x]$. Sehingga $p = 3$ tidak bisa digunakan untuk menguji ketak-tereduksian dari $f(x)$ di $\mathbb{Q}[x]$. ●

Contoh 8.4.12 Misalkan $f(x) = 3x^4 - 6x^3 + 10x^2 - 5x + 9 \in \mathbb{Z}[x]$, maka $\overline{f(x)} = x^4 + x + 1 \in \mathbb{Z}_2[x]$ mempunyai derajad 3. Polinomial $\overline{f(x)} = x^4 + x + 1$ tidak mempunyai akar di $\mathbb{Z}_2[x]$ sebab $\overline{f(0)} = \overline{f(1)} = \overline{1}$. Selanjutnya bila $\overline{f(x)} = x^4 + x + 1$ mempunyai pembagi yang berderajad 2, maka didapat

$$x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d).$$

Dengan menyamakan koefisien kedua ruas persamaan, didapat

$$bd = 1, bc + ad = 1, b + d + ac = 0 \quad \text{dan} \quad a + c = 0.$$

Kondisi yang didapat tidak pernah tercapai sebab $bd = 1$ berakibat $b = d = 1$. Sehingga $1 = bc + ad = b(a + c) = a + c$. Hal ini bertentangan dengan kondisi $a + c = 0$. Karena $\overline{f(x)}$ tidak bisa difaktorkan kedalam bentuk linier dan bentuk kuadrat, maka $\overline{f(x)}$ tak-tereduksi di $\mathbb{Z}_2[x]$. Akibatnya, $f(x)$ tak-tereduksi di $\mathbb{Q}[x]$. ●

Latihan

Latihan 8.4.1 Faktorkan menjadi polinomial-polinomial tak-tereduksi untuk masing-masing polinomial $f(x)$ di $\mathbb{F}[x]$ berdasarkan lapangan $\mathbb{F}$ yang diberikan.

1. $f(x) = x^4 - 1$ $\quad\quad$ $\mathbb{F} = \mathbb{R}$, $F = \mathbb{C}$
2. $f(x) = x^4 + 1$ $\quad\quad$ $\mathbb{F} = \mathbb{Z}_2$
3. $f(x) = x^4 + 4$ $\quad\quad$ $\mathbb{F} = \mathbb{Z}_5$

4. $f(x) = x^3 + 4x^2 + 5x + 2$ $\mathbb{F} = \mathbb{Z}_7$
5. $f(x) = x^2 + 2x - 1$ $\mathbb{F} = \mathbb{Z}_7$
6. $f(x) = x^2 + x + 3$ $\mathbb{F} = \mathbb{Z}_5$
7. $f(x) = x^2 + x + 1$ $\mathbb{F} = \mathbb{Q}$, $\mathbb{C}$
8. $f(x) = x^3 + x^2 + x + 1$ $\mathbb{F} = \mathbb{Z}_5$, $\mathbb{Q}$, $\mathbb{C}$.

Latihan 8.4.2 Tunjukkan bahwa $f(x) = x^3 + 2x + 1$ adalah tak-tereduksi atas $\mathbb{Z}_5$.

Latihan 8.4.3 Tunjukkan bahwa $f(x) = x^3 + x + 1$ adalah tak-tereduksi atas $\mathbb{Z}_7$.

Latihan 8.4.4 Tunjukkan bahwa $f(x) = x^4 - 2$ adalah tak-tereduksi atas $\mathbb{Q}$ tetapi tereduksi atas $\mathbb{R}$.

Latihan 8.4.5 Tunjukkan bahwa $f(x) = x^4 - 2x^2 - 4$ adalah tak-tereduksi atas $\mathbb{Q}$.

Latihan 8.4.6 Dapatkan semua akar dari masing-masing polinomial $f(x)$ sesuai atas lapangan yang diberikan.

1. $f(x) = x^3 + 2x^2 - 5x - 6$ atas lapangan $F = \mathbb{Q}$.
2. $f(x) = x^4 - 2x^2 - 4$ atas lapangan $F = \mathbb{R}$.
3. $f(x) = x^4 - 2x^2 - 4$ atas lapangan $F = \mathbb{C}$.
4. $f(x) = x^4 - x^3 - 8x^2 + 11x - 3$ atas lapangan $F = \mathbb{R}$.
5. $f(x) = x^4 - 3x^3 + 3x^2 - 6x + 2$ atas lapangan $F = \mathbb{C}$.
6. $f(x) = x^4 + x^3 + 3x^2 + 2x + 2$ atas lapangan $F = \mathbb{C}$.

Latihan 8.4.7 Tentukan bila mungkin dengang menggunakan kriteria teorema yang telah dibahas dalam bagian ini untuk menentukan masing-masing polinomial $f(x)$ di $\mathbb{Z}[x]$ adalah tereduksi atas lapangan $\mathbb{Q}$. Jelaskan jawaban saudara.

1. $f(x) = 10x^7 - 6x^4 + 15x^2 + 18x - 6$.
2. $f(x) = x^4 - 4x^2 + 4x - 1$.
3. $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$.
4. $2x^4 + x^3 - 2x^2 + x + 1$.
5. $3x^4 + 5x + 1$.
6. $x^6 + 2x^3 - 3x^2 + 1$.
7. $f(x) = x^4 + 4$.

Latihan 8.4.8 Buat suatu contoh baru dari suatu polinomial $f(x)$ di $\mathbb{Z}[x]$ yang tak-tereduksi atas $\mathbb{Q}$ tetapi tereduksi atas $\mathbb{R}$.

Latihan 8.4.9 Buat suatu contoh baru dari suatu polinomial $f(x)$ di $\mathbb{Z}[x]$ yang tak-tereduksi atas $\mathbb{Q}$ walaupun $\overline{f(x)}$ di $\mathbb{Z}_p[x]$ adalah tereduksi atas $\mathbb{Z}_p$ untuk setiap bilangan bulat prima p.

Latihan 8.4.10 Dapatkan semua polinomial berderajad 2 yang tak-tereduksi atas lapangan $\mathbb{Z}_3$.

Latihan 8.4.11 Untuk sebarang bilangan bulat prima p, tunjukkan bahwa banyaknya polinomial $x^2 + ax + b$ yang tak-tereduksi atas $\mathbb{Z}_p$ adalah $\frac{p(p-1)}{2}$.

Latihan 8.4.12 Untuk sebarang bilangan bulat prima p dan sebarang a di $\mathbb{Z}_p$, tunjukkan bahwa $x^p - a$ dan $x^p + a$ adalah tereduksi atas $\mathbb{Z}_p$.

Latihan 8.4.13 Diberikan $f(x) = x^{n-1} + x^{n-2} + \cdots + x + 1 \in \mathbb{Q}[x]$, dimana n bukan bilangan bulat prima. Tunjukkan bahwa $f(x)$ adalah tereduksi atas $\mathbb{Q}$.

Latihan 8.4.14 Diberikan suatu lapangan $\mathbb{F}$, misalkan $f(x)$ dan $g(x)$ di $\mathbb{F}[x]$ adalah polinomial monik. Tunju,kkan bahwa bila $g(x)$ adalah tak-tereduksi atas $\mathbb{F}$ dan $f(x) \mid g(x)$, maka $f(x) = 1$ atau $f(x) = g(x)$.

Latihan 8.4.15 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $\mathbb{F}(x)$ adalah lapangan dari fungsi-fungsi rasioanal atas $\mathbb{F}$ (lihat Definisi 8.1.6). Maka $f(x)/g(x) \in F(x)$ dikatakan mempunyai **bentuk tereduksi** if $g(x)$ adalah monik dan $\text{fpb}(f(x), g(x)) = 1$. Tunjukkan bahwa setiap elemen $f(x)/g(x) \in F(x)$ dapat dijadikan ke bentuk tereduksi dalam suatu cara yang tunggal.

8.5 Polinomial Kubik dan Kuartik

Kita semua belajar di aljabar sekolah menengah rumus kuadrat yang memungkinkan kita menemukan akar dari polinomial kuadrat (derajat 2) dengan koefisien di $\mathbb{R}$ bentuk akar kuadrat. (Tentu saja, akar mungkin berada di $\mathbb{C}$ dan bukan di $\mathbb{R}$.) Algoritma juga ada untuk menemukan akar dalam polinomial kubik (derajat 3) dan kuartik (derajat 4) dengan koefisien di $\mathbb{R}$, dalam bentuk akar kuadrat dan akar pangkat tiga , meskipun mereka jarang disebutkan di sekolah menengah. Karena menemukan akar dari suatu polinomial $f(x)$ atau, hal yang sama menemukan solusi untuk persamaan polinomial $f(x) = 0$ adalah bagian yang lama dan mendasar dari aljabar, pembaca harus diberikan penjelasan tentang algoritma ini, dan kita berikan ia di bab ini.

Dalam sekolah tingkat menengah telah dikenal menyelesaikan persamaan kuadrat

$$ax^2 + bx + c = 0,\ a, b, c \in \mathbb{R},\ \text{dan}\ a \neq 0. \tag{8.5}$$

Penyelesaiannya diberikan oleh

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{8.6}$$

Dari Persamaan 8.6 terlihat bahwa penyelesaian dari Persamaan 8.5 bisa mempunyai nilai di $\mathbb{C}$. Formula sebagaimana dalam persamaan kuadrat juga bisa dilakukan untuk polinomial derajad tiga (kubik) dan polinomial berderajad empat (kuartik) sebagaimana merupakan topik bahasan dalam bagian ini. Untuk polinomial berderajad lebih besar dari empat suatu hal yang tidak mungkin menemukan formula sebagaimana diberikan oleh polinomial

berderajad dua, tiga dan empat. Hal ini bisa ditunjukkan dengan menggunakan teori **Galois**. Sebelum membahas penyelesaian dari polinomial kubik dan kuartik dibahas dulu ide dari penyesaian persamaan kuadrat yang mana hal ini dapat digunakan untuk pembahasan penyelesaian polinomial kubik dan kuartik. Hal ini dilakukan sebagai berikut. Dalam Persamaan 8.5 kedua ruas bagi dengan a sehingga didapat

$$x^2 + \frac{b}{a}x + \frac{c}{a} = 0. \tag{8.7}$$

Selanjutnya substitusikan $x = y + d$ dalam (8.7) didapat

$$(y+d)^2 + \frac{b}{a}(y+d) + \frac{c}{a} = 0 \tag{8.8}$$

atau

$$y^2 + 2dy + d^2 + \frac{b}{a}y + \frac{bd}{a} + \frac{c}{a} = 0.$$

Dengan mengumpulkan koefisien y didapat

$$y^2 + \left(2d + \frac{b}{a}\right)y + \left(d^2 + \frac{bd}{a} + \frac{c}{a}\right) = 0. \tag{8.9}$$

Bila koefisien y dalam (8.9) adalah nol yaitu $2d + \frac{b}{a} = 0$ atau $d = -\frac{b}{2a}$, maka didapat

$$y^2 + \left(-\frac{b^2}{4a^2} + \frac{c}{a}\right) = 0$$

atau

$$y^2 = \frac{b^2 - 4ac}{4a^2} \tag{8.10}$$

Persamaan 8.10 mudah diselesaikan, yaitu

$$y = \pm\frac{\sqrt{b^2 - 4ac}}{2a}.$$

Dengan demikian penyelesaian dari Persamaan 8.5 adalah

$$x = d + y = -\frac{b}{2a} \pm \frac{\sqrt{b^2 - 4ac}}{2a}.$$

Nilai $b^2 - 4ac$ dinamakan ***diskriminan*** dari persamaan kudrat dan dinotasikan sebagai $D = b^2 - 4ac$. Jadi bila $D < 0$, maka nilai akar dari persamaan kuadrat adalah kompleks.

8.5.1 Formula polinomial kubik

Kita mulai dengan contoh yang sudah familiar, berkaitan dengan pangkat tiga atau akar-akar tingkat tiga.

Contoh 8.5.1 Misalkan $f(x) = x^3 - 1 \in \mathbb{R}[x]$. Karena $f(1) = 0$,, maka faktor-faktor $f(x)$ atas $\mathbb{R}$ adalah:

$$f(x) = (x-1)(x^2 + x + 1)$$

dan, dengan menggunakan rumus persamaan kuadrat, kita dapat menemukan akar-akar dari faktor kedua:

$$\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i \text{ dan } \omega^2 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i.$$

Jadi $1, \omega$, dan ω^2 adalah akar-akar tingkat-3 dari satuan. Perhatikan bahwa sesuai dengan Teorema 8.3.5, ω^2 adalah konjugat kompleks dari ω.

Contoh 8.5.2 Misal $f(x) = x^3 - a \in \mathbb{R}[x]$, di mana $a > 0$. Maka $\sqrt[3]{a}$ adalah salah satu akar dari $f(x)$. Untuk mendapatkan dua akar lainnya, perhatikan bahwa jika ω adalah suatu akar tingkat-3 dari satuan seperti pada contoh sebelumnya, maka $(\sqrt[3]{a}\omega)^3 = a \cdot \omega^3 = a \cdot 1 = a$. Oleh karena itu $\sqrt[3]{a}$, $\sqrt[3]{a}\omega$ dan $\sqrt[3]{a}\omega^2$ adalah tiga akar dari $f(x) = x^3 - a$. Sekali lagi $\sqrt[3]{a}\omega^2$ adalah konjugat kompleks dari $\sqrt[3]{a}\omega$.

Contoh 8.5.3 Misalkan $f(x) = x^3 + 1 \in \mathbb{R}[x]$. Karena $f(-1) = 0$,, maka faktor-faktor $f(x)$ atas $\mathbb{R}$ adalah:

$$f(x) = (x+1)(x^2 - x + 1)$$

dan, dengan menggunakan rumus persamaan kuadrat, kita dapat menemukan akar-akar dari faktor kedua:

$$-\omega = \frac{1}{2} - \frac{\sqrt{3}}{2}i \text{ dan } -\omega^2 = \frac{1}{2} + \frac{\sqrt{3}}{2}i.$$

Jadi, $1, -\omega, -\omega^2$ adalah tiga akar dari $f(x)$.

Contoh 8.5.4 Misal $f(x) = x^3 + a \in \mathbb{R}[x]$, di mana $a > 0$. Maka dari dua contoh sebelumnya, kita memperoleh hasil bahwa $-\sqrt[3]{a}$, $-\sqrt[3]{a}\omega$ dan $-\sqrt[3]{a}\omega^2$ adalah tiga akar dari polinomial $f(x) = x^3 + a \in \mathbb{R}[x]$, $a > 0$.

Contoh-contoh ini menunjukkan pentingnya akar-akar tingkat-3 dari satuan: $1, \omega$, dan ω^2. Khususnya, Contoh 8.5.2 dan 8.5.4 menunjukkan bahwa begitu kita mengetahui satu akar real dari $f(x)$, kita dapat segera menuliskan dua akar-akar kompleks lainnya. Contoh berikutnya adalah yang lebih sulit, dan menggambarkan metode yang digunakan dalam kasus umum, tetapi sekali lagi dalam contoh ini akar-akar tingkat-3 dari satuan memainkan peran penting.

Contoh 8.5.5 Misal $f(x) = x^3 + 3x + 1 \in \mathbb{R}[x]$. Penyelesaian dalam kasus ini menggunakan **suatu trik** dan yang membutuhkan **waktu ribuan tahun** bagi siapa pun untuk memikirkannya! Idenya adalah untuk menunjukkan bahwa kita bisa menemukan penyelesaian untuk persamaan yang kita minati jika kita bisa menemukan penyelesaian untuk beberapa persamaan lain, dan akhirnya mereduksi masalah yang ingin kita selesaikan menjadi masalah yang kita tahu bisa kita selesaikan. Pertama, kita ganti $u + v$ pada x. Untuk menyelesaikan persamaan $f(x) = 0$, cukup selesaikan persamaannya

$$\begin{aligned}
(u+v)^3 + 3(u+v) + 1 &= 0, \text{ atau} \\
u^3 + 3u^2v + 3uv^2 + v^3 + 3u + 3v + 1 &= 0, \text{ atau} \\
u^3 + v^3 + 1 &= -3(u^2v + uv^2 + u + v), \text{ atau} \\
u^3 + v^3 + 1 &= -3[(uv)(u+v) + (u+v)], \text{ atau} \\
u^3 + v^3 + 1 &= -3(uv+1)(u+v).
\end{aligned}$$

Salah satu cara persamaan ini dapat dipenuhi adalah jika kedua sisinya nol, yang akan terjadi jika kita memiliki

$$\begin{aligned} u^3 + v^3 + 1 &= 0 \qquad (8.11)\\ (uv + 1) &= 0. \qquad (8.12)\end{aligned}$$

Untuk memenuhi (8.12), kita dapat memisalkan $v = -\frac{1}{u} = -u^{-1}$. Maka (8.11) menjadi

$$\begin{aligned} u^3 + v^3 + 1 &= u^3 - u^{-3} + 1 = 0, \text{ atau}\\ u^3 - u^{-3} + 1 &= 0, \text{ atau}\\ u^3 + 1 - u^{-3} &= 0, \text{ atau}\\ u^6 + u^3 - 1 &= 0, \text{ atau}\\ (u^3)^2 + u^3 - 1 &= 0.\end{aligned}$$

Ini adalah persamaan kuadrat dalam u^3 jadi kita menyelesaikannya menggunakan rumus kuadrat, yang memberikan

$$u^3 = \frac{-1 \pm \sqrt{5}}{2} \in \mathbb{R}.$$

Karena $u^3 + v^3 = -1$ kita dapat mengambil

$$u^3 = \frac{-1 + \sqrt{5}}{2} \text{ dan } v^3 = \frac{-1 - \sqrt{5}}{2}. \qquad (8.13)$$

(Tidak masalah yang mana yang kita sebut u dan yang mana kita sebut v, karena peran u dan v benar-benar simetris.) Maka, ambil akar pangkat tiga di (8.13), akar-akar real yang kita cari dapat ditulis sebagai

$$x = u + v = \sqrt[3]{\frac{-1 + \sqrt{5}}{2}} + \sqrt[3]{\frac{-1 - \sqrt{5}}{2}} \in \mathbb{R}.$$

Sekarang, untuk mendapatkan dua akar-akar lainnya, kita menggunakan akar-akar tingkat-3 dari satuan ω dan ω^2. Ingat bahwa $1 + \omega + \omega^2 = 0$, $\omega^2 = \overline{\omega}$ dan $\omega^3 = (\omega^2)^3 = 1$. Misalkan u dan v adalah seperti sebelumnya, pertimbangkan sekarang $u\omega + v\omega^2$ dan konjugat kompleksnya $u\omega^2 + v\omega$. Kita mengklaim bahwa ini adalah dua akar-akar bilangan kompleks dari $f(x) = x^3 + 3x + 1$. Karena mereka adalah konjugat kompleks, cukup untuk memeriksa salah satunya:

$$\begin{aligned} (u\omega + v\omega^2)^3 + 3(u\omega + v\omega^2) + 1 &= u^3\omega^3 + 3u^2\omega^2 v\omega^2 + 3u\omega v^2\omega^4 + v^3\omega^6 + 3u\omega + 3v\omega^2 + 1\\ &= u^3 + 3u^2 v\omega + 3uv^2\omega^2 + v^3 + 3u\omega + 3v\omega^2 + 1\\ &= (u^3 + v^3 + 1) + 3(u^2 v\omega + uv^2\omega^2 + u\omega + v\omega^2)\\ &= (u^3 + v^3 + 1) + 3\left[uv(u\omega + v\omega^2) + (u\omega + v\omega^2)\right]\\ &= (u^3 + v^3 + 1) + 3(uv + 1)(u\omega + v\omega^2)\\ &= 0 + 3 \cdot 0 \cdot (u\omega + v\omega^2) \quad \text{(berdasarkan 8.11 dan 8.12)}\\ &= 0 + 0 = 0.\end{aligned}$$

Jadi

$$\begin{aligned} u+v &= \sqrt[3]{\frac{-1+\sqrt{5}}{2}} + \sqrt[3]{\frac{-1-\sqrt{5}}{2}}, \\ u\omega + v\omega^2 &= \sqrt[3]{\frac{-1+\sqrt{5}}{2}} \cdot \frac{-1+\sqrt{3}i}{2} + \sqrt[3]{\frac{-1-\sqrt{5}}{2}} \cdot \frac{-1-\sqrt{3}i}{2} \quad \text{dan} \\ u\omega^2 + v\omega &= \sqrt[3]{\frac{-1+\sqrt{5}}{2}} \cdot \frac{-1-\sqrt{3}i}{2} + \sqrt[3]{\frac{-1-\sqrt{5}}{2}} \cdot \frac{-1+\sqrt{3}i}{2} \end{aligned}$$

adalah tiga akar-akar dari $f(x)$. ●

Perhatikan bahwa dalam contoh sebelumnya, u^3 dan v^3 ternyata bilangan real. Ini tidak akan selalu terjadi.

Mengikuti langkah-langkah yang sama persis seperti pada Contoh 8.5.5, kita memperoleh penyelesaian yang lebih umum berikut:
Misalkan $f(x) = x^3 + px + q \in \mathbb{R}[x]$ dan misalkan u dan v diberikan oleh

$$u^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \quad \text{dan} \quad uv = -\frac{p}{3}.$$

Maka mengikuti apa yang telah dibahas dalam contoh sebelumnya, akar-akar dari $f(x)$ adalah $u+v, u\omega + v\omega^2$ dan $u\omega^2 + v\omega$.

Dengan demikian, untuk pembahasan formalnya kita mengikuti ide dalam pembahasan persamaan kuadrat untuk mendapatkan formula penyelesaian dari persamaan kubik sebagaimana berikut. Diberikan persamaan kubik

$$ax^3 + bx^2 + cx + d = 0, \;\; a,b,c,d \in \mathbb{R} \;\text{ dan }\; a \neq 0. \tag{8.14}$$

Karena $a \neq 0$, maka didapat

$$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0. \tag{8.15}$$

Selanjutnya lakukan substitusi $x = y + e$ kedalam Persamaan 8.15 dimana e dipilih supaya persamaan mudah diselesaikan, didapat

$$(y+e)^3 + \frac{b}{a}(y+e)^2 + \frac{c}{a}(y+e) + \frac{d}{a} = 0 \tag{8.16}$$

Ekspansikan pangkat dalam Persamaan 8.16 dan kelompokkan koefisien dari y sesuai dengan pangkat-pangkatnya, didapat

$$y^3 + \left(3e + \frac{b}{a}\right)y^2 + \left(3e^2 + \frac{2be}{a} + \frac{c}{a}\right)y + \left(e^3 + \frac{be^2}{a} + \frac{ce}{a} + \frac{d}{a}\right) = 0. \tag{8.17}$$

Mengikuti pembahasan dalam persamaan kuadrat, bila koefisen y^2 dalam Persamaan 8.17 adalah nol yaitu $3e + \frac{b}{a} = 0$ atau $e = -\frac{b}{3a}$, maka didapat

$$y^3 + \left(-\frac{b^2}{3a^2} + \frac{c}{a}\right)y + \left(\frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}\right) = 0 \tag{8.18}$$

Untuk penulisan yang sederhana dalam Persamaan 8.18, dimisalkan

$$p = -\frac{b^2}{3a^2} + \frac{c}{a} \quad \text{dan} \quad q = \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a},$$

sehingga didapat

$$y^3 + py + q = 0. \tag{8.19}$$

Substitusikan $y = z - \dfrac{p}{3z}$ kedalam Persamaan 8.19, didapat

$$\left(z - \frac{p}{3z}\right)^3 + p\left(z - \frac{p}{3z}\right) + q = 0$$

atau

$$z^3 - \frac{p^3}{27z^3} + q = 0. \tag{8.20}$$

Persamaan 8.20 adalah persamaan kuadrat dalam z^3 yaitu

$$(z^3)^2 + q(z^3) - \frac{p^3}{27} = 0. \tag{8.21}$$

Dengan menggunakan formula persamaan kuadrat, maka penyelesaian Persamaan 8.21 diberikan oleh

$$z^3 = \frac{-q \pm \sqrt{q^2 + \frac{4p^3}{27}}}{2} = -\frac{q}{2} \pm \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}. \tag{8.22}$$

Dalam Persamaan 8.22 bila

$$A = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \quad \text{dan} \quad B = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},$$

maka

$$z^3 = A \quad \text{atau} \quad z^3 = B.$$

Perhatikan bahwa

$$\begin{aligned} AB &= \left(-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}\right)\left(-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}\right) \\ &= \left(\frac{q}{2}\right)^2 - \left(\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\right) = -\frac{p^3}{27}, \end{aligned}$$

sehingga didapat

$$\sqrt[3]{A}\sqrt[3]{B} = -\frac{p}{3}.$$

Sebelum menyelesaikan Persamaan 8.21 dibahas dulu persamaan

$$z^3 - 1 = 0 \quad \text{atau} \quad z^3 = 1,$$

yang mempunyai penyelesaian diberikan oleh

$$z = \cos\ 0 + i \sin\ 0 = 1$$

$$z = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = \frac{-1 + \sqrt{3}i}{2}$$

$$z = \cos \frac{4\pi}{3} + i \sin \frac{4\pi}{3} = \frac{-1 - \sqrt{3}i}{2}.$$

Bila $\omega = \frac{-1+i\sqrt{3}}{2}$, maka akar-akar dari $z^3 = 1$ adalah

$$\sqrt[3]{1}, \quad \omega \sqrt[3]{1} \quad \text{dan} \quad \omega^2 \sqrt[3]{1}.$$

Dengan demikian penyelesaian dari $z^3 = A$ diberikan oleh

$$\sqrt[3]{A}, \quad \omega \sqrt[3]{A} \quad \text{dan} \quad \omega^2 \sqrt[3]{A}$$

dan penyelesaian dari $z^3 = B$ diberikan oleh

$$\sqrt[3]{B}, \quad \omega \sqrt[3]{B} \quad \text{dan} \quad \omega^2 \sqrt[3]{B}.$$

Jadi penyelesaian dari Persamaan 8.21 adalah

$$\sqrt[3]{A}, \quad \omega \sqrt[3]{A} \quad \omega^2 \sqrt[3]{A} \quad \text{dan} \quad \sqrt[3]{B}, \quad \omega \sqrt[3]{B} \quad \omega^2 \sqrt[3]{B}.$$

Untuk menyelesaikan Persamaan 8.19, substitusikan

$$y = z - \frac{p}{3z} = z + \frac{\sqrt[3]{A}\sqrt[3]{B}}{z}$$

dan fakta bahwa $\frac{1}{\omega} = \omega^2$ atau $\frac{1}{\omega^2} = \omega$, maka penyelesaian untuk y dari Persamaan 8.19 adalah

$$\sqrt[3]{A} + \sqrt[3]{B}, \quad \omega \sqrt[3]{A} + \omega^2 \sqrt[3]{B} \quad \text{dan} \quad \omega^2 \sqrt[3]{A} + \omega \sqrt[3]{B}$$

Sebelum melanjutkan pembahasan penyelesaian Persamaan 8.14 terlebih dulu diberikan contoh dari penyelesaian Persamaan 8.19.

Contoh 8.5.6 Diberikan persamaan

$$y^3 - 9y - 12 = 0.$$

Maka $p = -9$ dan $q = -12$, sehingga didapat

$$A = \frac{12}{2} + \sqrt{(-6)^2 + (-3)^3} = 6 + \sqrt{9} = 9, \qquad B = 6 - \sqrt{9} = 3.$$

Dengan demikian akar dari persamaan adalah:

$$\begin{aligned}
\sqrt[3]{A} + \sqrt[3]{B} &= \sqrt[3]{9} + \sqrt[3]{3}, \\
\omega\sqrt[3]{A} + \omega^2\sqrt[3]{B} &= \left(\frac{-1+\sqrt{3}i}{2}\right)\sqrt[3]{9} + \left(\frac{-1-\sqrt{3}i}{2}\right)\sqrt[3]{3} \\
&= -\frac{1}{2}(\sqrt[3]{9} + \sqrt[3]{3}) + \frac{\sqrt{3}i}{2}(\sqrt[3]{9} - \sqrt[3]{3}), \\
\omega^2\sqrt[3]{9} + \omega\sqrt[3]{3} &= \left(\frac{-1-\sqrt{3}i}{2}\right)\sqrt[3]{9} + \left(\frac{-1+\sqrt{3}i}{2}\right)\sqrt[3]{3} \\
&= -\frac{1}{2}(\sqrt[3]{9} + \sqrt[3]{3}) - \frac{\sqrt{3}i}{2}(\sqrt[3]{9} - \sqrt[3]{3}).
\end{aligned}$$

Selanjutnya, kembali pada persoalan untuk menyelesaikan Persamaan 8.14, yaitu formula untuk mendapatkan akar-akar persamaan umum kubik. Lakukan substitusi $x = y + e$, dimana nilai y adalah

$$\sqrt[3]{A},\ \omega\sqrt[3]{A}\ \omega^2\sqrt[3]{A} \quad \text{dan} \quad \sqrt[3]{B},\ \omega\sqrt[3]{B}\ \omega^2\sqrt[3]{B}; \qquad \text{dan nilai } e = -\frac{b}{3a}. \tag{8.23}$$

Karena $\frac{1}{\omega} = \omega^2$ atau $\frac{1}{\omega^2} = \omega$, maka penyelesaian untuk x dari Persamaan 8.14 adalah

$$x_1 = \sqrt[3]{A} + \sqrt[3]{B} - \frac{b}{3a},\ x_2 = \omega\sqrt[3]{A} + \omega^2\sqrt[3]{B} - \frac{b}{3a} \text{ dan } x_3 = \omega^2\sqrt[3]{A} + \omega\sqrt[3]{B} - \frac{b}{3a}, \tag{8.24}$$

dimana

$$\begin{aligned}
\omega &= \frac{-1+\sqrt{3}i}{2}, \qquad \omega^2 = \frac{-1-\sqrt{3}i}{2} \\
A &= -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}, \quad B = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3},
\end{aligned}$$

dengan

$$p = -\frac{b^2}{3a^2} + \frac{c}{a} \qquad \text{dan} \qquad q = \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a}.$$

Formula dalam (8.24) dikenal sebagai Formula **Cardano**.

Contoh 8.5.7 Diberikan polinomial kubik

$$x^3 - 3x^2 - 6x - 4 = 0,$$

maka $a = 1, b = -3, c = -6$ dan $d = -4$. Sehingga didapat

$$p = -\frac{b^2}{3a^2} + \frac{c}{a} = -\frac{9}{3} + \frac{-6}{1} = -9$$

dan

$$q = \frac{2b^3}{27a^3} - \frac{bc}{3a^2} + \frac{d}{a} = \frac{2(-27)}{27} - \frac{18}{3} + \frac{-4}{1} = -12.$$

Dengan demikian nilai A dan B adalah

$$A = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = 6 + \sqrt{(-6)^2 + (-3)^3} = 9$$

dan

$$B = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = 6 - \sqrt{(-6)^2 + (-3)^3} = 3.$$

Dengan menggunakan formula (8.24), maka akar-akar dari persamaan adalah

$$\begin{aligned}
x_1 &= \sqrt[3]{A} + \sqrt[3]{B} - \frac{b}{3a} = \sqrt[3]{9} + \sqrt[3]{3} + 1 \\
x_2 &= \omega\sqrt[3]{A} + \omega^2\sqrt[3]{B} - \frac{b}{3a} = -\frac{1}{2}(\sqrt[3]{9} + \sqrt[3]{3} - 2) + \frac{\sqrt{3}i}{2}(\sqrt[3]{9} - \sqrt[3]{3}) \\
x_3 &= \omega^2\sqrt[3]{A} + \omega\sqrt[3]{B} - \frac{b}{3a} = -\frac{1}{2}(\sqrt[3]{9} + \sqrt[3]{3} - 2) - \frac{\sqrt{3}i}{2}(\sqrt[3]{9} - \sqrt[3]{3}).
\end{aligned}$$

Definisi berikut mengenai diskriminan dari polinomial kubik yang dapat digunakan untuk mementukan kriteria bahwa semua akar-akar dari polinomial kubik adalah real.

Definisi 8.5.1 Misalkan $f(y) = y^3 + py + q$ mempunyai akar-akar c_1, c_2 dan c_3, maka

$$D = [(c_1 - c_2)(c_1 - c_3)(c_2 - c_3)]^2$$

dinamakan **diskriminan** dari polinomial $f(y)$.

Teorema 8.5.1 Diskriminan dari polinomial $f(y) = y^3 + py + q$ adalah $D = -4p^3 - 27q^2$.

Bukti Misalkan c_1, c_2 dan c_3 adalah akar-akar dari polinomial $f(y) = y^3 + py + q$. Maka didapat

$$f(y) = (y - c_1)(y - c_2)(y - c_3),$$

dimana

$$c_1 = \sqrt[3]{A} + \sqrt[3]{B}, \quad c_2 = \omega\sqrt[3]{A} + \omega^2\sqrt[3]{B}, \quad c_3 = \omega^2\sqrt[3]{A} + \omega\sqrt[3]{B}$$

dan

$$A = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}, \quad B = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}, \quad \omega = \frac{-1 + \sqrt{3}i}{2}.$$

Dengan menggunakan fakta bahwa $\omega^3 = 1$, didapat

$$\begin{aligned}
c_1 - c_2 &= (\sqrt[3]{A} + \sqrt[3]{B}) - (\omega\sqrt[3]{A} + \omega^2\sqrt[3]{B}) \\
&= \sqrt[3]{A} + \sqrt[3]{B} - \omega\sqrt[3]{A} - \omega^2\sqrt[3]{B} \\
&= (1 - \omega)(\sqrt[3]{A} - \omega^2\sqrt[3]{B}),
\end{aligned}$$

$$\begin{aligned}
c_1 - c_3 &= (\sqrt[3]{A} + \sqrt[3]{B}) - (\omega^2\sqrt[3]{A} + \omega\sqrt[3]{B}) \\
&= \sqrt[3]{A} + \sqrt[3]{B} - \omega^2\sqrt[3]{A} - \omega\sqrt[3]{B} \\
&= -\omega^2(1 - \omega)(\sqrt[3]{A} - \omega\sqrt[3]{B}),
\end{aligned}$$

$$\begin{aligned} c_2 - c_3 &= (\omega \sqrt[3]{A} + \omega^2 \sqrt[3]{B}) - (\omega^2 \sqrt[3]{A} + \omega \sqrt[3]{B}) \\ &= \omega \sqrt[3]{A} + \omega^2 \sqrt[3]{B} - \omega^2 \sqrt[3]{A} - \omega \sqrt[3]{B} \\ &= \omega(1-\omega)(\sqrt[3]{A} - \sqrt[3]{B}). \end{aligned}$$

Bila $C = (c_1 - c_2)(c_1 - c_2)(c_2 - c_3)$, maka

$$\begin{aligned} C &= -\omega^3(1-\omega)^3(\sqrt[3]{A} - \omega^2 \sqrt[3]{B})(\sqrt[3]{A} - \omega \sqrt[3]{B})(\sqrt[3]{A} - \sqrt[3]{B}) \\ &= 3i\sqrt{3}(\sqrt[3]{A} - \omega^2 \sqrt[3]{B})(\sqrt[3]{A} - \omega \sqrt[3]{B})(\sqrt[3]{A} - \sqrt[3]{B}) \\ &= 3i\sqrt{3}\Big(\sqrt[3]{A^3} - \omega^3 \sqrt[3]{B^3} + \omega^3 \sqrt[3]{A}\sqrt[3]{B^2} - \sqrt[3]{A^2}\sqrt[3]{B} \\ &\quad -\omega \sqrt[3]{A^2}\sqrt[3]{B} + \omega \sqrt[3]{A}\sqrt[3]{B^2} - \omega^2 \sqrt[3]{A^2}\sqrt[3]{B} + \omega^2 \sqrt[3]{A}\sqrt[3]{B^2}\Big) \\ &= 3i\sqrt{3}\Big(A - B + \sqrt[3]{A}\sqrt[3]{B^2} - \sqrt[3]{A^2}\sqrt[3]{B} \\ &\quad -\omega\Big(\sqrt[3]{A^2}\sqrt[3]{B} - \sqrt[3]{A}\sqrt[3]{B^2}\Big) - \omega^2\Big(\sqrt[3]{A^2}\sqrt[3]{B} - \sqrt[3]{A}\sqrt[3]{B^2}\Big)\Big) \\ &= 3i\sqrt{3}\Big(A - B + (-1-\omega-\omega^2)\Big(\sqrt[3]{A^2}\sqrt[3]{B} - \sqrt[3]{A}\sqrt[3]{B^2}\Big)\Big) \\ &= 3i\sqrt{3}(A-B) \qquad \text{(sebab: } -1-\omega-\omega^2 = 0) \\ &= 3\sqrt{3}i\sqrt{q^2 + \frac{4}{27}p^3}, \end{aligned}$$

hasil yang terakhir didapat dari

$$\begin{aligned} A - B &= -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} - \left(-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}\right) \\ &= 2\sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} \\ &= \sqrt{q^2 + \frac{4}{27}p^3}. \end{aligned}$$

Jadi diskriminan D adalah

$$D = C^2 = \left(3i\sqrt{3}\sqrt{q^2 + \frac{4}{27}p^3}\right)^2 = -4p^3 - 27q^2.$$

Teorema berikut memberikan kriteria akar-akar real dari polinomial $f(y) = y^3 + py + q$.

Teorema 8.5.2 Persamaan $y^3 + py + q = 0$ mempunyai tepat tiga akar real bila dan hanya bila $D \geq 0$, yaitu bila dan hanya bila $-4p^3 - 27q^2 \geq 0$.

Bukti ($\Rightarrow$) Misalkan c_1, c_2 dan c_3 adalah akar-akar real dari $y^3 + py + q = 0$. Maka

$$C = (c_1 - c_2)(c_1 - c_3)(c_2 - c_3)$$

adalah real. Dengan demikian diskriminan $D = C^2 \geq 0$.

($\Leftarrow$) Bukti sebaliknya digunakan kontraposisi. Asumsikan aka-akar dari $f(y) = y^3 + py + q$ tepat mempunyai satu akar real c_1 dan dua akar bukan real c_2 dan c_3. Sebagaimana telah

diketahui nilai bukan real tersebut haruslah saling berkonjuget satu dengan yang lainnya, maka misalkan $c_2 = z = a + bi$ dan $c_3 = \overline{z} = a - bi$. Sehingga didapat

$$\begin{aligned} C &= (c_1 - z)(c_1 - \overline{z})(z - \overline{z}) \\ &= (c_1 - (a + bi))(c_1 - (a - bi))(a + bi - (a - bi)) \\ &= 2bi\left((a - c_1)^2 + b^2\right). \end{aligned}$$

karena $b \neq 0$, maka didapat

$$D = C^2 = \left(2bi\left((a - c_1)^2 + b^2\right)\right)^2 = -4b^2\left((a - c_1)^2 + b^2\right)^2 < 0.$$

Contoh 8.5.8 Selidiki apakah polinomial

$$f(x) = x^3 - 6x^2 + 11x - 6 \tag{8.25}$$

semua akar-akarnya real? Selanjutnya dengan menggunakan formula Cardano tentukan semua akar-akarnya.

Jawab Koefisien dari $f(x)$ adalah $a = 1, b = -6, c = 11$ dan $d = -6$. Substitusikan $x = y + e$ dalam (8.25) dengan $e = -\frac{b}{3a} = -\frac{-6}{3} = 2$ didapat

$$g(y) = y^3 - y. \tag{8.26}$$

Terlihat bahwa koefisien dari $g(y)$ adalah $p = -1$ dan $q = 0$. Diskriminan dari $g(y)$ adalah

$$D = -4p^3 - 27q^2 = -4(-1) - 27(0) = 4 > 0.$$

Jadi semua akar dari $g(y) = y^3 - y$ adalah real, yaitu $y = c_1 = 0, y = c_2 = 1$ dan $y = c_3 = -1$. Dengan demikian semua akar dari Persamaan 8.25 adalah $x = y + e = y + 2$ dimana $y = 0, 1, -1 \in \mathbb{R}$. Sehingga didapat

$$x_1 = 0 + 2 = 2, \quad x_2 = 1 + 2 = 3, \quad \text{dan} \quad x_3 = -1 + 2 = 1.$$

Untuk menentukan akar-akar x_1, x_2 dan x_3 dengan menggunakan formula Cardano dibutuhkan nilai-nilai A dan B sebagai berikut

$$A = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = -\frac{0}{2} + \sqrt{0^2 + \left(\frac{-1}{3}\right)^3} = \sqrt{\frac{-1}{3^3}} = \sqrt{\frac{1}{27}}i,$$

dan

$$B = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = -\frac{0}{2} - \sqrt{0^2 + \left(\frac{-1}{3}\right)^3} = -\sqrt{\frac{-1}{3^3}} = -\sqrt{\frac{1}{27}}i,$$

Nilai akar-akar x_1, x_2 dan x_3 dengan menggunakan formula Cardano adalah

$$x_1 = \sqrt[3]{A} + \sqrt[3]{B} - \frac{b}{3a} = \sqrt[3]{\sqrt{\frac{1}{27}}i} + \sqrt[3]{-i\sqrt{\frac{1}{27}}} - \frac{-6}{3} = \sqrt[3]{\sqrt{\frac{1}{27}}i} - \sqrt[3]{\sqrt{\frac{1}{27}}i} + 2 = 2,$$

$$\begin{aligned} x_2 &= \omega\sqrt[3]{A} + \omega^2\sqrt[3]{B} - \frac{b}{3a} \\ &= \left(\frac{-1+\sqrt{3}i}{2}\right)\sqrt[3]{\sqrt{\frac{1}{27}}i} - \left(\frac{-1-\sqrt{3}i}{2}\right)\sqrt[3]{\sqrt{\frac{1}{27}}i} + 2 \\ &= \sqrt[3]{\sqrt{\frac{1}{27}}i}\left(\frac{-1+\sqrt{3}i}{2} + \frac{1+\sqrt{3}i}{2}\right) + 2 = \sqrt[3]{\sqrt{\frac{1}{27}}i}\,(\sqrt{3}i) + 2 \\ &= \sqrt[3]{\sqrt{\frac{1}{27}}i}\,\sqrt[3]{\sqrt{27}i^3} + 2 = \sqrt[3]{\sqrt{\frac{27}{27}}i^4} + 2 = \sqrt[3]{1} + 2 = 1 + 2 = 3 \end{aligned}$$

dan

$$\begin{aligned} x_3 &= \omega^2\sqrt[3]{A} + \omega\sqrt[3]{B} - \frac{b}{3a} \\ &= \left(\frac{-1-\sqrt{3}i}{2}\right)\sqrt[3]{\sqrt{\frac{1}{27}}i} - \left(\frac{-1+\sqrt{3}i}{2}\right)\sqrt[3]{\sqrt{\frac{1}{27}}i} + 2 \\ &= \sqrt[3]{\sqrt{\frac{1}{27}}i}\left(\frac{-1-\sqrt{3}i}{2} + \frac{1-\sqrt{3}i}{2}\right) + 2 = \sqrt[3]{\sqrt{\frac{1}{27}}i}\,(-\sqrt{3}i) + 2 \\ &= -\sqrt[3]{\sqrt{\frac{1}{27}}i}\,\sqrt[3]{\sqrt{27}i^3} + 2 = -\sqrt[3]{\sqrt{\frac{27}{27}}i^4} + 2 = -\sqrt[3]{1} + 2 = -1 + 2 = 1. \end{aligned}$$

Terlihat bahwa hasil nilai-nilai $x_1 = 2, x_2 = 3$ dan $x_3 = 1$ yang didapat sama dengan hasil sebelumnya. ●

8.5.2 Formula polinomial Kuartik

Kita mengakhiri bagian ini dengan beberapa diskusi tentang menemukan akar-akar dari polinomial kuartik $f(x) \in \mathbb{R}[x]$. Misalkan kita ingin menyelesaikan persamaan

$$f(x) == x^4 + ax^3 + bx^2 + cx + d = 0 \tag{8.27}$$

Jika kita dapat menemukan bilangan h, k, u dan v sehingga kita memiliki

$$f(x) = (x^2 + hx + k)^2 - (ux + v)^2 \tag{8.28}$$

maka persamaan awal (8.27) akan ekivelen dengan

$$\Big[(x^2 + hx + k) + (ux + v)\Big]\Big[(x^2 + hx + k) - (ux + v)\Big] = 0 \tag{8.29}$$

yang dapat diselesaikan dengan menerapkan rumus persamaan kuadrat dua kali.

Bagaimana kita bisa menemukan nilai-nilai penyelesaian tsb.? Ekspansikan sisi kanan (8.28) dan membandingkan koefisien dengan koefisien dalam (8.27), kita memperoleh yang berikut:

$$\begin{aligned} a = 2h \quad &\text{atau} \quad h = \frac{a}{2} \\ b = h^2 + 2k - u^2 \quad &\text{atau} \quad u^2 = h^2 + 2k - b = \left(\frac{a}{2}\right)^2 + 2k - b \\ c = 2hk - 2uv \quad &\text{atau} \quad 2uv = 2hk - c = ak - c \\ d = k^2 - v^2 \quad &\text{atau} \quad v^2 = k^2 - d. \end{aligned}$$

Persamaan ini cukup untuk menentukan h, u, v asalkan k dapat ditentukan. Untuk menentukan k perhatikan bahwa $4u^2v^2 - (2uv)^2 = 0$. Oleh karena itu, menggunakan ekspresi sebelumnya untuk $u^2, 2uv, v^2$ dalam hal k kita memiliki kondisi bahwa harus memenuhi

$$4\left[\left(\frac{a}{2}\right)^2 + 2k - b\right]\left[k^2 - d\right] - [ak - c]^2 = 0,$$

atau

$$8k^3 - 4bk^2 + (2ac - 8d)k + (4bd - a^2d - c^2) = 0. \tag{8.30}$$

Ini adalah persamaan kubik yang pada prinsipnya kita tahu bagaimana menyelesaikannya dalam bentuk akar-akar kuadrat dan pangkat tiga. Menyelesaikannya dan memperoleh k kita kemudian kembali untuk menentukan h, u, v dan kemudian menyelesaikan persamaan aslinya $f(x) = 0$.

Definisi 8.5.2 Persamaan kubik di (8.30) disebut **kubik pembantu** (***auxiliary cubic***) dari kuartik asli di (8.27).

Selanjutnya pembahasan dengan cara sedikit agak berbeda diberikan. Kita tuliskan lagi persamaan kuartik (8.27).

$$x^4 + ax^3 + bx^2 + cx + d = 0. \tag{8.31}$$

Lagi, digunakan substitusi yang memungkinkan untuk menghapus suku yang kedua, yaitu substitusikan $x = y - \frac{a}{4}$ kedalam Persamaan 8.31 sehingga didapat

$$y^4 + py^2 + qy + r = 0. \tag{8.32}$$

Selanjutnya diselesaikan Persamaan 8.31 sebagai berikut. Persamaan 8.31 dapat ditulis dalam bentuk

$$y^4 = -py^2 - q - r. \tag{8.33}$$

Ide dasar dari metode ini dirancang oleh Ferrari yang mana kedua ruas Persamaan 8.33 ditambahkan suatu bentuk kuadrat supaya bagian kiri persamaan menjadi bentuk kuadrat sempurnah. Tambahkan $ty^2 + \frac{t^2}{4}$ dalam Persamaan 8.33 dimana t belum ditentukan, sehingga didapat

$$y^4 + ty^2 + \frac{t^4}{4} = -py^2 - qy - r + ty^2 + \frac{t^2}{4},$$

atau

$$\left(y^2 + \frac{t}{2}\right)^2 = (t - p)y^2 - qy + \left(\frac{t^2}{4} - r\right). \tag{8.34}$$

Persamaan 8.34 dipenuhi bila dan hanya bila diskriminan dari bagian kanan persamaan sama dengan nol. Yaitu bila dan hanya bila

$$(-q)^2 - 4(t-p)\left(\frac{t^2}{4} - r\right) = 0. \tag{8.35}$$

Persamaan 8.35 dapat disederhanakan menjadi persamaan kubik dalam t sebagi berikut.

$$t^3 - pt^2 - 4rt + 4rp - q^2 = 0. \tag{8.36}$$

Persamaan 8.36 dinamakan **persamaan resolvent** dari $y^4+py+qy+r = 0$. Persamaan resolvent dapat diselesaikan dengan formula Cardano. Dengan demikian Persamaan 8.32 dapat diselesaikan. Sebelum melanjutkan pembahasan penyelesaian Persamaan 8.31, terlebih dahulu diberikan contoh menyelesaikan Persamaan 8.32.

Contoh 8.5.9 Diberikan persamaan

$$y^4 + y^2 - 2y + 6 = 0,$$

maka $p = 1, q = -2$ dan $r = 6$ dan persamaan resolvent diberikan oleh

$$t^3 - t^2 - 24t + 20 = 0,$$

yang mempunyai penyelesaian $t = 5$. Selanjutnya persamaan

$$\left(y^2 + \frac{t}{2}\right)^2 = (t-p)y^2 - qy + \left(\frac{t^2}{4} - r\right)$$

menjadi

$$\left(y^2 + \frac{5}{2}\right)^2 = 4y^2 + 2y + \frac{1}{4} = \left(2y + \frac{1}{2}\right)^2.$$

Sehingga didapat

$$y^2 + \frac{5}{2} = 2y + \frac{1}{2} \quad \text{atau} \quad y^2 + \frac{5}{2} = -2y - \frac{5}{2}.$$

atau

$$y^2 - 2y + 2 = 0 \quad \text{atau} \quad y^2 + 2y + 3 = 0.$$

Gunakan formula persamaan kuadrat didapat

$$y = 1 \pm i \quad \text{dan} \quad y = -1 \pm \sqrt{2}\,i. \qquad \bullet$$

Kembali pada pembahasan penyelesaian Persamaan 8.31. Setelah menyelesaikan Persamaan 8.32, yaitu didapat nilai y_1, y_1, y_3 dan y_4. Maka penyelesaian dari Persamaan 8.31 diberikan oleh

$$x_i = y_i - \frac{a}{4},\ i = 1, 2, 3, 4.$$

Contoh 8.5.10 Diberikan persamaan

$$x^4 + 4x^3 + 7x^2 + 4x + 6 = 0.$$

Kedalam persamaan substitusikan $x = y - \frac{a}{4}$ yaitu $x = y - 1$ didapat

$$(y-1)^4 + 4(y-1)^3 + 7(y-1)^2 + 4(y-1) + 6 = 0.$$

Persamaan hasil substitusi dapat disederhanakan menjadi

$$y^4 + y^2 - 2y + 6 = 0.$$

Berdasarkan Contoh 8.5.9, maka penyelesaiannya adalah

$$y_1 = 1 + i, y_2 = 1 - i, y_3 = -1 + \sqrt{2}\,i \quad \text{dan} \quad y_4 = -1 - \sqrt{2}\,i.$$

Jadi penyelesaian $x_i = y_i - 1,\ i = 1, 2, 3, 4$ diberikan oleh

$$x_1 = i, x_2 = -i, x_3 = -2 + \sqrt{2}\,i \quad \text{dan} \quad x_4 = -2 - \sqrt{2}\,i.$$

Latihan

Latihan 8.5.1 Nyatakan benar atau salah pernyataan berikut.

1. Setiap persamaan kubik atas $\mathbb{R}$ mempunyai setidaknya satu penyelesaian di $\mathbb{R}$.
2. Setiap persamaan kuartik atas $\mathbb{R}$ mempunyai setidaknya satu penyelesaian di $\mathbb{R}$.
3. Bila diskriminan dari polinomial kuadrat atau kubik atas $\mathbb{R}$ adalah positip, maka semua akar-akarnya harus real.
4. If diskriminan dari polinomial kuadrat atau kubik atas $\mathbb{R}$ adalah negatif, maka semua akar-akarnya harus bukan real.

$$\begin{bmatrix} 1 & 2 \\ 4 & 6 \end{bmatrix}$$

8.6 Ideal di $\mathbb{F}[x]$

Pada bagian ini kita mempelajari ideal-ideal dalam ring polinomial $\mathbb{F}[x]$, dimana $\mathbb{F}$ adalah suatu field. Kita telah mengetahui bahwa $n\mathbb{Z}$ adalah satu-satunya ideal dalam $\mathbb{Z}$, bahwa $p\mathbb{Z}$ adalah ideal prima dalam $\mathbb{Z}$ jika dan hanya jika p adalah bilangan bulat prima, dan $p\mathbb{Z}$ adalah ideal maksimal dalam $\mathbb{Z}$ jika dan hanya jika itu adalah ideal prima. Kita melihat bahwa ideal dalam $\mathbb{F}[x]$ memiliki struktur yang serupa dan polinomial tak tereduksi dalam $\mathbb{F}[x]$ berperilaku seperti bilangan prima dalam $\mathbb{Z}$.

Contoh 8.6.1 Ingat kembali dari Contoh 7.2.5 definisi ideal utama dalam suatu ring komutatif R Jika $a \in R$ maka ideal utama $\langle a \rangle$ yang dibangun oleh a adalah $\{ra \mid r \in R\}$ ideal yang terdiri dari semua kelipatan a Jadi jika $\mathbb{F}$ adalah suatu lapangan, maka ideal utama $\langle x \rangle$ dalam $\mathbb{F}[x]$ yang dibangun oleh x adalah himpunan semua kelipatan x yang artinya, himpunan semua polinomial dalam $\mathbb{F}[x]$ dengan suku konstan 0_R.

Definisi 8.6.1 Misalkan D adalah daerah integral. Maka D disebut **Daerah Ideal Utama** (DIU) jika setiap ideal di D adalah ideal utama.

Contoh 8.6.2 Dari Contoh 7.2.5 dan 7.2.6 kita tahu bahwa $\mathbb{Z}$ adalah DIU, karena seperti yang kita ketahui setiap ideal I dalam $\mathbb{Z}$ yang dibangun oleh sebarang elemen tetap $n \in I$, jadi ideal $I = n\mathbb{Z} = \langle n \rangle$.

Contoh 8.6.3 Sebarang lapangan $\mathbb{F}$ adalah DIU, karena idealnya hanya $\{0_{\mathbb{F}}\} = \langle 0_{\mathbb{F}} \rangle$ dan $\mathbb{F} = \langle 1_{\mathbb{F}} \rangle$.

Teorema 8.6.1 Misalkan $\mathbb{F}$ adalah suatu lapangan, maka $\mathbb{F}[x]$ adalah suatu DIU.

Bukti
Kita tahu dengan Teorema 8.1.1 bahwa $\mathbb{F}[x]$ adalah daerah integral. Kita perlu menunjukkan bahwa untuk setiap ideal I dalam $\mathbb{F}[x]$ terdapat elemen $f(x)$ dari I sedemikian rupa sehingga $I = \langle f(x) \rangle$. Jika I adalah $\{0_{\mathbb{F}}\}$ ideal nol, maka $I = \langle 0_{\mathbb{F}} \rangle$. Jika I bukan ideal nol, misalkan $g(x)$ adalah elemen bukan nol di I dengan derajat minimal. Kita menunjukkan bahwa $g(x)$ membangun I atau, dengan kata lain, $I = \langle g(x) \rangle$. Apa yang harus kita tunjukkan adalah bahwa jika $f(x)$ adalah sebarang elemen dari I, maka $g(x)$ adalah pembagi dari $f(x)$. Untuk menunjukkan ini, kita menerapkan algoritma pembagian untuk menulis $f(x) = q(x)g(x)+r(x)$ dengan $r(x) = 0_{\mathbb{F}}$ atau $\deg r(x) < \deg g(x)$. Karena $r(x) = f(x) - q(x)g(x)$ ada di I dan $g(x)$ dipilih untuk memiliki derajat minimal, kita tidak dapat memiliki $\deg r(x) < \deg g(x)$ dan harus memiliki $r(x) = 0_{\mathbb{F}}$, sehingga $f(x) = q(x)g(x)$ adalah kelipatan dari $g(x)$ sebagai mana yang kita kehendaki.

Dari pembuktian teorema tersebut kita melihat bahwa untuk menemukan generator untuk ideal I dalam $\mathbb{F}[x]$ kita hanya perlu memilih elemen I dengan derajat minimal. Jika $g(x)$ dan $h(x)$ keduanya merupakan elemen dari I berderajat minimal, maka sesuai dengan pembuktian teorema $I = \langle g(x) \rangle = \langle h(x) \rangle)$ dan $g(x) = ch(x)$ dimana c adalah unit dari $\mathbb{F}[x]$ dengan kata lain, konstanta bukan nol.

Teorema 8.6.2 Misalkan $\mathbb{F}$ adalah suatu lapangan. Suatu ideal nontrivial $I = \langle p(x) \rangle$ adalah suatu ideal maksimal dalam $\mathbb{F}[x]$ jika dan hanya jika $p(x)$ tak-tereduksi atas $\mathbb{F}$.

Bukti
($\Rightarrow$) Misalkan $I = \langle p(x) \rangle$ adalah suatu ideal maksimal dalam $\mathbb{F}[x]$. I bukan $\{0_{\mathbb{F}}\} = \langle 0_F \rangle$ atau $\mathbb{F}[x] = \langle 1_{\mathbb{F}} \rangle$ jadi $p(x)$ bukan polinomial nol atau bukan suatu unit di $\mathbb{F}[x]$ yang berarti bukan polinomial konstan. Jika $p(x) = g(x)h(x)$ maka $p(x) \in \langle g(x) \rangle$ dan $I = \langle p(x) \rangle \subseteq \langle g(x) \rangle \subseteq \mathbb{F}[x]\cdot$ Dengan asumsi bahwa I adalah ideal maksimal, kita harus memiliki salah satu $\langle p(x) \rangle = \langle g(x) \rangle$ atau $\langle g(x) \rangle = \mathbb{F}[x]\cdot$ Dalam kasus awal, $\deg g(x) = \deg p(x)$ sedangkan dalam kasus terakhir $\deg g(x) = 0$ dan $\deg h(x) = \deg p(x)$. Ini menunjukkan bahwa $p(x)$ tak-tereduksi atas $\mathbb{F}$. ($\Leftarrow$) Misalkan $p(x)$ tak-tereduksi atas $\mathbb{F}$ dan misalkan $J = \langle f(x) \rangle$ adalah ideal dengan $\langle p(x) \rangle \subseteq J = \langle f(x) \rangle \subseteq \mathbb{F}[x]$. Maka $p(x) \in \langle f(x) \rangle$, yang menyiratkan $p(x) = q(x)f(x)$ untuk beberapa $q(x)$ di $\mathbb{F}[x]$. Dengan asumsi bahwa $p(x)$ tak-tereduksi, kita harus memiliki $\deg f(x) = \deg p(x)$ dan $q(x)$ bukan konstanta nol, atau $\deg q(x) = \deg p(x)$ dan $f(x)$ bukan konstanta nol. Dalam kasus yang pertama, $\langle p(x) \rangle = \langle f(x) \rangle$. Dalam kasus terakhir, $\langle f(x) \rangle = \mathbb{F}[x]$. Ini menunjukkan bahwa $I = \langle p(x) \rangle$ adalah ideal maksimal.

Akibat 8.6.1 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $p(x)$ suatu polinomial bukan nol dalam $\mathbb{F}[x]$. Maka $\langle p(x)\rangle$ adalah ideal prima dalam $\mathbb{F}[x]$ jika dan hanya jika $p(x)$ tak-tereduksi atas $\mathbb{F}$.

Bukti
Anggap pertama bahwa $p(x)$ tak-tereduksi atas $\mathbb{F}$. Maka dengan Teorema 8.6.2, $\langle p(x)\rangle$ adalah ideal maksimal, dan karenanya merupakan ideal prima dalam $\mathbb{F}[x]$. Sebaliknya, jika $\langle p(x)\rangle$ adalah ideal prima dalam $\mathbb{F}[x]$ dan $p(x) = g(x)h(x)$, maka $g(x) \in I = \langle p(x)\rangle$ atau $h(x) \in I = \langle p(x)\rangle$. Dalam kasus yang pertama $\deg g(x) = \deg p(x)$ dan dalam kasus terakhir $\deg h(x) = \deg p(x)$. Ini menunjukkan bahwa $p(x)$ tak-tereduksi atas $\mathbb{F}$. ∎

Akibat 8.6.2 Misalkan $\mathbb{F}$ adalah suatu lapangan dan I ideal nontrivial dalam $\mathbb{F}[x]$. Maka I adalah ideal prima dalam $\mathbb{F}[x]$ jika dan hanya jika I adalah ideal maksimal dalam $\mathbb{F}[x]$.

Bukti
Sebagai Latihan! ∎

Karakterisasi ideal maksimal dalam $\mathbb{F}[x]$ yang disediakan oleh Teorema 8.6.2 memberi kita alat yang sangat penting untuk mengkonstruksi suatu lapangan baru yang memuat lapangan asli $\mathbb{F}$.

Akibat 8.6.3 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $p(x)$ polinomial bukan nol dalam $\mathbb{F}[x]$. Maka $p(x)$ tak-tereduksi atas $\mathbb{F}$ jika dan hanya jika $\mathbb{F}[x]/\langle p(x)\rangle$ adalah suatu lapangan.

Bukti
Sebagai Latihan! ∎

Asumsi dalam Teorema 8.6.1 bahwa $\mathbb{F}$ adalah suatu lapangan sangat penting, seperti dapat dilihat dari contoh berikut, dimana $\mathbb{F}$ bukanlah suatu lapangan.

Contoh 8.6.4 Jika $\mathbb{F}$ adalah suatu lapangan, maka $\mathbb{F}[x][y] = \mathbb{F}[x, y]$ adalah suatu ring polinomial dalam dua tak-tentu (*indeterminates*) x dan y dengan koefisien di $\mathbb{F}$ bukan daerah ideal utama. Untuk mempertimbangkannya sebagai ideal

$$I = \langle x, y\rangle = \{xf(x, y) + yg(x, y) \mid f(x, y), g(x, y) \in \mathbb{F}[x, y]\}.$$

Ideal $I = \langle x, y\rangle$ bukan ideal utama, sebab jika $I = \langle h(x, y)\rangle$ maka karena $x, y \in I, x$ dan y keduanya harus kelipatan dari $h(x, y)$ yang tidak mungkin kecuali $h(x, y)$ adalah konstanta, dalam hal ini $h(x, y) \notin \langle x, y\rangle$. ●

Contoh 8.6.5 Daerah Integral $\mathbb{Z}[x]$ bukan **DIU**. Untuk mempertimbangkannya sebagai ideal

$$I = \langle 2, x\rangle = \{2f(x) + xg(x) \mid f(x), g(x) \in \mathbb{Z}[x]\}.$$

Ideal $I = \langle 2, x\rangle$ bukan merupakan ideal utama, sebab jika $I = \langle h(x)\rangle$ maka karena $2, x \in I; 2$ dan x keduanya merupakan kelipatan dari $h(x)$ yang tidak mungkin kecuali $h(x) = \pm 1$ dalam hal ini $h(x) \notin \langle 2, x\rangle$. ●

Latihan

Dalam Latihan 1 sampai 7: (a) Tunjukkan bahwa himpunan yang ditunjukkan I adalah ideal dalam $\mathbb{Q}[x]$· (b) Tentukan polinomial $g(x)$ dalam $\mathbb{Q}[x]$ sedemikian hingga $I = \langle g(x)\rangle$. (c) Tentukan apakah I adalah ideal maksimal dalam $\mathbb{Q}[x]$.

1. $I = \{f(x) \in \mathbb{Q}[x] \mid f(2) = 0\}$
2. $I = \{f(x) \in \mathbb{Q}[x] \mid f(2) = f(3) = 0\}$
3. $I = \{f(x) \in \mathbb{Q}[x] \mid f(\sqrt{2}) = 0\}$
4. $I = \{f(x) \in \mathbb{Q}[x] \mid f(\sqrt{2}) = f(\sqrt{3}) = 0\}$
5. $I = \{f(x) \in \mathbb{Q}[x] \mid f(1-i) = f(1+i) = 0\}$
6. $I = \{f(x) \in \mathbb{Q}[x] \mid f(i) = f(-i) = 0\}$
7. $I = \{f(x) \in \mathbb{Q}[x] \mid f(1-\sqrt{2}) = f(1+\sqrt{2}) = 0\}$.

Dalam Latihan 8 hingga 14 tentukan apakah ideal yang ditunjukkan maksimal atau tidak dalam $\mathbb{Q}[x]$· Berikan alasan untuk jawaban saudara.

8. $I = \langle x^4 - 4\rangle$
9. $I = \langle x^2 - 5\rangle$
10. $I = \langle x^2 + x + 1\rangle$
11. $I = \langle x^4 - 1\rangle$
12. $I = \langle 6x^5 + 14x^3 - 21x + 42\rangle$
13. $I = \langle x^4 + 4\rangle$
14. $I = \langle 3x^4 + 5x + 1\rangle$.

15. Misalkan R adalah sembarang ring dan I sembarang ideal dalam R. Tunjukkan bahwa $I[x]$ adalah ideal dalam $R[x]$.

16. Dengan $I[x]$ seperti pada soal sebelumnya, jelaskan semua ideal $I[x]$ dalam $R[x]$ untuk
    (a) $R = \mathbb{Z}$ $R = \mathbb{Q}$.

17. Dapatkan semua ideal maksimal $I = \langle g(x)\rangle$ dalam $\mathbb{Z}_3[x]$ dengan $g(x)$ berbentuk $x^2 + ax + b$.

18. Dapatkan semua ideal maksimal $I = \langle g(x)\rangle$ dalam $\mathbb{Z}_5[x]$ dengan $g(x)$ berbentuk $x^2 + ax + 1$.

Dalam Latihan 19 sampai 22 buatlah suatu homomorpisma ring $\phi : \mathbb{Q}[x] \to \mathbb{C}$ yang memiliki ideal K yang ditunjukkan dalam $\mathbb{Q}[x]$ sebagai kernelnya.

19. $K = \langle x^2 - 3\rangle$
20. $K = \langle x^2 + 1\rangle$
21. $K = \langle x^2 + x + 1\rangle$
22. $K = \langle x^4 - 5\rangle$.

23. Buktikan Akibat 8.6.2.

24. Buktikan Akibat 8.6.3.

25. Misalkan $f(x)$ and $g(x)$ adalah dua polinomial tak-nolb di $\mathbb{F}[x]$ dimana $\mathbb{F}$ adalah suatu lapangan. Tunjukkan bahwa ada dengan tunggal suatu polinomial monik $m(x) \in \mathbb{F}[x]$ sedemikian hingga
    (a) $f(x) \mid m(x)$ dan $g(x) \mid m(x)$.
    (b) Bila $f(x) \mid q(x)$ dan $g(x) \mid q(x)$ untuk beberapa $q(x)\mathbb{F}[x]$, maka $m(x) \mid q(x)$.

Dalam hal ini, suatu polinomial $m(x)$ dinamakan kelipatan persekutuan terkecil dari $f(x)$ dan $g(x)$: ditulis sebagai $m(x) = \text{kpk}(f(x), g(x))$.

26. Misalkan $f(x)$ and $g(x)$ adalah dua polinomial tak-nol di $\mathbb{F}[x]$ dimana $\mathbb{F}$ adalah suatu lapangan. Tunjukkan bahwa
    (a) $\langle f(x)\rangle + \langle g(x)\rangle = \langle \text{fpb}(f(x), g(x))\rangle$.
    (b) $\langle f(x)\rangle \cap \langle g(x)\rangle = \langle \text{kpk}(f(x), g(x))\rangle$.

8.7 Ring Kuasi dari $\mathbb{F}[x]$

Pada bagian ini kita membahas ring kuasi dari $\mathbb{F}[x]$ yang merupakan suatu inspirasi penting bagi topik bahasan lapangan berhingga.

Kita akan menggunakan apa yang kita ketahui tentang himpunan bilangan bulat $\mathbb{Z}$ dan ring kuasi $\mathbb{Z}/n\mathbb{Z}$ sebagai panduan untuk memahami struktur ring kuasi $\mathbb{F}[x]/I$ dari ring polinomial $\mathbb{F}[x]$ atas lapangan $\mathbb{F}$.

Mari kita ambil $I \neq \{0_{\mathbb{F}}\}$ ideal dalam $\mathbb{F}[x]$. Dengan Teorema 8.6.1, $I = \langle g(x)\rangle$ untuk suatu polinomial $g(x) \in \mathbb{F}[x]$. Misal $\deg g(x) = n$. Pertimbangkan sembarang polinomial $f(x) \in \mathbb{F}[x]$. Terapkan algoritma pembagian untuk menulis $f(x) = q(x)g(x) + r(x)$ dengan sisa $r(x) = 0_{\mathbb{F}}$ atau $\deg r(x) < \deg g(x) = n$. Jadi $r(x) \in r(x) + I$, dimana

$$r(x) = a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

dan a_i adalah elemen di $\mathbb{F}$. Jadi $f(x)$ berada dalam koset I yang dapat ditulis sebagai

$$(a_{n-1}x^{n-1} + \cdots + a_1x + a_0) + I.$$

Sekarang ingat bahwa I adalah elemen nol, identitas aditif, dalam $F[x]/I$. Kita membuat perubahan notasi untuk membuat perhitungan menjadi tidak rumit. Mulai sekarang kita tulis elemen $x + I \in \mathbb{F}[x]/I$ sebagai α. Maka karena I adalah ideal, $\alpha^i = (x + I)^i = x^i + I$ dan untuk $c_i \in \mathbb{F}$:

$$c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = (c_{n-1}x^{n-1} + \cdots + c_1x + c_0) + I.$$

Khususnya, $g(\alpha) = g(x) + I$, dan karena $I = \langle g(x)\rangle$ kita memiliki $g(\alpha) = I = 0$ di $\mathbb{F}[x]/I$.

Contoh 8.7.1 Sekarang kita dapat mendeskripsikan elemen-elemen dari ring kuasi $\mathbb{Q}[x]/\langle x^2+x+1\rangle$ sebagai berikut. Dapat diselidiki bahwa polinomial $p(x) = x^2+x+1 \in \mathbb{Q}[x]$ tak-tereduksi. Maka berdasarkan Akibat 8.6.3 ring kuasi $\mathbb{Q}[x]/(x^2 + x + 1)$ adalah lapangan. Selanjutnya, karena $I = \langle x^2 + x + 1\rangle$, maka sisa $r(x)$ mod I akan memiliki derajat tidak melebihi satu. Yaitu $r(x) = a_0 + a_1x, \forall a_0, a_1 \in \mathbb{Q}$. Jadi, lapangan

$$\mathbb{Q}[x]/\langle x^2 + x + 1\rangle = \{a_0 + a_1x \mid a_0, a_1 \in \mathbb{Q}\}.$$ ●

Dalam Contoh 8.7.1, banyaknya elemen/kardinalitas dari lapangan $\mathbb{Q}[x]/\langle x^2 + x + 1\rangle$ tak-berhingga. Hal ini bisa kita selidiki dalam SageMath sebagai berikut.

Input

```
%display latex
x=var("x")
R.<x>=QQ[]
p=R(x^2+x+1)
pretty_print(html("$p(x)=%s\\in\\mathbb{Q}[x]$"%latex(p)))
```

Output $p(x) = x^2 + x + 1 \in \mathbb{Q}[x]$

Input

```
pretty_print(html("Apakah $p(x)$ tak-tereduksi?\
$%s$"%latex(p.is_irreducible())))
```

Output Apkah $p(x)$ tak-tereduksi? True

Input

```
I␣=␣R.ideal(p)
pretty_print(html("$I=$␣$%s$"%latex(I)))
```

Output $I = \left(x^2 + x + 1\right)\mathbb{Q}[x]$

Input

```
#␣Mendefinisikan␣ring␣kuasi␣Q[x]/I
R1=R.quotient(I)
```

Input

```
R1.is_field()
```

Output True

Input

```
R1.cardinality()
```

Output $+\infty$

Berbeda dengan contoh sebelumya, contoh berikut mengkonstruksi suatu lapangan berhingga.

Contoh 8.7.2 Karena $x^2 + x + 1$ tak-tereduksi atas $\mathbb{Z}_2$, maka, lagi berdasarkan Akibat 8.6.3 ring kuasi $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ adalah suatu lapangan. Elemen-elemen dari ring kuasi ini adalah

$$\{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{Z}_2\} = \{0, 1, \alpha, 1 + \alpha\},$$

dimana $\alpha^2 + \alpha + 1 = 0$. Perkalian elemen-elemen tak-nol diberikan pada Tabel 8.1:

Tabel 8.1: Perkalian elemen lapangan $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$

$\times$	1	α	$1+\alpha$
1	1	α	$1+\alpha$
α	α	$1+\alpha$	1
$1+\alpha$	$1+\alpha$	1	α

Sedangkan banyaknya elemen-elemen dari lapangan $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ adalah $2^2 = 4$. ●

Perintah-perintah dalam Sagemath untuk menampilkan lapangan berhingga dengan banyaknya elemen $2^2 = 4$, sebagai berikut:

Input

```
%display␣latex
```

```
F_4=GF(2^2,'alpha')
F_4.list()
```

Output $[0, \alpha, \alpha+1, 1]$

Contoh 8.7.3 Kita dapat membuat suatu lapangan dengan elemen $8 = 2^3$ sebagai berikut. Kita mulai dengan $\mathbb{Z}_2[x]$ dan mengambil polinomial berderajat 3 yang tak tereduksi atas $\mathbb{Z}_2$, misalnya, $g(x) = x^3 + x + 1$. Maka $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ adalah lapangan, dan sisa mod $I = \langle x^3 + x + 1\rangle$ adalah polinomial derajat paling besar 2, maka sisa $r(x) = a_2x^2 + a_1x + a_0$ mod I dengan a_i adalah elemen dari $\mathbb{Z}_2$. Karena itu,

$$\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{Z}_2\},$$

dimana $g(\alpha) = \alpha^3 + \alpha + 1 = 0$. Jadi delapan elemen-elemen lapangan ini adalah $0, 1, \alpha + 1, \alpha, \alpha^2, \alpha^2 + 1, \alpha^2 + \alpha$, dan $\alpha^2 + \alpha + 1$. Kita dapat dengan mudah mengerjakan tabel perkalian untuk lapangan ini menggunakan fakta bahwa $\alpha^3 + \alpha + 1 = 0$. Misalnya,

$$\begin{aligned}
\alpha^2(\alpha+1) &= \alpha^3 + \alpha^2 = (\alpha^3 + \alpha + 1) + \alpha^2 + \alpha + 1 = \alpha^2 + \alpha + 1 \\
(\alpha^2)^2 &= \alpha^4 = \alpha(\alpha^3 + \alpha + 1) + \alpha^2 + \alpha = \alpha^2 + \alpha \\
(\alpha^2+1)(\alpha^2+\alpha) &= \alpha^4 + \alpha^3 + \alpha^2 + \alpha = (\alpha+1)(\alpha^3 + \alpha + 1) + \alpha + 1 = \alpha + 1,
\end{aligned}$$

dan begitu juga untuk hasil perkalian lainnya. Hasil perkalian elemen-elemen tak nol dari lapangan berhingga $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ disajikan oleh tabel berikut:

$*$	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1
α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α
$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α	$\alpha+1$
α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α	$\alpha+1$	α^2
α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α	$\alpha+1$	α^2	α^2+1
$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$
$\alpha^2+\alpha+1$	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$

Perintah-perintah dalam Sagemath untuk menampilkan lapangan berhingga dengan banyaknya elemen $2^3 = 8$, sebagai berikut:

Input

```
%display␣latex
F_8=GF(2^3,'alpha')
F_8.list()
```

Output $[0, \alpha, \alpha^2, \alpha+1, \alpha^2+\alpha, \alpha^2+\alpha+1, \alpha^2+1, 1]$

Dari dua contoh terakhir ini kita dapat dengan mudah melihat metode untuk mengkonstruksi suatu lapangan berhingga dengan elemen-elemen sebanyak p^n, dimana p adalah sebarang bilangan prima dan n adalah sebarang bilangan bulat positif. Nanti kita akan melihat bahwa semua lapangan berhingga $\mathbb{F}$ memiliki order p^n untuk $p = \text{khar}(\mathbb{F})$ dan beberapa $n > 0$. Untuk mengetahui karakteristik dari suatu lapangan dalam SageMath, kita gunakan perintah berikut:

Input

```
%display latex
F_8=GF(2^3,'alpha')
F_8.characteristic()
```

Output 2

Contoh 8.7.4 Mari kita lihat bagaimana menemukan invers perkalian dari elemen tak-nol di $\mathbb{F} = \mathbb{Q}[x]/\langle x^2 - 2\rangle$, yang merupakan suatu lapangan sebab $x^2 - 2$ tak-tereduksi atas $\mathbb{Q}$. Faktanya, seperti pada contoh sebelumnya, kita dapat mengetahui bahwa

$$\mathbb{Q}[x]/\langle x^2 - 2\rangle = \{a_0 + a_1\alpha \mid a_0, a_1 \in \mathbb{Q}\},$$

dimana $\alpha^2 = 2$ atau, dengan kata lain, $\mathbb{F} = \mathbb{Q}(\sqrt{2})$. Kita dapat menulis sebarang elemen b di $\mathbb{F}$ sebagai

$$b = a_0 + a_1\sqrt{2},$$

dimana $a_0, a_1 \in \mathbb{Q}$. Jika $b \neq 0$, maka a_0 dan a_1 tidak boleh keduanya nol. Invers b^{-1} juga akan menjadi elemen dari $\mathbb{Q}(\sqrt{2})$ dan karenanya berbentuk

$$b^{-1} = c_0 + c_1\sqrt{2}.$$

Untuk mendapatkan c_0 dan c_1 pertimbangkan dalam $\mathbb{R}$:

$$b^{-1} = \frac{1}{a_0 + a_1\sqrt{2}} = \frac{1}{a_0 + a_1\sqrt{2}} \times \frac{a_0 - a_1\sqrt{2}}{a_0 - a_1\sqrt{2}} = \frac{a_0 - a_1\sqrt{2}}{a_0^2 - 2a_1^2} = \frac{a_0}{a_0^2 - 2a_1^2} - \frac{a_1}{a_0^2 - 2a_1^2}\sqrt{2}.$$

Perhatikan $a_0^2 - 2a_1^2 \neq 0$ karena alasan berikut: Karena a_0 dan a_1 tidak mungkin keduanya nol, jika $a_0^2 - 2a_1^2 = 0$ atau, dengan kata lain, $a_0^2 = 2a_1^2$, keduanya tidak boleh nol, dan kita akan memiliki $a_0/a_1 = \pm\sqrt{2}$, yang tidak mungkin jika $a_0, a_1 \in \mathbb{Q}$, karena $\sqrt{2} \notin \mathbb{Q}$. Jadi kita telah menemukan invers:

$$b^{-1} = c_0 + c_1\sqrt{2} = \frac{a_0}{a_0^2 - 2a_1^2} - \frac{a_1}{a_0^2 - 2a_1^2}\sqrt{2}$$

sebagaimana yang kita inginkan. ●

Contoh yang baru saja dibahas ini, kita selidiki menggunakan SageMath sebagai berikut:

Input

```
%display latex
R.<x>=QQ[x]
p=R(x^2-2)
```

Output $x^2 - 2$

Input

```
%display latex
I=R.ideal(p)
Rp=R.quotient(I)
pretty_print(html("$\\mathbb{Q}[x]/<I>: %s$"%(Rp)))
```

Output $\mathbb{Q}[x]/\langle I\rangle$: Univariate Quotient Polynomial Ring in xbar over Rational Field with modulus $x^2 - 2$

Input

```
Rp.is_field()
```

Output True

Input

```
Rp.characteristic()
```

Output 0

Input

```
Rp.order()
```

Output $+\infty$

Contoh yang dibahas ini dapat digeneralisasi.

Proposisi 8.7.1 Misalkan $f(x)$ dan $g(x)$ merupakan polinomial di $\mathbb{F}[x]$ keduanya tak dapat direduksi atas $\mathbb{F}$ sehingga $f(x) = cg(x)$ untuk setiap *unit* c di $\mathbb{F}[x]$. Maka

(1) $\text{fpb}(f(x), g(x)) = 1$.

(2) Ada $u(x)$ and $v(x)$ di $\mathbb{F}[x]$ sedemikian hingga $1 = u(x)f(x) + v(x)g(x)$.

(3) $u(x)$ adalah invers perkalian dari $f(x)$ di $\mathbb{F}[x]/\langle g(x)\rangle$.

Bukti
Sebagai latihan! ∎

Contoh 8.7.5 Kita dapat menemukan invers terhadap perkalian dari x dalam $\mathbb{Q}[x]/\langle x^3 - 2\rangle$, yang merupakan suatu lapangan sebab $x^3 - 2$ tak-tereduksi atas $\mathbb{Q}$, sebagai berikut. Kita menggunakan algoritma Euclidean:

$$\begin{aligned} x^3 - 2 &= x^2 \cdot x + (-2) \\ x &= (-x/2)(-2) + 0 \end{aligned}$$

untuk memperoleh $1 = (x^2/2)x - (1/2)(x^3 - 2)$, maka $x^2/2$ adalah invers terhadap perkalian dari x di $\mathbb{Q}[x]/\langle x^3 - 2\rangle$. ●

Kita mengerjakan contoh yang baru saja dibahas dalam SageMath sebagai berikut:

Input

```
%display␣latex
R.<x>=QQ[x]
g=R(x^3-2)
```

Output $x^3 - 2$

Input

```
I=R.ideal(g)
Rp=R.quotient(I)
f=R(x)
d,u,v=xgcd(f,g)
(d,u,v)
```

Output $\left(1, \frac{1}{2}x^2, -\frac{1}{2}\right)$

Input

```
1==u*f+v*g
```

Output True

Input

```
f=Rp(x)
f
```

Output *xbar*

Input

```
f^-1
```

Output $\frac{1}{2}xbar^2$

Input

```
f*f^-1
```

Output 1

Input

```
f^-1*f
```

Output 1

Contoh 8.7.6 Kita sekarang menentukan invers terhadap perkalian dari elemen $x + 4$ di $\mathbb{Z}_5[x]/\langle x^3 + x + 1\rangle$ sebagai berikut. (Perhatikan bahwa $x^3 + x + 1$ tak-tereduksi atas $\mathbb{Z}_5$, sebab ia berderajat 3 dan tidak memiliki akar di $\mathbb{Z}_5$.) Kita menggunakan algoritma Euclidean:

$$x^3 + x + 1 = (x^2 + x + 2)(x + 4) + 3.$$

Mengalikan kedua sisi dengan 2 mod 5, kita dapatkan

$$2(x^3 + x + 1) = 2(x^2 + x + 2)(x + 4) + 1,$$

dari sini didapat $(3x^2 + 3x + 1)(x + 4) = 1$ dalam $\mathbb{Z}_5[x]/\langle x^3 + x + 1\rangle$ dan $3x^2 + 3x + 1$ adalah invers terhadap perkalian dari $x + 4$ dalam $\mathbb{Z}_5[x]/\langle x^3 + x + 1\rangle$. ●

Lagi, kita kerjakan contoh ini dalam SageMath sebagai berikut:

Input

```
%display␣latex
Z5␣=␣Integers(5)
R.<x>=Z5[]
g=R(x^3+x+1)
I=R.ideal(g)
Rp=R.quotient(I)
f=Rp(x+4)
f
```

Output $xbar + 4$

Input

```
f^-1
```

Output $3\,xbar^2 + 3\,xbar + 1$

Latihan

Dalam Latihan 1 sampai 4 buatlah suatu lapangan dengan banyaknya elemen n sebagaimana yang ditunjukkan.

1. $n = 9$ 2. $n = 27$
3. $n = 16$ 4. $n = 25$.

Dalam Latihan 5 hingga 14 tentukan apakah ring kuasi yang ditunjukkan adalah lapangan. Jelaskan jawaban saudara.

5. $\mathbb{Q}[x]/\langle x^2 - 5\rangle$ 6. $\mathbb{Q}[x]/\langle x^2 + 3x + 2\rangle$
7. $\mathbb{Z}_3[x]/\langle x^2 + x + 1\rangle$ 8. $\mathbb{C}[x]/\langle x^2 + x + 1\rangle$
9. $\mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ 10. $\mathbb{Q}[x]/\langle x^2 + 1\rangle$
11. $\mathbb{Q}[x]/\langle x^2 - 4\rangle$ 12. $\mathbb{Q}[x]/\langle x - 1\rangle$
13. $\mathbb{C}[x]/\langle x - 2\rangle$ 14. $\mathbb{C}[x]/\langle x^2 + 1\rangle$.

15. Tunjukkan bahwa untuk sebarang p prima ada lapangan dengan banyaknya elemen p^2.

16. Jelaskan elemen dari $\mathbb{Q}[x]/\langle x^2 - 3\rangle$, dan tunjukkan bahwa ring kuasi dari $\mathbb{Q}[x]$ isomorpik dengan $\mathbb{Q}(\sqrt{3})$.

17. Tunjukkan bahwa $\mathbb{R}[x]/\langle x^2 + 1\rangle$ isomorpik dengan $\mathbb{C}$.

18. Tunjukkan bahwa ideal $I = \langle x^2 + 1\rangle$ adalah suatu ideal prima tetapi buka suatu ideal maximal dalam $\mathbb{Z}[x]$.

Dalam Latihan 19 hingga 24, hitung hasil perkalian dari polinomial yang ditunjukkan dalam ring kuasi yang diberikan.

19. $3x + 2$ dan $5x - 3$ dalam $\mathbb{Q}[x]/\langle x - 2\rangle$
20. $5x + 1$ dan $2x + 3$ dalam $\mathbb{Q}[x]/\langle x^2 - 2\rangle$
21. $x^2 + 2x - 3$ dan $x^2 + 3x + 1$ dalam $\mathbb{Q}[x]/\langle x^3 + 2\rangle$
22. $x^2 + x + 1$ dan $x^2 + 1$ dalam $\mathbb{Z}_2[x]/\langle x^4 + x + 1\rangle$
23. $x^2 + 2x + 2$ dan $x^2 + 2$ dalam $\mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle$
24. $ax + b$ dan $cx + d$ dalam $\mathbb{Q}[x]/\langle x^2 + 1\rangle$.

Dalam Latihan 25 hingga 30 tentukan generator dari ideal yang ditunjukkan dalam ring yang diberikan.

25. $\langle 4\rangle \cap \langle 6\rangle$ dalam $\mathbb{Z}$
26. $\langle x - 1\rangle \cap \langle x^2 - 1\rangle$ dalam $\mathbb{Q}[x]$
27. $\langle x^2 + x + 1\rangle \cap \langle x^3 - 1\rangle$ dalam $\mathbb{Q}[x]$
28. $\langle x + 1\rangle \cap \langle x^2 + 1\rangle$ dalam $\mathbb{Z}_2[x]$
29. $\langle x^2 - 5x + 6\rangle \cap \langle x^2 - 3x + 2\rangle$ dalam $\mathbb{Q}[x]$
30. $\langle x^2 + x + 1\rangle \cap \langle x^2 + 2\rangle$ dalam $\mathbb{Z}_3[x]$.

31. Misalkan $\mathbb{F}$ adalah suatu lapangan dan misalkan $I = \langle f(x)\rangle$ dan $J = \langle g(x)\rangle$ adalah dua ideal dalam $\mathbb{F}[x]$. Buktikan hasil umum tentang generator dari ideal $I \cap J$. (Petunjuk: Lihat latihan sebelumnya.)

32. Buktikan Proposisi 8.7.1.

Dalam Latihan 33 hingga 37, tentukan invers terhadap perkalian dari elemen yang ditunjukkan dalam lapangan yang diberikan.

33. x dalam $\mathbb{R}[x]/\langle x^2 + 1\rangle$
34. $x + 1$ dalam $\mathbb{Z}_5[x]/\langle x^3 + x + 1\rangle$
35. $x^2 + 1$ dalam $\mathbb{Z}_3[x]/\langle x^3 + 2x + 1\rangle$
36. $x^2 - x + 1$ dalam $\mathbb{Q}[x]/\langle x^3 - 2\rangle$
37. $x + 3$ dalam $\mathbb{Q}[x]/\langle x^2 - 2\rangle$.

8.8 Terorema Sisa untuk $\mathbb{F}[x]$

Dalam semua contoh bagian sebelumnya, kita menganggap ring kuasi $\mathbb{F}[x]/\langle p(x)\rangle$ dimana $p(x)$ adalah polinomial tak tereduksi atas $\mathbb{F}$ sehingga ring kuasi adalah suatu lapangan. Pada bagian ini kita mempertimbangkan ring kuasi dimana $p(x)$ belum tentu tak-tereduksi atas $\mathbb{F}$ sehingga ring kuasi mungkin bukan daerah integral. Sebagai kunci untuk memahami struktur ring tersebut, kita menggunakan teorema sisa Cina untuk $\mathbb{F}[x]$. Kita mencoba untuk memahami setidaknya beberapa ring kuasi $\mathbb{F}[x]/\langle p(x)\rangle$ dimana $p(x)$ bukan tak-tereduksi atas $\mathbb{F}$.

Contoh 8.8.1 diberikan

$$\mathbb{Z}_2[x]/\langle x^2 + x\rangle = \{a_0 + a_1\alpha \mid a_i \in \mathbb{Z}_2, \alpha^2 + \alpha = 0\}$$

Ini adalah ring dengan empat elemen $0, 1, \alpha, 1 + \alpha$ dengan tabel penjumlahan dan perkalian ditunjukkan pada tabel berikut.

Jika kita memisalkan $\phi : \mathbb{Z}_2[x]/\langle x^2 + x\rangle \to \mathbb{Z}_2 \times \mathbb{Z}_2$ adalah suatu homomorpisma ring sedemikian rupa sehingga

$$\phi(0) = (0, 0), \phi(1) = (1, 1), \phi(\alpha) = (1, 0), \phi(1 + \alpha) = (0, 1).$$

Tabel: Penjumlahan

+	0	1	α	1+α
0	0	1	α	1+α
1	1	0	1+α	α
α	α	1+α	0	1
1+α	1+α	α	1	0

Tabel: Perkalian

·	1	α	1+α
1	1	α	1+α
α	α	α	0
1+α	1+α	0	1+α

Kita dapat dengan mudah memverifikasi bahwa ϕ adalah suatu isomorpisma ring, dengan demikian $\mathbb{Z}_2[x]/\langle x^2+x\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. ●

Contoh 8.8.2 Pertimbangkan ring kuasi

$$\mathbb{Q}[x]/\langle x^3-2x\rangle = \{a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{Q} \text{ dan } \alpha^3 - 2\alpha = 0\}.$$

Untuk sebarang polinomial $f(x)$ di $\mathbb{Q}[x]$ kita mempertimbangkan tiga pembagian, membagi $f(x)$ dengan x^3-2x dengan dua faktor yang tak-tereduksi, x dan x^2-2:

$$\begin{aligned} f(x) &= q(x)(x^3-2x) + (a_0 + a_1x + a_2x^2) \\ f(x) &= q(x)(x^2-2)x + (a_1 + a_2x)x + a_0 \\ f(x) &= q(x)x(x^2-2) + a_2(x^2-2) + (a_0 + 2a_2 + a_1x). \end{aligned}$$

Dengan demikian, kita memiliki

$$\begin{aligned} f(x) &= (a_0 + a_1x + a_2x^2) \mod \langle x^3-2x\rangle \\ f(x) &= a_0 \mod \langle x\rangle \\ f(x) &= (a_0 + 2a_2 + a_1x) \mod \langle x^2-2\rangle. \end{aligned}$$

Pertimbangkan homomorpisma evaluasi:

$$\phi_0 : \mathbb{Q}[x] \to \mathbb{Q}[x]/\langle x\rangle \cong \mathbb{Q},$$

dimana $\phi_0(f(x)) = f(0) = a_0$ dan

$$\phi_{\sqrt{2}} : \mathbb{Q}[x] \to \mathbb{Q}[x]/\langle x^2-2\rangle \cong \mathbb{Q}(\sqrt{2}),$$

dimana $\phi_{\sqrt{2}}(f(x)) = f(\sqrt{2}) = (a_0 + 2a_2) + a_1\sqrt{2}$.

Dua homomorpisma ring tsb. menginduksi homomorpisma ring:

$$\phi : \mathbb{Q}[x] \to \mathbb{Q} \times \mathbb{Q}(\sqrt{2}),$$

dimana $\phi(f(x)) = \big(\phi_0(f(x)), \phi_{\sqrt{2}}(f(x))\big)$.

Perhatikan bahwa $f(x)$ berada di kernel ϕ tepat ketika $f(x)$ berada di kernel ϕ_0 dan $\phi_{\sqrt{2}}$ atau, dengan kata lain, ketika

$$f(x) \in \langle x\rangle \cap \langle x^2-2\rangle = \langle x^3-2x\rangle.$$

Juga, ϕ pada sebab diberikan sebarang elemen $(a_0, b+a_1\sqrt{2})$ di $\mathbb{Q}\times\mathbb{Q}(\sqrt{2})$, kita dapat memilih

$$g(x) = a_0 + a_1x + \frac{b-a_0}{2}x^2$$

yang memenuhi $\phi(g(x)) = (a_0, b+a_1\sqrt{2})$. Jadi, ϕ menghasilkan isomorpisma $\mathbb{Q}[x]/\langle x^3-2x\rangle \cong \mathbb{Q}\times\mathbb{Q}(\sqrt{2})$. ●

Dalam kedua contoh, kita mengambil suatu ideal mod hasil bagi dengan polinomial yang dapat direduksi sebagai generator. Pada contoh pertama,

$$I = \langle x^2 + x \rangle = \langle x(x+1) \rangle.$$

Pada contoh yang kedua,

$$I = \langle x^3 - 2x \rangle = \langle x(x^2 - 2) \rangle.$$

Generator dalam kedua kasus memfaktorkan menjadi dua faktor yang relatif prima dan ring kuasi ternyata berbentuk $R_1 \times R_2$. Pada contoh pertama,

$$\mathbb{Z}_2[x]/\langle x^2 + x \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Pada contoh kedua,

$$\mathbb{Q}[x]/\langle x^3 - 2x \rangle \cong \mathbb{Q} \times \mathbb{Q}(\sqrt{2}).$$

Ini bukanlah suatu kebetulan, seperti yang kita lihat dalam teorema berikut.

Teorema 8.8.1 ***(Teorema Sisa Pembagian China)*** Misalkan $\mathbb{F}$ adalah suatu lapangan dan misalkan

$$I_1 = \langle g_1(x) \rangle, I_2 = \langle g_2(x) \rangle, \ldots, I_n = \langle g_n(x) \rangle$$

adalah ideal dalam $\mathbb{F}[x]$ sehingga untuk semua i dan j dengan $i \neq j$ kita miliki

$$\text{fpb}(g_i(x), g_j(x)) = 1,$$

dan misalkan $f_1(x), \ldots, f_n(x)$ sembarang polinomial dalam $\mathbb{F}[x]$. Maka

(1) Ada suatu $f(x) \in \mathbb{F}[x]$ sedemikian hingga untuk $i = 1, 2, \ldots n$ berlaku $f(x) - f_i(x) \in I_i$.

(2) $f(x)$ ini ditentukan secara tunggal hingga kongruensi modulo ideal

$$J = \langle g_1(x) \cdot g_2(x) \cdots g_n(x) \rangle.$$

Bukti

(1) Untuk sebarang tetap $s = 1, 2, \ldots, n$, misalkan

$$J_s = \bigcap_{i \neq s} I_i = \langle g_1(x) \cdots g_{s-1}(x) \cdot g_{s+1}(x) \cdots g_n(x) \rangle .$$

Maka J_s dan $I_s = \langle g_s(x) \rangle$ adalah dua ideal dalam $\mathbb{F}[x]$ yang generatornya relatif prima. Oleh karena itu $\mathbb{F}[x] = I_s + J_s$. Akibatnya, untuk setiap $f_s(x)$ di $\mathbb{F}[x]$ terdapat $h_s(x)$ di I_s dan $k_s(x)$ di J_s sedemikian rupa sehingga $f_s(x) = h_s(x) + k_s(x)$. Selanjutnya, $k_s(x) + I_s = f_s(x) + I_s$ dan $k_s(x) + I_j = 0 + I_j$ untuk $j \neq s$. Misal $f(x) = k_1(x) + \cdots + k_n(x)$; maka $[f(x) - f_i(x)] + I_i = [f(x) - k_i(x)] + I_i = 0 + I_i$ dan (1) terbukti.

(2) Jika $f'(x) \in \mathbb{F}[x]$ sedemikian rupa sehingga $f'(x) - f_i(x) \in I_i$ untuk $i = 1, \ldots, n$, maka $f(x) - f'(x) \in I_i$ untuk $i = 1, \ldots, n$ dan

$$f(x) - f'(x) \in \bigcap_{i=1}^{n} I_i = J$$

dengan demikian (2) terbukti. ✓

Akibat wajar berikutnya memberi kita alat penting untuk menghitung ring kuasi dari $\mathbb{F}[x]$.

Akibat 8.8.1 Misalkan $\mathbb{F}$ adalah suatu lapangan dan misalkan $I_i = \langle g_i(x)\rangle$ untuk $i = 1, \ldots, n$ adalah ideal dalam $\mathbb{F}[x]$, dengan fpb $(g_i(x), g_j(x)) = 1$ untuk $i \neq j$ dan misalkan $J = \langle g_1(x) \cdots g_n(x)\rangle$. Maka

$$\mathbb{F}[x]/J \cong \mathbb{F}[x]/I_1 \times \cdots \times \mathbb{F}[x]/I_n.$$

Bukti
Pertama kita definisikan homomorpisma. Pertimbangkan ring homomorpisma $\phi_i : \mathbb{F}[x] \to \mathbb{F}[x]/I_i$ dimana ϕ_i memetakan setiap polinomial $f(x) \in \mathbb{F}[x]$ ke sisa mod I_i. Pemetaan ϕ_i menginduksi suatu homomoipisma ring:

$$\phi : \mathbb{F}[x] \to \mathbb{F}[x]/I_1 \times \cdots \times \mathbb{F}[x]/I_n,$$

dimana

$$\phi(f(x)) = \Big(\phi_1(f(x)), \ldots, \phi_n(f(x))\Big), \ \forall f(x) \in \mathbb{F}[x].$$

Selanjutnya kita tunjukkan $\ker(\phi) = J$. Misalkan K adalah kernel dari ϕ. Maka $f(x) \in K$ jika dan hanya jika $\phi(f(x)) = (0, \ldots, 0)$, dan ini terjadi jika dan hanya jika $f(x) \in I_i$ untuk semua $i = 1, \ldots, n$, dan karenanya jika dan hanya jika $f(x) \in J$.

Terakhir, kita tunjukkan bahwa ϕ pada. Diberikan sebarang

$$(g_1(x), \ldots, g_n(x)) \in \mathbb{F}[x]/I_1 \times \cdots \times \mathbb{F}[x]/I_n,$$

karena setiap homomorpisma ϕ_i adalah pada, maka $g_i = \phi_i(f_i(x))$ untuk beberapa $f_i(x) \in \mathbb{F}[x]$. Jadi menurut Teorema 8.8.1 terdapat $f(x) \in \mathbb{F}[x]$ sedemikian hingga $f(x) - f_i(x) \in I_i$ untuk semua $i = 1, \ldots, n$. Oleh karena itu $\phi_i(f(x) - f_i(x)) = 0$ dan $\phi(f(x)) = (\phi_1(f_1(x)), \ldots, \phi_n(f_n(x))) = (f_1(x), \ldots, f_n(x))$ Jadi akibat wajarnya mengikuti teorema isomorpisma pertama untuk ring (Teorema 7.2.2), didapat $\mathbb{F}[x]/J \cong \mathbb{F}[x]/I_1 \times \cdots \times \mathbb{F}[x]/I_n$. ∎

Contoh 8.8.3 Kita membahas ring kuasi $\mathbb{Q}[x]/\langle x^4 - 8x^2 + 15\rangle$. Kita mempunyai $x^4 - 8x^2 + 15 = (x^2 - 3)(x^2 - 5)$, dengan faktor $x^2 - 3$ dan $x^2 - 5$ relatif prima. Karena itu, dengan menggunakan Akibat 8.8.1, didapat

$$\mathbb{Q}[x]/\langle x^4 - 8x^2 + 15\rangle \cong \mathbb{Q}[x]/\langle x^2 - 3\rangle \times \mathbb{Q}[x]/\langle x^2 - 5\rangle \cong \mathbb{Q}(\sqrt{3}) \times \mathbb{Q}(\sqrt{5}).$$ ●

Contoh 8.8.4 Diberikan ring kuasi $\mathbb{Q}[x]/\langle x^3 + 3x^2 + 2x\rangle$. Kita mempunyai $x^3 + 3x^2 + 2x = x(x + 1)(x + 2)$, dengan faktor $x, x + 1$ dan $x + 2$ relatif prima dan $\mathbb{Q}[x]/\langle x + a\rangle \cong \mathbb{Q}$. Dengan demikian, menurut Akibat 8.8.1 kita mempunyai $\mathbb{Q}[x]/\langle x^3 + 3x^2 + 2x\rangle \cong \mathbb{Q}[x]/\langle x\rangle \times \mathbb{Q}[x]/\langle x + 1\rangle \times \mathbb{Q}[x]/\langle x + 2\rangle \cong \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$. ●

Contoh 8.8.5 Diberikan ring kuasi $\mathbb{R}[x]/\langle x^3 + x\rangle$. Kita mempunyai $x^3 + x = x(x^2 + 1)$, dengan faktor x dan $x^2 + 1$ relatif prima; dan $\mathbb{R}[x]/\langle x\rangle \cong \mathbb{R}$ juga $\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C}$. Dengan demikian, sekali lagi menurut Akibat 8.8.1 kita mempunyai $\mathbb{R}[x]/\langle x^3 + x\rangle \cong \mathbb{R}[x]/\langle x\rangle \times \mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{R} \times \mathbb{C}$. ●

Akhirnya, kita melihat beberapa ring kuasi $\mathbb{F}[x]/\langle f(x)\rangle$ dimana polinomial $f(x)$ memiliki faktor berulang.

Tabel Penjumlahan

+	0	1	α	1+α
0	0	1	α	1+α
1	1	0	1+α	α
α	α	1+α	0	1
1+α	1+α	α	1	0

Tabel Perkalian

·	1	α	1+α
1	1	α	1+α
α	α	0	α
1+α	1+α	α	1

Contoh 8.8.6 Mari kita membahas ringnya.

$$\mathbb{Z}_2[x]/\langle x^2\rangle = \{a_0 + a_1\alpha \mid a_i \in \mathbb{Z}_2 \text{ dan } \alpha^2 = 0\}.$$

Ini adalah ring dengan empat elemen $0, 1, \alpha, 1+\alpha$ dengan tabel penjumlahan dan perkalian seperti pada tabel berikut:

Perhatikan bahwa **Tabel Penjumlahan**, sama dengan **Tabel Penjumlahan** $\mathbb{Z}_2 \times \mathbb{Z}_2$, tetapi **Tabel Perkalian**, sama dengan **Tabel Perkalian** untuk $\mathbb{Z}_4$. Oleh karena itu, ini adalah ring dengan empat elemen yang bukan merupakan daerah integral dan tidak isomorpik baik terhadap $\mathbb{Z}_2 \times \mathbb{Z}_2$ atau $\mathbb{Z}_4$. ●

Contoh 8.8.7 Pertimbangkan ring kuasi

$$\mathbb{Q}[x]/\langle x^2\rangle = \{a_0 + a_1\alpha \mid a_i \in \mathbb{Q} \text{ dan } \alpha^2 = 0\}.$$

Tabel penjumlahan ring kuasi ini sama dengan tabel penjumlahan $\mathbb{Q} \times \mathbb{Q}$. Tetapi tabel perkalian diberikan oleh

$$(a_0 + a_1\alpha)(b_0 + b_1\alpha) = a_0b_0 + (a_0b_1 + a_1b_0)\alpha.$$

Untuk mendapatkan gambaran yang lebih baik dari ring kuasi ini, untuk $a_0, a_\in\mathbb{Q}$, pertimbangkan matriks $M(a_0, a_1)$ yang diberikan oleh

$$M(a_0, a_1) = \begin{bmatrix} a_0 & 0 \\ a_1 & a_0 \end{bmatrix}.$$

Selanjutnya, misalkan $M_2 = \{M(a_0, a_1) \mid a_i \in \mathbb{Q}\}$. Maka M_2 adalah suatu ring dan sebarang elemen dari M_2 dapat ditulis ulang sebagai $a_0\mathbf{1} + a_1\boldsymbol{u}$ dimana,

$$\mathbf{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \boldsymbol{u} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.$$

Dan akhirnya, $\mathbb{Q}[x/\langle x^2\rangle \cong M_2$. ●

Latihan

Dalam Latihan 1 sampai 6 jelaskan ring kuasi yang ditunjukkan (seperti pada Contoh 8.8.3 sampai 8.8.5).

1. $\mathbb{Q}[x]/\langle x^2 + x\rangle$
2. $\mathbb{Q}[x]/\langle x^3 + x\rangle$
3. $\mathbb{R}[x]/\langle x^2 + x\rangle$
4. $\mathbb{C}[x]/\langle x^3 + x\rangle$
5. $\mathbb{Z}_2[x]/\langle x^3 + x^2 + x\rangle$
6. $\mathbb{Z}_3[x]/\langle x^3 + x\rangle$.

7. Misalkan $\mathbb{F}$ adalah suatu lapangan dan misalkan $I = \langle f(x)\rangle$ dan $J = \langle g(x)\rangle$ adalah dua ideal dalam $\mathbb{F}[x]$, dimana fpb$(f(x), g(x)) = 1$. Tunjukkan bahwa $I + J = \mathbb{F}[x]$.

8. Misalkan R adalah suatu ring dengan elemen satuan 1_R, dan misalkan $I_1, \ldots, I_n$ adalah ideal dalam R sedemikian hingga $I_i + I_j = R$ untuk semua $i \neq j$. Tunjukkan bahwa untuk $a_1, \ldots, a_n$ di R ada b di R sedemikian rupa sehingga $b - a_i \in I_i$ untuk semua $i = 1, \ldots, n$. (Petunjuk: Pertama tunjukkan bahwa $I_s + \bigcap_{i \neq s} I_i = R$. Kemudian tirulah pembuktian Teorema 8.8.1.)

9. Misalkan R merupakan ring dengan elemen satuan 1_R, dan misalkan $I_1, \ldots, I_n$ merupakan ideal dalam R sehingga $I_i + I_j = R$ untuk semua $i \neq j$. Tunjukkan bahwa terdapat suatu isomorpisma ring:

$$\theta : R/(I_1 \cap \cdots \cap I_n) \to R/I_1 \times \cdots \times R/I_n.$$

(Petunjuk: Gunakan Latihan 8.)

Dalam Latihan 10 sampai 13 tuliskan tabel penjumlahan dan perkalian untuk ring kuasi berikut (seperti pada Contoh 8.8.6).

10. $\mathbb{Z}_2[x]/\langle x^3\rangle$ 11. $\mathbb{Z}_3[x]/\langle x^2\rangle$

12. $\mathbb{Z}_2[x]/\langle x^2 + 1\rangle$ 13. $\mathbb{Z}_3[x]/\langle x^2 + x + 1\rangle$.

14. Misalkan $M_2 = \left\{ \begin{bmatrix} a_0 & 0 \\ a_1 & a_0 \end{bmatrix} \middle| a_0, a_1 \in \mathbb{Q} \right\}$. Tunjukkan bahwa

(a) M_2 adalah ring terhadap penjumlahan dan perkalian matriks.

(b) Sebagai grup terhadap penjumlahan matriks, M_2 isomorpik dengan $\mathbb{Q} \times \mathbb{Q}$.

(c) M_2 isomorpik dengan $\mathbb{Q}[x]/\langle x^2\rangle$.

15. Dengan menggunakan latihan sebelumnya, tulis empat matriks yang sesuai dengan empat elemen dari $\mathbb{Z}_2/\langle x^2\rangle$ (seperti pada Contoh 8.8.6).

16. Dengan menggunakan Contoh 8.8.7 dan latihan sebelumnya sebagai model kita, buatlah suatu ring matriks isomorpik dengan $\mathbb{Q}[x]/\langle x^3\rangle$.

17. Generalisasikan hasil latihan sebelumnya ke $\mathbb{Q}[x]/\langle x^n\rangle$ untuk sebarang $n > 1$.

18. Misalkan $N_2 = \left\{ \begin{bmatrix} a_0 - a_1 & 0 \\ a_1 & a_0 - a_1 \end{bmatrix} \middle| a_0, a_1 \in \mathbb{Q} \right\}$. Tunjukkan bahwa

(a) N_2 adalah ring terhadap penjumlahan dan perkalian matriks.

(b) N_2 isomorpik dengan $\mathbb{Q}[x]/\langle (x+1)^2\rangle$.

(c) $\mathbb{Q}[x]/\langle (x+1)^2\rangle$ isomorpik dengan $\mathbb{Q}[x]/\langle x^2\rangle$.

Bab 9

Daerah Euclid

Telah dikenal dua daerah integral yaitu $\mathbb{Z}$ dan $\mathbb{F}[x]$ dimana $\mathbb{F}$ adalah suatu lapangan, dengan kesamaan dari keduanya. Telah dibuktikan teorema faktorisasi tunggal untuk $\mathbb{Z}$ (berdasarkan Teorema aritmatika, 1.3.7) dan untuk $\mathbb{F}[x]$ (Teorema 8.4.2). Telah ditunjukkan bahwa keduanya adalah daerah integral yang merupakan ideal utama (Contoh 7.2.2 dan Teorema 8.6.1). Bila dilihat kembali pada cara penurunan sifat mendasar dari $\mathbb{Z}$ dan $\mathbb{F}[x]$, hal ini tidak lain bahwa kesemuanya adalah akibat dari satu teorema kunci yaitu: algoritma pembagian, Teorema 1.3.4 untuk $\mathbb{Z}$ dan Teorema 8.2.1 untuk $\mathbb{F}[x]$. Dalam bab ini pertama dibahas daerah integral yang mana memenuhi suatu algorithma pembagian (Daerah Euclide). Selanjutnya ditunjukkan bahwa derah integral yang demikian selalu merupakan daerah ideal utama (DIU) dan dalam DIU suatu teorema faktorisasi tunggal selalu dipenuhi. Kemudian dibahas daerah integral yang demikian tersebut yaitu mempunyai sifat faktorisasi tunggal (DFT) dan dibuktikan inklusi klas dari daerah integral berikut:

Daerah Integral $\supset$ **DFT** $\supset$ **DIU** $\supset$ Lapangan

Akhir dari bab ini adalah pembahasan mengenai himpunan bilangan bulat Gaussian $\mathbb{Z}[i]$ dan suatu aplikasinya yang dikenal dalam teori bilangan yaitu teorema Fermat.

9.1 Algorithma Pembagian dan Daerah Euclid

Algoritma pembagian memungkinkan kita untuk mendefinisikan pengertian seperti FPB tersebut dan KPK dari dua bilangan bulat. Definisi yang sama diperkenalkan di Bab 8 untuk polinomial dengan koefisien di lapangan, sebagai konsekuensi dari Teorema 8.2.1. Dalam kasus $\mathbb{Z}$ nilai mutlak dari suatu bilangan bulat digunakan untuk mengekspresikan sisa r dari pembagian suatu bilangan bulat dengan bilangan bulat b dimana $|r| < b$. Dalam kasus $\mathbb{F}[x]$ digunakan derajad dari polinomial untuk mengungkapkan sisa $r(x)$ dari pembagian suatu polinomial di $\mathbb{F}[x]$ dengan polinomial $g(x)$, dimana $\deg(r(x)) < \deg(g(x))$. Oleh karena itu, dalam rangka untuk mencari daerah integral yang lain dengan algoritma pembagian, harus dicari daerah integral yang dilengkapi dengan fungsi mirip dengan nilai mutlak seperti di $\mathbb{Z}$ atau seperti derajad sebagaimana di $\mathbb{F}[x]$ yang mengaitkan setiap elemen dari daerah integral dengan bilangan bulat taknegatif.

Contoh 9.1.1 Jika $\mathbb{F}$ adalah suatu lapangan, maka untuk $a, b \neq 0$ dalam $\mathbb{F}, a = qb + r$, dimana $r = 0$ dan $q = ab^{-1}$. Secara khusus, dalam lapangan bilangan kompleks $\mathbb{C}$, pertimbangkan $z = 3 + 2i$ dan $w = 1 + i$. Maka

$$zw^{-1} = (3 + 2i)(1 + i)^{-1} = (3 + 2i)(1 - i)^{-1}(1 - i)(1 + i)^{-1} = \frac{5}{2} - \frac{i}{2}. \tag{9.1}$$

Oleh karena itu dalam $\mathbb{C}, z = \left(\frac{5}{2} - \frac{i}{2}\right) w = qw$.

Sekarang mari kita pertimbangkan $z = 3+2i$ dan $w = 1+i$ sebagai elemen dari himpunan bilangan bulat Gaussian $\mathbb{Z}[i]$, yang merupakan subdomain dari $\mathbb{C}$. Pembagian yang baru saja kita lakukan di (9.1) tidak bisa dilakukan dalam $\mathbb{Z}[i]$, karena $q = \frac{5}{2} - \frac{i}{2} \notin \mathbb{Z}[i]$. Mari kita manipulasi q untuk menghilangkan penyebutnya:

$$q = \frac{5}{2} - \frac{i}{2} = (2 - i) + \left(\frac{1}{2} + \frac{i}{2}\right).$$

Karena itu,

$$z = 3 + 2i = qw = (2 - i)w + \left(\frac{1}{2} + \frac{i}{2}\right) w = (2 - i)(1 + i) + \left(\frac{1}{2} + \frac{i}{2}\right)(1 + i).$$

Jadi, $z = (2 - i)w + i \in \mathbb{Z}[i]$. Dengan demikian, kita bisa menulis z dalam bentuk $z = q'q + r'$ dimana $q', r' \in \mathbb{Z}[i]$. Perhatikan bahwa sisa $r' = i$ yang kita temukan memenuhi kondisi berikut:

$$|i|^2 = 1 < 2 = |1 + i|^2.$$

Untuk setiap elemen $x = a + bi \in \mathbb{Z}[i], |x|^2 = a^2 + b^2 = x\bar{x}$ dan jika $y \in \mathbb{Z}[i]$, maka

$$|x|^2 \leq |xy|^2 = |x|^2|y|^2.$$

Seperti yang kita lihat dalam Proposisi 9.1.1, fungsi $v : \mathbb{Z}[i] - \{0\} \to \mathbb{Z}$ yang didefinisikan oleh $v(x) = |x|^2$ memunculkan algoritma pembagian untuk himpunan bilangan bulat Gaussian $\mathbb{Z}[i]$. ●

Kita sekarang memperkenalkan definisi dasar untuk bab ini.

Definisi 9.1.1 Daerah integral D disebut **Daerah Euclide** jika ada ada fungsi $v : D - \{0_D\} \to \mathbb{Z}^+ \cup \{0\}$ dari himpunan elemen bukan nol D ke himpunan bilangan bulat tak negatif sedemikian rupa sehingga

(1) Untuk $x \neq 0_D$ and $y \neq 0_D$ di D

$$v(x) \leq v(xy).$$

(2) Diberikan a dan $b \neq 0_D$ di D terdapat q dan r di D sedemikian rupa sehingga

$$a = qb + r, \text{ dimana } r = 0_D \text{ atau } v(r) < v(b).$$

Elemen q disebut **hasil bagi** dan elemen r merupakan **sisa pembagian**. ●

Contoh 9.1.2 Kita sudah mengetahui beberapa contoh daerah Euclide.

(1) $\mathbb{Z}$ adalah daerah Euclide dengan $v(a) = |a|$ untuk semua $0 \neq a \in \mathbb{Z}$, karena untuk bilangan bulat bukan nol $a, b, 1 < |b|$ menyiratkan $v(a) = |a| < |a|\,|b| = |ab| = v(ab)$.

(2) Sebarang lapangan $\mathbb{F}$ adalah daerah Euclide dengan $v(a) = 0_{\mathbb{F}}$ untuk semua $a \in \mathbb{F}^*$.

(3) Jika $\mathbb{F}$ adalah suatu lapangan, maka $\mathbb{F}[x]$ adalah daerah Euclide dengan $v(f(x)) = \deg(f(x))$.

Perhatikan bahwa kondisi (1) dari Definisi 9.1.1 dipenuhi dari Teorema 8.1.1, bagian (4), dan kondisi (2) diberikan oleh Teorema 8.2.1. ●

Proposisi 9.1.1 Himpunan bilangan bulat Gaussian $\mathbb{Z}[i]$ dengan fungsi $v(z) = a^2 + b^2$ untuk semua $z = a + i \neq 0$ di $\mathbb{Z}[i]$ adalah daerah Euclide.

Bukti

(1) Jika $z = a + bi \neq 0$, maka $v(z) = a^2 + b^2 \geq 1$. Sebagai tambahan, $a^2 + b^2 = z\overline{z}$, dan karenanya untuk $w \neq 0$ di $\mathbb{Z}[i]$, maka $v(zw) = zw\ \overline{zw} = zw\ \overline{z}\ \overline{w} = z\overline{z}\ w\overline{w} = v(z)v(w)$ dan $1 \leq v(z), 1 \leq v(w)$. Oleh karena itu $v(z) \leq v(z)v(w) = v(zw)$.

(2) Kita menunjukkan bahwa algoritma pembagian berlaku di $\mathbb{Z}[i]$. Diberikan sebarang z dan $w \neq 0$ di $\mathbb{Z}[i]$, pertimbangkan z dan w terlebih dahulu sebagai elemen di $\mathbb{C}$. Maka

$$zw^{-1} = z(\overline{w}\ \overline{w}^{-1})w^{-1} = z\overline{w}(\overline{w}w)^{-1}.$$

Oleh karena itu, $z(w)^{-1} \in \mathbb{Q}(i)$. Jadi $z(w)^{-1} = u + vi$, dimana $u, v \in \mathbb{Q}$. Sekarang misalkan

$$u = a + u' \text{ dan } v = b + v',$$

dimana a dan b masing-masing adalah bilangan bulat yang paling dekat dengan u dan v. Jadi

$$|u'| \leq \frac{1}{2} \quad \text{dan} \quad |v'| \leq \frac{1}{2}.$$

Oleh karena itu

$$\begin{aligned} z &= (u + vi)w \\ &= uw + vwi \\ &= (a + u')w + (bi + v'i)w \\ &= (a + bi)w + (u' + v'i)w. \end{aligned}$$

Amati bahwa $(u' + v'i)w = z - (a + bi)w \in \mathbb{Z}[i]$, dan oleh karena itu $z = qw + r$, dimana $q = a + bi \in\ Z[i]$ dan $r = (u' + v'i)w \in \mathbb{Z}[i]$. Tinggal menunjukkan bahwa

$$r = 0 \text{ atau } v(r) < v(w).$$

Ini berlaku, sebab bila $r \neq 0$, maka

$$\begin{aligned} v(r) &= v((u' + v'i)w) \\ &= v((u' + v'i))v(w) \\ &= (|u'|^2 + |v'|^2)v(w) \\ &\leq (\frac{1}{4} + \frac{1}{4})v(v) = \frac{1}{2}v(w) \quad (\text{sebab } |u'| \leq \frac{1}{2} \quad \text{dan} \quad |v'| \leq \frac{1}{2}) \\ &\leq v(w) \quad (\text{sebab } 1 \leq v(w)). \end{aligned}$$

●

Perhatikan bahwa dalam definisi Daerah Euclide, hasil bagi q dan sisa r tidak harus tunggal.

Contoh 9.1.3 Dalam Contoh 9.1.1 kita membagi $z = 3 + 2i$ dengan $w = 1 + i$ di $\mathbb{Z}[i]$ dan diperoleh

$$3 + 2i = (2 - i)(1 + i) + i.$$

Kita sebenarnya memiliki tiga pilihan lagi untuk hasil bagi q dan sisa r.

$$\begin{aligned} 3 + 2i &= (3 - i)(1 + i) - 1 \\ 3 + 2i &= (2)(1 + i) + 1 \\ 3 + 2i &= (3)(1 + i) - i. \end{aligned}$$

Dalam keempat kasus, $v(r) = 1 < 2 = v(1 + i) = v(w)$. ●

Konsekuensi langsung dari Definisi 9.1.1 adalah bahwa dalam Daerah Euclidean, setiap ideal adalah ideal utama. Perhatikan bahwa pembuktian yang kita berikan selanjutnya hampir sama dengan pembuktian Teorema 8.6.1, dimana fungsi v adalah derajat.

Teorema 9.1.1 Setiap **Daerah Euclide** (**DE**) adalah **DIU**.

Bukti
Misalkan I adalah sebarang ideal dalam Daerah Euclide D. Jika $I = \{0_D\}$, maka $I = \langle 0_D \rangle$. Jika $I \neq \langle 0_D \rangle$, misalkan $0_D \neq a \in I$ suatu elemen di I sehingga $v(a) < v(x)$ untuk semua $0_D \neq x$ inI. Kita menunjukkan bahwa $I = \langle a \rangle$. Misalkan sebarang $b \in I$. Maka ada q dan r di D sedemikian rupa sehingga $b = qa + r$ dengan $r = 0_D$ atau $v(r) < v(a)$. Karena $r = b - qa$ kita memiliki $r \in I$. Dengan sifat minimal $v(a) < v(x)$, $\forall 0_D \neq x \in I$ kita memperoleh $r = 0_D$ dan $b = qa \in \langle a \rangle$. Jadi $b \in \langle a \rangle$ untuk semua $b \in I$, dengan demikian $I = \langle a \rangle$. ✓

Menentukan apakah suatu daerah integral yang diberikan adalah Daerah Euclide bisa menjadi masalah yang sulit. Tetapi teorema yang baru saja kita buktikan dapat berguna, karena biasanya lebih mudah untuk menunjukkan bahwa suatu daerah integral tertentu **bukan** DIU. Dalam hal ini, kita dapat secara otomatis menyimpulkan bahwa itu bukan Daerah Euclide.

Contoh 9.1.4 Pertimbangkan $\mathbb{Z}[\sqrt{5}i]$ dan untuk setiap $z = a + b\sqrt{5}i$ didefinisikan fungsi $v(z) = z\overline{z} = a^2 + 5b^2$. Misalkan $I = \langle 3, 1 + 2\sqrt{5}i \rangle$, ideal yang dibangun oleh 3 dan $1 + 2\sqrt{5}i$.

(1) Perhatikan bahwa I adalah ideal sejati, sebab jika kita memiliki $1 \in I$ kita akan memiliki

$$1 = 3u + (1 + 2\sqrt{5}i)w, \quad \text{dimana} \quad u, w \in \mathbb{Z}[\sqrt{5}i].$$

Kalikan dua sisi dengan $1 - 2\sqrt{5}i$, kita mempunyai

$$1 - 2\sqrt{5}i = 3(1 - 2\sqrt{5}i)u + 21w.$$

Ini menyiratkan bahwa $(1 - 2\sqrt{5}i)$ adalah kelipatan 3 di $\mathbb{Z}[\sqrt{5}i]$, yang tidak mungkin.

(2) Misalkan I adalah ideal utama dan $I = \langle x + y\sqrt{5}i \rangle$. Maka

$$3 = \alpha(x + y\sqrt{5}i) \quad \text{dan} \quad 1 + 2\sqrt{5}i = \beta(x + y\sqrt{5}i)$$

Tetapi ini menyiratkan bahwa $v(x + y\sqrt{5}i) = x^2 + 5y^2$ adalah pembagi dari

$$v(3) = 9 \quad \text{dan} \quad v(1 + 2\sqrt{5}i) = 21.$$

Oleh karena itu $x^2 + 5y^2 = 1$ atau 3. Tetapi $x^2 + 5y^2 = 3$ tidak memiliki solusi bilangan bulat, dan $x^2 + 5y^2 = 1$ jika dan hanya jika $x = \pm 1$ dan $y = 0$ dalam hal ini $I = \mathbb{Z}[\sqrt{5}i]$, yang bertentangan (1). Oleh karena itu, I bukan ideal utama, dan $\mathbb{Z}[\sqrt{5}i]$ bukan **DIU**. dan karenanya bukan **Daerah Euclide**. ●

Salah satu akibat langsung dari algoritma pembagian di Bab 1 dan di Bab 8 adalah adanya pembagi persekutuan terbesar dan algoritma Euclide. Generalisasi Teorema 1.3.6 dan Teorema 8.2.2 diberikan sekarang untuk sembarang daerah Euclide, tetapi pertama-tama kita memerlukan beberapa definisi.

Definisi 9.1.2 Misalkan R adalah suatu ring komutatif dan misalkan $a, b \in R$ dengan $b \neq 0_R$.

(1) b dikatakan sebagai **pembagi** dari a di R yang ditulis $b \mid a$ jika terdapat $x \in R$ sehingga $a = xb$.

(2) $c \in R$ dikatakan sebagai pembagi persekutuan dari a dan b jika $c \mid a$ dan $c \mid b$. ✓

Definisi 9.1.3 Misalkan R adalah suatu ring komutatif dan misalkan $a, b \in R$. **Pembagi persekutuan terbesar** dari a dan b adalah elemen bukan nol $d \in R$ sedemikian sehingga

(1) d adalah pembagi persekutuan dari a dan b.

(2) Bila c adalah pemebagi persekutuan yang lain dari a dan b, maka $c \mid d$. ✓

Teorema 9.1.2 Misalkan D adalah suatu daerah Euclide dan $a, b \in D$ dua elemen bukan nol di D. Maka ada elemen $d \in D$ sedemikian rupa sehingga

(1) d adalah pembagi persekutuan dari a dan b.

(2) Ada $u, v \in D$ sedemikian hingga $d = ua + vb$.

Bukti
Misal $I = \{xa + yb \mid x, y \in D\}$. Himpunan I adalah ideal dalam D, ideal yang dibangun oleh a dan b. Menurut Teorema 9.1.1, $I = \langle d \rangle$ untuk beberapa $d \in D$. Karena $d \in I$, maka $d = ua + vb$ untuk beberapa $u, v \in D$. Juga, karena $I = \langle d \rangle$, maka setiap elemen di I berbentuk xd untuk beberapa $x \in D$. Karena $a \in I$ kita memperoleh $d \mid a$, juga karena $b \in I$ kita memperoleh $d \mid b$. Jadi d adalah pembagi persekutuan dari a dan b. Selanjutnya, jika c adalah pembagi persekutuan yang lain dari a dan b, maka $c \mid a$ dan $c \mid b$ ini berarti $a = xc$ dan $b = yc$ untuk beberapa $x, y \in D$. Dengan demikian, kita mempunyai $d = ua + vb = uxc + vyc = (ux + vy)c$. Jadi, $c \mid d$ dan pembuktiannya selesai. ✓

Dalam daerah Euclide D kita dapat menggunakan algoritma Euclide seperti pada Bab 1 dan Bab 8 untuk mendapatkan pembagi persekutuan terbesar. Misalkan $a, b \in D$ dengan $b \neq 0_D$. Maka menerapkan algoritma Euclide, kita memiliki

$$\begin{aligned}
a &= q_1 b + r_1 \quad \text{dimana } v(r_1) < v(b), \text{ bila } r_1 \neq 0_D \\
b &= q_2 r_1 + r_2 \quad \text{dimana } v(r_2) < v(r_1), \text{ bila } r_2 \neq 0_D \\
r_1 &= q_3 r_2 + r_3 \quad \text{dimana } v(r_3) < v(r_2), \text{ bila } r_3 \neq 0_D \\
&\vdots \\
r_{k-1} &= q_{k+1} r_k + r_{k+1} \quad \text{dimana } v(r_{k+1}) < v(r_k), \text{ bila } r_k \neq 0_D.
\end{aligned}$$

Karena $v(b) > v(r_1) > v(r_2) > \cdots > v(r_k) > v(r_{k+1} > \cdots \geq 0$ adalah barisan menurun dari bilangan bulat tak negatif, maka untuk beberapa bilangan bulat positip n kita harus memiliki $r_{n+1} = 0$. Oleh karena itu $r_n \mid r_{n-1}$ dan $r_n \mid r_i$ untuk semua $i \leq n$; oleh karena itu $r_n \mid b$ dan $r_n \mid a$. Selain itu, jika $c \mid a$ dan $c \mid b$, maka $c \mid r_i$ untuk semua $i \leq n$, dan karenanya $c \mid r_n$. Jadi r_n adalah pembagi persekutuan terbesar dari a dan b.

Contoh 9.1.5 Dalam kasus polinomial $f(x)$ dan $g(x)$ di $\mathbb{F}[x]$ jika $d(x)$ dan $d'(x)$ keduanya merupakan pembagi persekutuan terbesar dari $f(x)$ dan $g(x)$, maka $d(x) = c(x)d'(x)$, dengan $\deg c(x) = 0$. Oleh karena itu $c(x)$ adalah konstanta bukan nol, dan oleh karena itu merupakan unit dalam $\mathbb{F}[x]$. ●

Proposisi 9.1.2 Misalkan D adalah suatu daerah integral dan misalkan $a, b \in D$. Maka jika d dan d' adalah pembagi persekutuan terbesar dari a dan b di D maka $d = ud'$ untuk beberapa unit $u \in D$.

Bukti
Karena d dan d' adalah pembagi persekutuan terbesar dari a dan b, maka $d \mid d'$ dan $d' \mid d$. Oleh karena itu $d' = vd$ dan $d = ud'$ untuk beberapa u dan v di D. Oleh karena itu, $d = u(vd) = (uv)d$ dan $(1_D - uv)d = 0_D$. Karena $d \neq 0_D$ dan D adalah daerah integral, kita memperoleh $uv = 1_D$, jadi u adalah unit dengan invers v di D. ✓

Definisi 9.1.4 Misalkan R adalah suatu ring komutatif dengan elemen satuan. Dua elemen a dan b di R dikatakan **berasosiasi** jika $a = ub$ untuk beberapa unit $u \in R$. ✓

Proposisi 9.1.2 menyatakan bahwa dua pembagi persekutuan terbesar dari a dan b adalah berasosiasi. Ini dapat digeneralisasikan ke proposisi berikut.

Proposisi 9.1.3 Misalkan D adalah suatu daerah integral dan I ideal utama dalam D. Bila $I = \langle d \rangle = \langle d' \rangle$, maka d dan d' berasosiasi.

Bukti
Jelas bahwa $d \in \langle d' \rangle$ dan $d' \in \langle d \rangle$. Akibatnya, $d = ud'$ dan $d' = vd$ untuk beberapa $u, v \in D$. Oleh karena itu, $d = u(vd) = (uv)d$ dan $(1_D - uv)d = 0_D$. Karena $d \neq 0_D$ dan D adalah daerah integral, kita memperoleh $uv = 1_D$. Jadi u adalah unit dengan invers v di D yang memenuhi $d = ud'$. Dengan demikian d dan d' berasosiasi. ✓

Teorema 9.1.3 Misalkan D adalah suatu daerah Euclide. Maka

(1) $v(1_D) \leq v(a)$ untuk semua $0_D \neq a \in D$.

(2) $v(1_D) = v(a)$ bila dan hanya bila a adalah suatu unit di D.

Bukti
(1) $v(1_D) \leq v(1_D \cdot a) = v(a)$, untuk semua $0_D \neq a \in D$.
(2) Jika a adalah suatu unit di D maka $v(a) \leq v(a \cdot a^{-1}) = v(1_D) \leq v(a)$, maka $v(1_D) = v(a)$. Sebaliknya, jika $v(1_D) = v(a)$, dengan algoritma pembagian terdapat q dan r dalam D sedemikian rupa sehingga $1_D = qa + r$ dengan $r = 0_D$ atau $v(r) < v(a)$. Tetapi, karena $v(a) = v(1_D)$ dan karena dari (1) $v(1_D) < v(r)$, kita tidak dapat memiliki $v(r) < v(a)$, dan harus memiliki $r = 0_D$. Jadi $1_D = qa$ dan a adalah suatu unit di D. ✓

Contoh 9.1.6 Dalam $\mathbb{Z}[i]$, maka $v(z) = a^2 + b^2 = z\bar{z}$, $z = a + bi \in \mathbb{Z}[i]$. sehingga $v(1) = 1$ dan z adalah unit di $\mathbb{Z}[i]$ jika dan hanya jika $v(z) = 1$. Oleh karena itu $1, -1, i, -i$ adalah unit di $\mathbb{Z}[i]$. ●

Latihan

Pada Latihan 1 sampai 3 tunjukkan bahwa daerah integral yang diberikan oleh $\mathbb{Z}[\sqrt{d}]$ adalah daerah Euclide dengan fungsi $v(z) = |z\overline{z}|$, dimana untuk $z = a + b\sqrt{d}, \overline{z} = a - b\sqrt{d}$.
(1) $\mathbb{Z}[\sqrt{2}]$ (2) $\mathbb{Z}[\sqrt{2}i]$ (3) $\mathbb{Z}[\sqrt{3}]$.

Dalam Latihan 4 hingga 7 dapatkan hasil bagi q dan sisa r dalam daerah Euclide yang diberikan, dimana $a = qb + r$
(4) $a = 5 + 3i$ $b = 2 + i$ di $\mathbb{Z}[i]$
(5) $a = 3 + 4i$ $b = 4 - 3i$ di $\mathbb{Z}[i]$
(6) $a = 3 + 2\sqrt{2}$ $b = 1 + \sqrt{2}$ di $\mathbb{Z}[\sqrt{2}]$
(7) $a = 5 + 2\sqrt{2}$ $b = 3 + \sqrt{2}$ di $\mathbb{Z}[\sqrt{2}]$.

Dalam Latihan 8 sampai 11, tentukan pembagi persekutuan terbesar d dari a dan b dalam daerah Euclide yang diberikan, dan nyatakan $d = ua + vb$.
(8) $a = 7 + 5\sqrt{2}$ $b = 1 + \sqrt{2}$ di $\mathbb{Z}[\sqrt{2}]$
(9) $a = -3 + 7\sqrt{3}$ $b = 7 - \sqrt{3}$ di $\mathbb{Z}[\sqrt{3}]$
(10) $a = 2 + 8i$ $b = 6 + 8i$ di $\mathbb{Z}[i]$
(11) $a = 4 + 7i$ $b = 8 - i$ di $\mathbb{Z}[i]$.

Dalam Latihan 12 sampai 14 tentukan generator untuk ideal I dalam daerah Euclide yang diberikan.

(12) I = ideal yang dibangun oleh $f(x) = x^3 + x^2 - 2x - 2$ dan $g(x) = x^3 - x^2 - 2x + 1$ di $\mathbb{Q}[x]$.

(13) I = ideal yang dibangun oleh $5 + 5i$ dan $3 - i$ di $\mathbb{Z}[i]$.

(14) I = ideal yang dibangun oleh 13 dan $3 + 2i$ di $\mathbb{Z}[i]$.

(15) Buktikan atau bantah bahwa $\mathbb{Z}[x]$ adalah daerah Euclidean.

(16) Buktikan atau bantah bahwa untuk sebarang lapangan $\mathbb{F}$, maka $\mathbb{F}[x, y]$ adalah daerah Euclidean.

(17) Misalkan D adalah suatu daerah Euclide dan elemen a dan b di D. Tunjukkan bahwa

(1) Bila a dan b berasosiasi, maka $v(a) = v(b)$.

(2) Bila $v(a) = v(b)$ dan $a \mid b$, maka a dan b berasosiasi.

(18) Misalkan D adalah suatu daerah Euclide dan elemen a dan b bukan nol di D. Tunjukkan bahwa $v(a) < v(ab)$ jika dan hanya jika b bukan merupakan unit di D.

(19) Tunjukkan bahwa $\mathbb{Z}[\sqrt{3}i]$ bukan daerah Euclide. (Gunakan Teorema 9.1.1.)

(20) Misalkan D adalah suatu daerah integral. Tunjukkan bahwa ketiga pernyataan berikut ekuivalen: (a) D suatu lapangan, (b) $D[x]$ suatu daerah Euclide (c) $D[x]$ suatu DIU.

(21) Misalkan D adalah suatu daerah Euclide, a, b dan c elemen bukan nol di D dan d merupakan pembagi persekutuan terbesar dari a dan b. Tunjukkan bahwa jika $a \mid bc$ maka $(a/d) \mid c$.

(22) Misalkan x_0, y_0 dalam $\mathbb{Z}$ adalah solusi dari persamaan $ax + by = c$, dimana $a \neq 0, b \neq 0$, dan c berada di $\mathbb{Z}$. Tunjukkan bahwa himpunan penyelesaian lengkap $x, y \in \mathbb{Z}$ diberikan oleh

$$x = x_0 + k\left(\frac{b}{\text{fpb}(a,b)}\right), \quad y = y_0 - k\left(\frac{a}{\text{fpb}(a,b)}\right),$$

untuk semua nilai $k \in \mathbb{Z}$.

(23) Gunakan latihan sebelumnya untuk menemukan himpunan penyelesaian lengkap dalam $\mathbb{Z}$ dari:
(a) $3x - 6y = 10$ (b) $3x - 6y = 9$ (c) $385x - 275y = 495$.

(24) Misakan R adalah suatu ring komutatif dengan elemen satuan. Untuk $a, b \in R$, suatu **kelipatan persekutuan terkecil** dari a dan b adalah elemen $m \in R$ sedemikian sehingga

(1) $a \mid m$ dan $b \mid m$.

(2) Bila $a \mid n$ dan $b \mid n$, maka $m \mid n$.

Tunjukkan bahwa bila R adalah suatu daerah Euclide, maka

(a) Kelipatan Persekutuan Terkecil m dari a dan b **ada**.

(b) Setiap kelipatan persekutuan dari a dan b berasosiasi.

(c) Jika d adalah pembagi persekutuan terbesar dari a dan b maka $\frac{ab}{d}$ adalah kelipatan persekutuan terkecil dari a dan b.

(d) Ideal $\langle a \rangle \cap \langle b \rangle$ adalah ideal yang dibangun oleh kelipatan persekutuan terkecil dari a dan b.

(25) Misalkan $d \in \mathbb{Z}$ sedemikian rupa sehingga $\sqrt{d} \notin \mathbb{Q}$. Dalam $\mathbb{Z}[\sqrt{d}]$ misalkan

$$v(z) = |z\overline{z}| = |a^2 - db^2|, \text{ dimana } z = a + b\sqrt{d}.$$

(a) (**Persamaan Pell**) Tunjukkan bahwa $a + b\sqrt{d}$ adalah suatu unit di $\mathbb{Z}[\sqrt{d}]$ bila dan hanya bila $a^2 - db^2 = \pm 1$.

(b) Asumsikan bahwa untuk sembarang bilangan rasional x dan y terdapat bilangan bulat n dan m sedemikian rupa sehingga $\left|(x-n)^2 - d(y-m)^2\right| < 1$. Tunjukkan bahwa dalam kasus ini $\mathbb{Z}[\sqrt{d}]$ adalah daerah Euclide dengan $v(a+b\sqrt{d}) = |a^2 - db^2|$.

(26) Dalam $\mathbb{Z}[\sqrt{2}]$ tunjukkan bahwa

(a) $1 + \sqrt{2}$ adalah unit.

(b) $\pm(1 + \sqrt{2})^n$ untuk $n \in \mathbb{Z}$ adalah suatu unit.

(c) $\pm(1 + \sqrt{2})^n$ untuk $n \in \mathbb{Z}$ semuanya adalah unit.

9.2 Daerah Faktorisasi Tunggal

Seperti yang ditunjukkan dalam pengantar bab ini, teorema dasar aritmatika (Teorema 1.3.7) dan teorema faktorisasi tunggal untuk $\mathbb{F}[x]$ (Teorema 8.4.2) masing-masing merupakan konsekuensi dari algoritma pembagian. Pada bagian sebelumnya kita menyebut daerah integral dengan algoritma pembagian sebagai daerah Euclide dan menunjukkan bahwa setiap daerah Euclide adalah **DIU**. Pada bagian ini kita menunjukkan bahwa setiap **DIU** memiliki sifat faktorisasi yang tunggal. Daerah integral dengan sifat ini disebut Daerah Faktorisasi Tunggal (**DFT**). Jadi, dalam bagian ini, kita melengkapi bukti penyertaan kelas-kelas daerah integral berikut:

Daerah Integral $\supset$ **DFT** $\supset$ **DIU** $\supset$ **Daerah Euclide** $\supset$ Lapangan

Kita pertama-tama melihat dua konsep yang dalam pembahasan kita sejauh ini tampaknya bertepatan.

Contoh 9.2.1 Pertimbangkan elemen 3 di $\mathbb{Z}[\sqrt{5}i]$ dan fungsi

$$v(z) = z\overline{z} = a^2 + 5b^2, \text{ dimana } z = a + b\sqrt{5}i.$$

(1) Kita coba memfaktorkan $3 = zw$ di $\mathbb{Z}[\sqrt{5}i]$. Kita harus punya

$$9 = v(3) = v(zw) = zw\,\overline{zw} = zw\,\overline{z}\,\overline{w} = z\overline{z}\,w\overline{w} = v(z)v(w).$$

Bila $z = a + b\sqrt{5}i$, maka $v(z) = a^2 + 5b^2$ harus membagi 9, dan karena $a^2 + 5b^2 = 3$ tidak memiliki solusi bilangan bulat, $v(z)$ harus sama dengan 1 atau 9. Jika $v(z) = 1$, maka z merupakan satuan, sedangkan jika $v(z) = 9$, maka $v(w) = 1$ dan w merupakan satuan. Jadi jika $3 = zw$, salah satu dari z atau w harus berupa unit di $\mathbb{Z}[\sqrt{5}i]$.

(2) Sekarang pertimbangkan $z = 2 + \sqrt{5}i$ dan $w = 2 - \sqrt{5}i$. Di sini 3 tidak membagi z dan tidak membagi w, tetapi 3 membagi $zw = 9$. ●

Definisi 9.2.1 Misalkan D adalah suatu daerah integral dan $a \in D, a \neq 0$, dan a bukan unit dalam D. Maka

(1) Elemen a disebut **tak-tereduksi** di D bilamana $a = xy$, maka salah satu dari x adalah unit atau y adalah unit. Bila tidak demikian, maka a **tereduksi** di D.

(2) Elemen a dinamakan **prima** di D, bila $a \mid xy$ dengan $x, y \in D$, maka salah satu dari $a \mid x$ atau $a \mid y$. ✓

Contoh 9.2.2 Perhatikan kontras dalam contoh berikut.

(1) Dalam $\mathbb{Z}$ dan $\mathbb{F}[x]$ dimana $\mathbb{F}$ adalah suatu lapangan, bilangan **prima** dan elemen **tak tereduksi** adalah pengertian yang sama.

(2) Dalam Contoh 9.2.1 kita tunjukkan bahwa dalam $\mathbb{Z}[\sqrt{5}i]$, elemen 3 tak-tereduksi tetapi bukan prima. ●

Proposisi 9.2.1 Dalam daerah integral D, setiap elemen prima adalah tak-tereduksi.

Bukti
Misalkan D adalah suatu daerah integral dan misalkan p adalah prima di D. Jika $p = xy$ untuk beberapa $x, y \in D$, maka salah satu $p \mid x$ atau $p \mid y$. Katakan $p \mid x$. Maka $x = cp$ untuk beberapa $c \in D$. Maka, kita memiliki $p = xy = (cp)y = (cy)p$. Oleh karena itu, $(1_D - cy)p = 0_D$, dan karena D adalah daerah integral serta $p \neq 0_D$, maka $cy = 1_D$, jadi y adalah unit dalam D. Demikian pula, jika $p \mid y$, maka x adalah unit di D. Jadi p tak-tereduksi. ✓

Dalam suatu daerah integral D suatu elemen p adalah prima jika dan hanya jika ideal utama $I = \langle p \rangle$ yang dibangun oleh p adalah ideal prima dalam D. Dua proposisi berikutnya akan menunjukkan kepada kita bahwa dalam **DIU** dua konsep **tak-tereduksi** dan **prima** adalah pengertian yang sama.

Proposisi 9.2.2 Misalkan D adalah suatu **DIU**. Maka $p \in D$ **tak-tereduksi** jika dan hanya jika ideal utama $I = \langle p \rangle$ yang dibangun oleh p adalah **ideal maksimal** dalam D.

Bukti
($\Leftarrow$) Asumsikan bahwa D adalah **DIU** dan $I = \langle p \rangle$ adalah **ideal maksimal** dalam D. Jika $p = xy \in D$, maka $I = \langle p \rangle \subseteq \langle x \rangle \subseteq D$. Karena I maksimal, $\langle p \rangle = \langle x \rangle$ atau $\langle x \rangle = D = \langle 1_D \rangle$. Jika $\langle p \rangle = \langle x \rangle$, maka menurut Teorema 9.1.3, p dan x adalah berasosiasi, dan y adalah unit. Jika $\langle x \rangle = \langle 1_D \rangle$, maka x dan 1_D adalah berasosiasi, jadi x adalah unit. Oleh karena itu jika $p = xy \in D$, maka x atau y adalah unit, dengan demikian p **tak-tereduksi**.
($\Rightarrow$) Asumsikan bahwa D adalah **DIU** dan p **tak-tereduksi**. Jika J adalah ideal dalam D sehingga $I = \langle p \rangle \subseteq J \subseteq D$ maka karena D adalah **DIU**, $J = \langle q \rangle$ untuk beberapa $q \in D$. Oleh karena itu, $p \in \langle q \rangle$ dan $p = cq$ untuk beberapa $c \in D$. Karena p **tak-tereduksi**, maka salah satu c atau q adalah unit dalam D. Jika c adalah suatu unit, maka p dan q berasosiasi dan berdasarkan Proposisi 9.1.3, maka $I = \langle p \rangle = \langle q \rangle = J$. Jika q adalah suatu unit, maka $1_D \in J$; jadi $J = D$. Dengan demikian $I = \langle p \rangle$ adalah **ideal maksimal**. ✓

Perhatikan bahwa kita membuktikan proposisi sebelumnya dalam kasus khusus dimana $D = \mathbb{F}[x]$ seperti Teorema 8.6.2.

Proposisi 9.2.3 Misalkan D adalah suatu **DIU**. Maka elemen tak-nol p adalah prima di D jika dan hanya jika p tak-tereduksi di D.

Bukti
Sebagai Latihan! ✓

Dalam Contoh 9.1.4 kita menunjukkan bahwa $\mathbb{Z}[\sqrt{5}i]$ bukan **daerah Euclide** dengan menunjukkan bahwa ia bukan **DIU**. Seperti ditunjukkan pada Contoh 9.2.1, $\mathbb{Z}[\sqrt{5}i]$ memuat elemen tak-tereduksi yang bukan prima. Oleh karena itu Proposisi 9.2.3 memberi kita bukti lain dari fakta bahwa **daerah integral** ini bukan **DIU** dan oleh karena itu bukan **daerah Euclide**.

Contoh 9.2.3 Dalam $\mathbb{Z}[\sqrt{5}i]$ pertimbangkan dua faktorisasi dari 21:

$$\begin{aligned} 21 &= 3 \times 7 \\ 21 &= (1 + 2\sqrt{5}i)(1 - 2\sqrt{5}i). \end{aligned}$$

(1) Dalam Contoh 9.2.1 kita tunjukkan bahwa 3 tak-tereduksi dalam $\mathbb{Z}[\sqrt{5}i]$. Demikian pula, 7 tak-tereduksi, karena jika $7 = zw$, dimana $z = a+b\sqrt{5}i$, maka $49 = v(7) = v(z)v(w)$ dan $v(z) = a^2 + 5b^2$. Oleh karena itu $v(z)$ membagi 49, dan karena $a^2 + 5b^2 = 7$ tidak memiliki solusi bilangan bulat, baik untuk $v(z) = 1$ atau $v(z) = 49$, maka $v(w) = 1$, demikian juga untuk salah satu dari z unit atau w unit.

(2) Kita juga dapat menunjukkan bahwa $p = 1 + 2\sqrt{5}i$ dan $q = 1 - 2\sqrt{5}i$ tak-tereduksi. Karena jika $p = zw$, maka $21 = v(p) = v(z)v(w)$ dan $v(z) = a^2 + 5b^2$. Jadi $v(z)$ membagi 21, dan karena $a^2 + 5b^2 = 3$ dan $a^2 + 5b^2 = 7$ tidak memiliki solusi bilangan bulat, maka $v(z) = 1$ atau $v(z) = 21$ dan $v(w) = 1$, begitu juga untuk z unit atau w unit. Juga, karena $v(q) = 2l$, argumen yang sama menunjukkan bahwa q tak tereduksi.

Jadi, kita memiliki satu elemen, yaitu 21 di $\mathbb{Z}[\sqrt{5}i]$ yang dapat difaktorkan menjadi faktor-faktor tak-tereduksi dalam dua cara yang sama sekali berbeda. ●

Definisi 9.2.2 Daerah integral D dikatakan sebagai Daerah Faktorisasi Tunggal (**DFT**) jika dua kondisi berikut terpenuhi:

(1) Setiap elemen tak-nol a di D yang bukan merupakan unit dapat ditulis sebagai hasil perkalian elemen tak-tereduksi p_i di D:

$$a = p_1 p_2 \cdots p_r.$$

(2) Bila

$$a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

dimana p_i dan q_j semuanya tak-tereduksi, maka $r = s$ dan q_j dapat diindeks ulang sehingga p_i dan q_i adalah berasosiasi di D untuk semua $i, 1 \leq i \leq r$. ✓

Contoh 9.2.4 Kita sudah mengetahui beberapa contoh.

(1) Himpunan $\mathbb{Z}$ adalah suatu **DFT** menurut Teorema 1.3.7.

(2) Himpunan $\mathbb{F}[x]$ dimana $\mathbb{F}$ adalah suatu lapangan merupakan **DFT** menurut Teorema 8.4.2.

(3) Himpunan $\mathbb{Z}[\sqrt{5}i]$ bukan suatu **DFT** menurut Contoh 9.2.3. ●

Proposisi 9.2.4 Dalam suatu **DFT**, elemen bukan nol adalah prima jika dan hanya jika tak-tereduksi.

Bukti
Dengan Proposisi 9.2.1 kita hanya perlu menunjukkan bahwa jika p tak-tereduksi di D dimana D adalah **DFT**, maka p adalah elemen prima. Jadi, misalkan $p \in D$ tak-tereduksi di D dan misalkan $p \mid xy$ untuk beberapa $x, y \in D$. Karena D diasumsikan sebagai **DFT**, maka $x = p_1 p_2 \cdots p_r$ dan $y = p_{r+1} p_{r+2} \cdots p_s$, dimana p_i tak-tereduksi di D. Oleh karena itu $xy = p_1 p_2 \cdots p_r p_{r+1} p_{r+2} \cdots p_s$. Karena $p \mid xy$, maka terdapat $c \in D$ sedemikian rupa sehingga $xy = pc$ dan karena D adalah **DFT**, maka $c = q_1 q_2 \cdots q_t$ untuk beberapa q_j tak-tereduksi. Jadi $p_1 p_2 \cdots p_r p_{r+1} p_{r+2} \cdots p_s = p q_1 q_2 \cdots q_t$ dan p harus merupakan asosiasi dari beberapa p_i dengan $1 \leq i \leq s$. Jika $i \leq r$, maka $p \mid x$, dan jika $r < i$ maka $p \mid y$. Jadi p adalah prima. ✓

Akibat 9.2.1 Misalkan D adalah suatu **DFT** dan misalkan $a_1, a_2, \ldots, a_n$ adalah elemen tak-nol di D yang bukan merupakan unit di D. Maka terdapat elemen d dan m di D sedemikian rupa sehingga

(1) d adalah suatu pembagi persekutuan terbesar dari $a_1, a_2, \ldots, a_n$,

(2) m adalah suatu kelipatan persekutuan terkecil dari $a_1, a_2, \ldots, a_n$.

Bukti
Sebagai Latihan!

Kita menyatakan sekarang salah satu teorema utama dari bagian ini. Namum sebelumnya diberikan proposisi berikut.

Proposisi 9.2.5 Misalkan D adalah suatu **DIU** dan

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_k \subseteq I_{k+1} \subseteq \cdots$$

adalah suatu barisan ideal yang menaik di D. Maka ada $m \in \mathbb{N}$ sedemikian hingga $I_m = I_{m+i}$ untuk semua $i \in \mathbb{N}$.

Bukti
Misalkan

$$I = \bigcup_{i=1}^{\infty} I_i,$$

jelas bahwa I adalah suatu ideal dari D. Karena D adalah **DIU**, maka ada beberapa d di I yang memenuhi $I = \langle d \rangle$. Karena $d \in I$, maka d harus terletak di beberapa I_m. Tetapi $I_m \subseteq I = \langle d \rangle \subseteq I_m$ hal ini berakibat $I = I_m$ dan $I_m \subseteq I_{m+i} \subseteq I = I_m$, $i = 1, 2, \ldots$. Jadi $I_m = I_{m+i}$ untuk semua $i \in \mathbb{N}$.

Teorema 9.2.1 Setiap **DIU** adalah suatu **DFT**.

Bukti
Misalkan D adalah suatu **DIU** dan sebarang $a \neq 0_D$ bukan suatu unit di D. Andaikan a tidak mempunyai faktorisasi dari elemen-elemen tak-tereduksi di D, sehingga didapat $a = a_1 b_1$ untuk beberapa $a_1, b_1 \in D$ dengan a_1 dan b_1 bukan unit. Setidaknya satu dari a_1 atau b_1 harus tidak mempunyai suatu faktor kalau tidak faktorisasi a_1 dan b_1 secara bersama akan menghasilkan suatu faktorisasi dari a. Misalkan dalam hal ini a_1 tidak mempunyai suatu faktorisasi. Jadi a dan a_1 tidak berasosiasi. Sehingga didapat $\langle a \rangle \subset \langle a_1 \rangle$. Karena a_1 tidak mempunyai suatu faktorisasi, maka $a_1 = a_2 b_2$ untuk beberapa $a_2, b_2 \in D$ dengan a_2 dan b_2 bukan unit. Dalam hal ini a_2 atau b_2 harus tidak mempunyai suatu faktor kalau tidak faktorisasi a_2 dan b_2 secara bersama akan menghasilkan suatu faktorisasi dari a_1. Misalkan a_2 tidak mempunyai suatu faktorisasi. Maka didapat $\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle$. Proses lakukan berulang pada a_2 Sehingga didapat suatu barisan tak-berhingga rantai menaik dari ideal utama di D

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \cdots \subset \langle a_m \rangle \subset \langle a_{m+1} \rangle \subset \cdots$$

Hal ini bertentangan dengan kenyataan Sifat Barisan Ideal menaik di DIU yang berhenti pada suatu yang berhingga (Proposisi 9.2.5) yaitu ada $m \in \mathbb{N}$ sehingga $\langle a_m \rangle = \langle a_{m+i} \rangle$, $i \in \mathbb{N}$. Jadi

haruslah sebarang elemen $a \neq 0_D$ bukan suatu unit di D dapat difaktorkan menjadi faktorisi elemen-elemen tak-tereduksi. Tinggal menunjukkan bahwa faktorisasi dari a adalah tunggal. Misalkan

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$$

adalah dua faktorisasi tak-tereduksi dari a. Maka

$$p_1 p_2 \cdots p_n = q_1(q_2 \cdots q_m).$$

Sehingga didapat

$$q_1 | p_1 p_2 \cdots p_n.$$

Karena q_1 dan p_i tak-tereduksi, maka setidaknya satu dari $p_1, p_2, \ldots, p_n$ dapat dibagi oleh q_1. Misalkan dalam hal ini $q_1|p_1$ dan karena q_1 dan p_1 keduanya tak-tereduksi, maka p_1 berasosiasi dengan q_1. Sehingga didapat $p_1 = u_1 q_1$ dengan u_1 adalah unit dan

$$u_1 q_1(p_2 \cdots p_n) = q_1(q_2 \cdots q_m).$$

Lakukan kanselasi pada kedua ruas persamaan didapat

$$u_1(p_2 \cdots p_n) = q_2(q_3) \cdots q_m).$$

Selanjutnya $q_2|u_1(p_2 \cdots p_n)$, dengan argumentasi yang sama didapat $p_2 = u_2 q_2$ dimana u_2 adalah unit di D. Sehingga didapat

$$u_1 u_2 q_2(p_3 \cdots p_n) = q_2(q_3) \cdots q_m).$$

Lakukan kanselasi pada kedua ruas persamaan didapat

$$u_1 u_2(p_3 \cdots p_n) = q_3(q_4 \cdots q_m).$$

Bila $n > m$, lakukan sebagaimana proses sebelumnya sehingga didapat

$$u_1 u_2 \cdots u_m(p_{m+1} \cdots p_n) = 1,$$

hal ini berakibat masing-masing $p_{m+1}, \ldots, p_n$ adalah unit. Bertentangan dengan kenyataan $p_i,\ i = 1, 2, \ldots, n$ adalah bukan unit. Selanjutnya bila $n < m$ didapat

$$u_1 u_2 \cdots u_n = q_{n+1} \cdots q_m. \tag{9.2}$$

Selanjutnya pilih elemen unit $v_i \in D$ yang memenuhi $v_i u_i = 1,\ i = 1, 2, \ldots, n$ dan kalikan $v_i,\ i = 1, 2, \ldots, n$ pada kedua ruas Persamaan 9.2 sehingga didapat

$$1 = (v_1 v_2 \cdots v_n)(q_{n+1} \cdots q_m),$$

hal ini berakibat masing-masing $q_{n+1}, \ldots, q_m$ adalah unit. Bertentangan dengan kenyataan $q_i, i = 1, 2, \ldots, m$ adalah bukan unit. Dengan demikian $m = n$. Sehingga didapat pemfaktoran sebarang $a \neq 0_D$ bukan suatu unit di D diberikan oleh

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_n$$

dengan megurutkan indeks dari p_i atau q_i bila perlu dan karena p_i dan q_i masing-masing adalah tak-tereduksi maka didapat $p_i = u_i q_i,\ i = 1, 2, \ldots, n$ dengan u_i adalah suatu unit di D. Jadi p_i berasosiasi dengan q_i, untuk $i = 1, 2, \ldots, n$. Dengan demikian faktorisasi dari a adalah tunggal. Jadi D adalah **DFT**.

Kita mengakhiri bagian ini dengan teorema yang sangat penting: "Jika D adalah **DFT**, maka $D[x]$ adalah **DFT**." Kita membuktikan dalam bab sebelumnya kasus khusus dimana $D = \mathbb{F}$ suatu lapangan (Teorema 8.4.2). Untuk kasus umum dimana D adalah sebarang **DFT**, kita mulai dengan mencatat bahwa karena $f(x) \in D[x] \subseteq Q[x]$ dapat dilihat sebagai elemen dari $Q[x]$ dimana Q adalah lapangan pecahan dari D menurut Teorema 8.4.2 $f(x)$ memiliki faktorisasi tunggal menjadi faktor-faktor tak-tereduksi di $Q[x]$. Bagian yang sulit dari pembuktian adalah untuk menunjukkan bahwa ini akan memberikan faktorisasi tunggal menjadi faktor-faktor tak-tereduksi di $D[x]$. Untuk ini kita memerlukan beberapa definisi dan lemma, yang kita telah bahas di Bab 8 untuk kasus khusus $D = \mathbb{Z}$. Beberapa bukti dibiarkan sebagai latihan dengan mengacu pada bukti kasus khusus pada bab sebelumnya.

Definisi 9.2.3 Misalkan D adalah suatu **DFT** dan $f(x) \in D[x]$ polinomial tak konstan. Maka $f(x)$ dikatakan **primitif** di $D[x]$ jika 1_D adalah **fpb** dari semua koefisien $f(x)$.

Contoh 9.2.5 Mari kita jelaskan semua elemen tak-tereduksi dalam $\mathbb{Z}[x]$. Pertama perhatikan bahwa $f(x) = 2x^3 - 10 = 2(x^3 - 5)$ tak-tereduksi di $\mathbb{Z}[x]$ karena 2 bukan merupakan unit dalam $\mathbb{Z}[x]$. Unit di $\mathbb{Z}[x]$ menurut Proposisi 8.1.1 adalah polinomial konstan 1 dan -1. Jika $\deg g(x) = 0$ dan $g(x)$ tak-tereduksi di $\mathbb{Z}[x]$ maka $g(x) = p$ dimana p adalah bilangan prima di $\mathbb{Z}$. Sebaliknya, jika $\deg g(x) > 0$ dan polinomial $g(x)$ tak-tereduksi di $\mathbb{Z}[x]$ maka $g(x)$ harus primitif, karena jika **fpb** dari koefisien $g(x)$ di $\mathbb{Z}$ adalah $c \neq 0$, maka membagi dengan c kita memperoleh $g(x) = ch(x)$ dimana baik c maupun $h(x)$ adalah bukan unit di $\mathbb{Z}[x]$.

Lemma 9.2.1 Misalkan D adalah suatu **DFT** dan $f(x) \in D[x]$ polinomial tak konstan. Maka ada elemen $c \in D$, dan polinomial primitif $g(x) \in D[x]$ sedemikian rupa sehingga $f(x) = cg(x)$. Di sini c dan $g(x)$ tunggal dalam arti mereka berasosiasi dengan masing-masing elemen yang terkait; yaitu jika $f(x) = dh(x)$ dimana $d \in D$ dan $h(x) \in D[x]$ adalah primitif, maka d dan c adalah berasosiasi di D dan $g(x)$ dan $h(x)$ adalah berasosiasi di $D[x]$

Bukti
Dimulai dengan $f(x) = cg(x)$, dimana c adalah **fpb** dari semua koefisien $f(x)$ di D, pembuktian dapat diselesaikan dengan menunjukkan bahwa $g(x)$ primitif dan tunggal dalam arti berasosiasi dengan suatu elemen terkait.

Perhatikan bahwa gagasan tentang **polinomial primitif** **sangat penting** dalam kasus dimana daerah koefisien D bukan suatu lapangan. Karena, dalam kasus lapangan, semua koefisien bukan nol adalah unit.

Lemma 9.2.2 ***(Lemma Gauss)*** Misalkan D adalah suatu **DFT** dan misalkan $f(x)$ dan $g(x)$ adalah polinomial primitif di $D[x]$. Maka $f(x)g(x)$ juga merupakan polinomial primitif.

Bukti
Misalkan $f(x)g(x)$ bukan primitif. Maka dengan Lemma 9.2.1, $f(x)g(x) = ck(x)$ dimana c bukan merupakan unit di D. Jadi, misalkan p suatu elemen prima di D yang membagi c. Ideal $I = \langle p \rangle$ adalah ideal prima di D, maka $D_p = D/\langle p \rangle$ adalah daerah integral, dan $D_p[x]$ juga merupakan daerah integral (dengan Teorema 8.1.1 (4)). Misalkan $\phi : D \to D_p$ adalah suatu homomorpisma alami (***natural***), dan $\phi^* : D[x] \to D_p[x]$ adalah suatu homomorpisma induksi (seperti pada Bagian 8.1). Pembuktian sekarang dapat diselesaikan dengan mengikuti pembuktian **Lemma Gauss** untuk $\mathbb{Z}$ (Lemma 8.4.1).

Sekarang kita memiliki semua alat yang kita butuhkan untuk pembuktian generalisasi Teorema 8.4.5.

Teorema 9.2.2 Misalkan D adalah suatu **DFT**, Q lapangan pecahan dari D, dan misalkan polinomial $f(x) \in D[x]$. Maka $f(x)$ dapat difaktorkan ke dalam hasil perkalian polinomial derajat r dan s di $Q[x]$ jika dan hanya jika $f(x)$ dapat difaktorkan ke dalam perkalian polinomial derajat r dan s di $D[x]$.

Bukti
Pembuktian dapat dilakukan dengan mengikuti langkah-langkah pembuktian Teorema 8.4.5, menggunakan Lemma 9.2.1 dan generalisasi lemma Gauss, Lemma 9.2.2. ✓

Akibat 9.2.2 Misalkan D adalah suatu **DFT** dan Q suatu lapangan pecahan dari D, dan $f(x) \in D[x]$ polinomial tak-konstan. Jika $f(x)$ tak-tereduksi di $D[x]$, maka $f(x)$ tak-tereduksi di $Q[x]$.

Bukti
Ini mengikuti langsung dari Teorema 9.2.2. ✓

Teorema 9.2.3 Bila D adalah suatu **DFT**, maka $D[x]$ adalah suatu **DFT**.

Bukti
Misalkan $f(x) \in D[x]$ adalah suatu polinomial bukan nol yang bukan merupakan unit di $D[x]$. Jika deg $f(x) = 0$, maka $f(x) = c$ suatu polinomial konstan, di mana $c \in D$ bukan merupakan unit di D. Dalam hal ini, karena D adalah suatu **DFT**, maka $f(x) = c$ dapat difaktorkan secara tunggal kecuali untuk urutan dan perkalian dengan unit, menjadi hasil perkalian

$$f(x) = p_1 p_2 \cdots p_s \in D,$$

dimana p_i adalah elemen di D yang tak-tereduksi, atau polinomial yang ekivalen dengan derajat 0 di $D[x]$ dengan demikian teorema terbukti.

Sekarang misalkan deg $f(x) > 0$. Misalkan Q adalah suatu lapangan pecahan dari D. Karena deg $f(x) > 0$, maka $f(x)$ bukan merupakan unit di $Q[x]$ dan dengan Teorema 8.4.2 kita dapatkan

$$f(x) = p_1(x)p_2(x)\cdots p_s \in Q[x],$$

dimana $p_i(x)$ tak-tereduksi di $Q[x]$. Koefisien dari setiap $p_i(x)$ berbentuk ed^{-1}, di mana $e, d \in D$. Misalkan $d_i \in D$ merupakan kelipatan persekutuan terkecil dari semua penyebut d dari koefisien ed^{-1} dari polinomial $p_i(x)$, misalkan d adalah hasil kali semua d_i dan misalkan $q_i(x) = d_i p_i(x)$. Maka kita mempunyai

$$df(x) = q_1(x)\cdots q_s(x) \in D[x],$$

dimana $q_i(x) \in D[x]$. Karena d_i adalah unit di Q dan $p_i(x)$ tak-tereduksi di $Q[x]$, maka $q_i(x)$ masih tak-tereduksi di $Q[x]$. Menurut Lemma 9.2.1, kita mempunyai $f(x) = cg(x)$ dimana $c \in D$ dan $g(x) \in D[x]$ adalah primitif. Demikian pula, setiap $q_i(x) = c_i h_i(x)$, dimana $c_i \in D$ dan $h_i(x) \in D[x]$ adalah primitif. Jadi kita mempunyai

$$dcg(x) = (c_1 \cdots c_s)h_i(x)\cdots h_s(x) \in D[x].$$

Karena c_i adalah unit di Q, dan $q_i(x)$ tak-tereduksi di $Q[x]$, maka $h_i(x)$ masih tak-tereduksi di $Q[x]$. Dengan pernyataan ketunggalan di Lemma 9.2.1, maka dc dan $c_1 \cdots c_s$ berasosiasi di D. Jadi ada unit $u \in D$ sedemikian sehingga

$$df(x) = dcg(x) = (dcu)(h_1(x) \cdots h_s(x)) \Rightarrow f(x) = (cu)(h_1(x) \cdots h_s(x)),$$

di mana $h_i(x)$ primitif di $D[x]$ dan tak-tereduksi di $Q[x]$ maka juga tak-tereduksi di $D[x]$. Karena D adalah **DFT**, maka cu dapat ditulis sebagai perkalian elemen prima $a_1, \ldots, a_r$ di D. Jadi kita memiliki eksistensi faktorisasi $f(x)$ sebagai hasil perkalian dari polinomial tak-tereduksi di $D[x]$

$$f(x) = a_1 \cdots a_r h_1(x) \cdots h_s(x),$$

dimana a_j tak-tereduksi di D dan $h_i(x)$ primitif dan tak-tereduksi di $D[x]$ dan karenanya juga tak-tereduksi di $Q[x]$.

Yang tersisa untuk ditunjukkan adalah ketunggalan. Misalkan

$$f(x) = b_1 \cdots b_{r'} k_1(x) \cdots k_{s'}(x),$$

dimana b_j tak-tereduksi di D dan $k_i(x)$ primitif juga tak-tereduksi di $D[x]$ dan karenanya tak-tereduksi di $Q[x]$ oleh Akibat 9.2.2. Kita ingin menunjukkan bahwa $r' = r, s' = s$ dan bahwa penataan ulang jika perlu, a_j dan b_j adalah berasosiasi di D dan $h_i(x)$ dan $k_i(x)$ adalah berasosiasi di $D[x]$.

Perhatikan terlebih dahulu bahwa dalam Q elemen a_j dan b_j adalah unit. Maka mengikuti dari fakta bahwa $Q[x]$ adalah **DFT** jadi $s = s'$ dan bahwa penyusunan ulang jika perlu, $h_i(x)$ dan $k_i(x)$ adalah berasosiasi di $Q[x]$, katakan $k_i(x) = v_i w_i^{-1} h_i(x)$ dan karenanya $w_i k_i(x) = v_i h_i(x)$ untuk beberapa $v_i, w_i \in D$. Perhatikan sekarang bahwa jika kita memisalkan v dan w masing-masing adalah hasil perkalian dari v_i dan w_i, juga $h(x)$ dan $k(x)$ masing-masing adalah hasil perkalian dari $h_i(x)$ dan $k_i(x)$, maka menurut Lemma Gauss 9.2.2 $wk(x) = vh(x)$ dan karena $h(x)$ dan $k(x)$ primitif. Selanjutnya, berdasarkan Lemma 9.2.1 kita mempunyai v dan w adalah berasosiasi di D, misalkan $w = uv$ di mana u adalah unit di D. Dengan demikian, Kita memiliki

$$a_1 \cdots a_r uvk(x) = a_1 \cdots a_r wk(x) = a_1 \cdots a_r vh(x) = vf(x) = b_1 \cdots b_{r'} vk(x) \Rightarrow ua_1 \cdots a_r = b_1 \cdots b_{r'}$$

dimana u adalah suatu unit di D. Karena D adalah suatu **DFT**, maka $r = r'$ dan jika perlu menyusun ulang, maka a_j dan b_j berasosiasi. ✓

Contoh 9.2.6 Himpunan $\mathbb{Z}$ adalah **DFT**, oleh karena itu, $\mathbb{Z}[x]$ adalah **DFT**. Kita telah menunjukkan (dalam Contoh 8.6.5) bahwa $\mathbb{Z}[x]$ bukan **DIU**, jadi kita sekarang memiliki contoh suatu **DFT** yang bukan suatu **DIU**. ●

Contoh 9.2.7 Himpunan $\mathbb{F}[x]$ adalah **DFT**, dimana $\mathbb{F}$ adalah suatu lapangan oleh karena itu, $\mathbb{F}[x, y] = \mathbb{F}[x][y]$ adalah suatu **DFT**. Kita telah menunjukkan (dalam Contoh 8.6.4) bahwa $\mathbb{F}[x, y]$ bukan **DIU**, jadi ini adalah contoh lain suatu **DFT** yang bukan suatu **DIU**. ●

Latihan

1. Tentukan semua unit dari daerah yang diberikan:
(a) $\mathbb{Z}[\sqrt{2}i]$ (b) $\mathbb{Z}_7[x]$ (c) $\mathbb{Z}[i][x]$ (d) $\mathbb{C}[x]$.

Dalam Latihan 2 sampai 6 tentukan apakah pasangan elemen yang ditunjukkan adalah berasosiasi di daerah yang diberikan.

2. 1 dan $2+\sqrt{3}$ di $\mathbb{Z}[\sqrt{3}]$
3. $5x-10$ dan $x-2$ di $\mathbb{Z}[x]$
4. $3+2\sqrt{2}$ dan $1-\sqrt{2}$ di $\mathbb{Z}[\sqrt{2}]$
5. $5x^2+x+3$ dan x^3+3x+2 di $\mathbb{Z}_7[x]$
6. $1+\sqrt{5}i$ dan $1-\sqrt{5}i$ di $\mathbb{Z}[\sqrt{5}i]$.

Dalam Latihan 7 sampai 10, tentukan apakah elemen yang ditunjukkan adalah prima di daerah yang ditunjukkan. Jika tidak, tentukan apakah mereka tak-tereduksi di daerah yang ditunjukkan.

7. $6x-21$ di $\mathbb{Z}[x]$ di $\mathbb{Q}[x]$ di $\mathbb{Z}_7[x]$
8. 5 di $\mathbb{Z}[\sqrt{5}i]$ di $\mathbb{Z}$ di $\mathbb{Q}$
9. 11 di $\mathbb{Z}[\sqrt{3}]$ di $\mathbb{Z}$ di $\mathbb{R}$
10. 19 di $\mathbb{Z}[\sqrt{3}i]$ di $\mathbb{Z}[\sqrt{2}i]$ di $\mathbb{C}$.

Dalam Latihan 11 sampai 16 tentukan apakah daerah integral yang ditunjukkan adalah **DFT** atau bukan.

11. $\mathbb{Z}_3[x]$ **12.** $\mathbb{Z}[x,y]$ **13.** $\mathbb{Z}[i]$
14. $\mathbb{Z}[\sqrt{2}]$ **15.** $\mathbb{Z}[\sqrt{2}i]$ **16.** $\mathbb{Z}[\sqrt{3}i]$.

17. Tunjukkan bahwa dalam daerah integral D, elemen bukan nol $p \in D$ adalah prima jika dan hanya jika $\langle p \rangle$ adalah ideal prima dalam D.

18. Misalkan D adalah suatu **DIU**. Tunjukkan bahwa elemen bukan nol $p \in D$ tak-tereduksi di D jika dan hanya jika p prima di D.

19. Apakah Proposisi 9.2.2 berlaku jika kondisi "Misalkan D adalah suatu **DIU**" diganti dengan "Misalkan D adalah suatu **DFT**"? Jika ya, berikan bukti; jika tidak, berikan contoh penyangkalnya.

20. Misalkan D adalah suatu **DIU**, p elemen tak-tereduksi di D, dan elemen $b_1, \ldots, b_r$ di D sedemikian rupa sehingga p membagi hasil perkalian $b_1 \cdots b_r$. Tunjukkan bahwa p membagi b_i untuk beberapa $1 \leq i \leq r$.

21. Buktikan Akibat 9.2.1, bagian (1).

22. Buktikan Akibat 9.2.1, bagian (2).

23. Misalkan a dan b adalah elemen di **DFT**. Tunjukkan bahwa jika c adalah **fpb** dari a dan b; dan d adalah **kpk** dari a dan b maka cd dan ab adalah berasosiasi.

24. Buktikan Lemma 9.2.1.

25. Lengkapi bukti generalisasi lemma Gauss, Lemma 9.2.2.

26. Lengkapi bukti Teorema 9.2.2.

27. Buktikan Akibat 9.2.2.

9.3 Bilangan Bulat Gaussian

Daerah Euclide pertama yang kita temui setelah ring bilangan himpunan bilangan bulat $\mathbb{Z}$ dan ring polinomial $\mathbb{F}[x]$ atas suatu lapangan $\mathbb{F}$ adalah $\mathbb{Z}[i]$, ring bilangan bulat Gaussian. Suatu studi lebih lanjut dari ring penting secara historis ini mengungkapkan hubungan yang sangat menarik dengan teori bilangan. Lebih konkretnya, karakterisasi elemen prima di $\mathbb{Z}[i]$ memberi kita bukti teorema Fermat yang sangat nontrivial.

Seperti yang ditunjukkan dalam Proposisi 9.1.1, $\mathbb{Z}[i]$ adalah daerah Euclide dengan fungsi

$$v(z) = z\bar{z} = a^2 + b^2 \quad \text{untuk } z = a + bi \in \mathbb{Z}[i].$$

Oleh karena itu, $\mathbb{Z}[i]$ adalah **DIU** dan karenanya merupakan **DFT** (menurut Teorema 9.1.1 dan 9.2.1). Akibatnya, menurut Proposisi 9.2.4 elemen **prima** dan elemen **tak-tereduksi** di $\mathbb{Z}[i]$ merupakan pengertian yang sama. Berdasarkan Teorema 9.1.3, $z \in \mathbb{Z}[i]$ adalah suatu unit jika dan hanya jika $v(z) = v(1) = 1$. Oleh karena itu hanyalah $1, -1, i$, dan $-i$ yang merupakan unit di $\mathbb{Z}[i]$.

Contoh 9.3.1 Pertimbangkan 5 sebagai elemen di $\mathbb{Z}[i]$. Kita dapat dengan mudah melihat bahwa 5 bukan bilangan prima di $\mathbb{Z}[i]$, karena $5 = (1+2i)(l-2i)$. Tetapi pertimbangkan $1+2i$. Jika $1 + 2i = (a + bi)(c + di)$ maka $5 = v(1 + 2i) = (a^2 + b^2)(c^2 + d^2)$ yang menyiratkan bahwa $a^2 + b^2 = 1$ atau $c^2 + d^2 = 1$, dan karenanya $a + bi$ atau $c + di$ adalah unit dalam $\mathbb{Z}[i]$. Dengan kata lain, $1 + 2i$ adalah bilangan prima dalam $\mathbb{Z}[i]$, dan demikian pula $1 - 2i$.

Proposisi 9.3.1 Misalkan $z = a + bi \in \mathbb{Z}[i]$ sedemikian rupa sehingga $v(z) = a^2 + b^2$ adalah bilangan prima di $\mathbb{Z}$. Maka $z = a + bi$ adalah elemen prima di $\mathbb{Z}[i]$.

Bukti
Misalkan $z = x + yi$ adalah suatu elemen di $\mathbb{Z}[i]$ sedemikian rupa sehingga $v(z) = x^2 + y^2 = p$ adalah bilangan prima di $\mathbb{Z}$. Jika
(1) $z = (a + bi)(c + di)$ di $\mathbb{Z}[i]$
maka
(2) $p = v(z) = (a^2 + b^2)(c^2 + d^2)$ di $\mathbb{Z}$.
Jadi karena p prima di $\mathbb{Z}$, salah satu faktor dalam (2) harus 1, yang menyiratkan bahwa salah satu faktor dalam (1) harus berupa unit. Ini menunjukkan bahwa z tak-tereduksi dan karenanya prima di $\mathbb{Z}[i]$ (Proposisi 9.2.4)·

Akibat 9.3.1 Jika p adalah bilangan prima di $\mathbb{Z}$ yang dapat ditulis sebagai jumlah dari dua kuadrat $p = a^2 + b^2$ maka $a + bi$ adalah elemen prima di $\mathbb{Z}[i]$.

Bukti
Langsung dari Proposisi sebelumnya.

Apa yang baru saja kita tunjukkan tentang elemen prima di $\mathbb{Z}[i]$ dapat digunakan untuk membuktikan teorema Fermat dalam teori bilangan tentang karakterisasi bilangan prima di $\mathbb{Z}$ yang dapat ditulis sebagai jumlah dari dua kuadrat. Diberikan bilangan prima ganjil $p \in \mathbb{Z}$,

maka salah satu dari $p \equiv 1 \mod 4$ atau $p \equiv 3 \mod 4$. Teorema Fermat dapat dinyatakan sebagai berikut.

Teorema 9.3.1 *(Teorema Fermat tentang jumlah kuadrat)* Suatu bilangan prima ganjil p di $\mathbb{Z}$ dapat ditulis sebagai jumlah dari dua kuadrat $p = a^2 + b^2$ jika dan hanya jika $p \equiv 1 \mod 4$.

Bukti
Misalkan p adalah suatu bilangan prima ganjil di $\mathbb{Z}$.
($\Rightarrow$) Misalkan $p = a^2 + b^2$. Sekarang untuk sembarang bilangan bulat a dan b di $\mathbb{Z}$, a^2 dan b^2 masing-masing kongruen dengan salah satu dari $0 \mod 4$ atau $1 \mod 4$. Karena p ganjil, maka a^2 dan b^2 tidak dapat keduanya kongruen dengan 0 atau keduanya kongruen dengan 1 modulo 4. Oleh karena itu mereka kongruen dengan $0 \mod 4$ dan yang lainnya dengan 1 mod 4. Jadi p kongruen dengan $1 \mod 4$.
($\Leftarrow$) Asumsikan $p \equiv 1 \mod 4$. Pertimbangkan grup perkalian $\mathbb{Z}_p^*$, yang merupakan grup siklik dengan order $p - 1$. Karena 4 membagi $p - 1$, terdapat elemen $x \in \mathbb{Z}_p^*$ dengan order $|x| = 4$ dan $|x^2| = 2$. Oleh karena itu $x^2 = -1$ di $\mathbb{Z}_p$ dan $x^2 + 1 = 0$ di $\mathbb{Z}_p$. Dengan kata lain, $p \mid x^2 + 1$. Sekarang pertimbangkan $x^2 + 1 = (x + i)(x - i)$ di $\mathbb{Z}[i]$. Jika p prima di $\mathbb{Z}[i]$, itu akan membagi salah satu dari dua faktor, misalnya $x + i$. Dalam hal ini kita akan memiliki $x + i = p(a + bi)$ di $\mathbb{Z}[i]$. Tetapi ini akan menyiratkan $pb = 1$ di $\mathbb{Z}$, yang tidak mungkin. Oleh karena itu p bukan bilangan prima di $\mathbb{Z}[i]$, dan $p = (a + bi)(c + di)$ di $\mathbb{Z}[i]$, di mana tidak ada faktor yang merupakan suatu unit. Oleh karena itu, $p^2 = v(p) = (a^2 + b^2)(c^2 + d^2)$, di mana tidak ada faktor sama dengan 1, dan karenanya masing-masing harus p. Oleh karena itu $p = a^2 + b^2$ dan p adalah jumlah dari dua kuadrat yang diinginkan. ✓

Akibat 9.3.2 Jika p adalah bilangan prima di $\mathbb{Z}$ dengan $p \equiv 3 \mod 4$, maka p adalah elemen prima di $\mathbb{Z}[i]$.

Bukti
Misalkan p adalah suatu bilangan prima di $\mathbb{Z}$ dengan $p \equiv 3 \mod 4$. Jika
(1) $p = (a + bi)(c + di)$ di $\mathbb{Z}[i]$,
maka
(2) $p^2 = v(p) = (a^2 + b^2)(c^2 + d^2)$ di $\mathbb{Z}$.
Menurut Teorema 9.3.1, p bukan jumlah dari dua kuadrat (sebab $p \equiv 3 \mod 4$). Maka tidak ada faktor dalam (2) yang bisa sama dengan p. Oleh karena itu, satu faktor harus sama dengan 1. Berdasarkan Teorema 9.1.3 bagian (2), maka satu faktor dalam (1) harus merupakan suatu unit. Ini menunjukkan bahwa p tak-tereduksi dan berdasarkan Proposisi 9.2.4 maka p adalah elemen prima di $\mathbb{Z}[i]$. ✓

Kita sekarang dapat melengkapi karakterisasi elemen prima di $\mathbb{Z}[i]$.

Lemma 9.3.1 Misalkan $a + bi$ adalah suatu elemen prima di $\mathbb{Z}[i]$. Maka $a - bi$ adalah suatu elemen prima di $\mathbb{Z}[i]$·

Bukti
Jika $a - bi = xy$ adalah faktorisasi tak-trivial dari $a - bi$ di $\mathbb{Z}[i]$, maka

$$a + bi = \overline{xy} = \overline{x}\,\overline{y}$$

akan menjadi faktorisasi tak-trivial dari $a + bi$. ✓

Lemma 9.3.2 Misalkan $a + bi$ adalah suatu elemen prima di $\mathbb{Z}[i]$ dengan $a \neq 0$ dan $b \neq 0$. Maka $a^2 + b^2$ adalah bilangan prima di $\mathbb{Z}$.

Bukti
Pertama perhatikan bahwa jika elemen prima $z = a+bi$ membagi bilangan bulat m katakanlah, $zw = m$ maka

$$m = \overline{m} = \overline{zw} = \overline{z}\,\overline{w} \in \mathbb{Z}[i]$$

dan $\overline{z} = a - bi$, yang oleh lemma sebelumnya juga prima, juga membagi m. Sekarang karena $a \neq 0$ dan $b \neq 0$, maka z dan $\overline{z}$ dapat berasosiasi hanya jika $a = \pm b$ dalam hal ini $a + bi = a(1 \pm i)$ dapat menjadi prima hanya jika $a = \pm 1$, dalam hal ini $a^2 + b^2 = 2$, yang merupakan bilangan prima di $\mathbb{Z}$. Jika elemen prima $a + bi$ dan $a - bi$ tak-berasosiasi, karena masing-masing membagi m, maka hasil perkaliannya $a^2 + b^2$ juga harus membagi m. Ini berarti tidak mungkin ada faktorisasi tak-trivial $a^2 + b^2 = mn$ di $\mathbb{Z}$ atau, dengan kata lain, $a^2 + b^2$ adalah bilangan prima di $\mathbb{Z}$. ✓

Proposisi 9.3.2 Semua elemen prima dalam himpunan bilangan bulat Gaussian $\mathbb{Z}[i]$ adalah elemen-elemen berikut dan asosiasinya:

(1) $1 + i$ dan $1 - i$,

(2) p bilangan prima di $\mathbb{Z}$ dengan $p \equiv 3 \mod 4$

(3) $a + bi$ dan $a - bi$ dengan $(a + bi)(a - bi) = a^2 + b^2 = p$, dimana p adalah bilangan prima di $\mathbb{Z}$ dan $p \equiv 1 \mod 4$.

Bukti

(1) Karena $v(1 \pm i) = 2$ adalah bilangan prima di $\mathbb{Z}$, maka menurut Proposisi 9.3.2 $1 \pm i$ adalah elemen prima di $\mathbb{Z}[i]$.

(2) Jika p adalah bilangan prima di $\mathbb{Z}$ dengan $p \equiv 3 \mod 4$, maka berdasarkan Kesimpula 9.3.2, p adalah elemen prima di $\mathbb{Z}[i]$.

(3) Jika p adalah bilangan prima di $\mathbb{Z}$ dengan $p \equiv 1 \mod 4$ dan $p = a^2 + b^2$ sesuai dengan Teorema 9.3.1, maka menurut Akibat 9.3.1 $a \pm bi$ adalah elemen prima di $\mathbb{Z}[i]$.

Ini menunjukkan bahwa semua bilangan di (1) sampai (3) adalah elemen prima di $\mathbb{Z}[i]$, serta asosiasinya.

Sekarang sebaliknya misalkan $z = a + bi$ adalah elemen prima di $\mathbb{Z}[i]$. Jika $b = 0$, maka z adalah bilangan bulat dan harus prima di $\mathbb{Z}$ seperti pada (2). Jika $a = 0$, maka iz juga prima di $\mathbb{Z}[i]$ dan berasosiasi dengan z; dan iz adalah bilangan bulat oleh karena itu harus prima di $\mathbb{Z}$ seperti pada (2), dan z akan berasosiasi dengan bilangan prima tsb. Jika $a \neq 0$ dan $b \neq 0$, maka dengan Lemma 9.3.2, $a^2 + b^2$ adalah prima di $\mathbb{Z}$. Jika $a^2 + b^2 = 2$, maka $a + bi$ adalah elemen prima sebagai mana dalam (1). Jika $a^2 + b^2$ ganjil, maka $a \pm bi$ adalah elemen prima di $\mathbb{Z}[i]$ seperti pada (3). Jadi kita telah menemukan semua bilangan prima di $\mathbb{Z}[i]$. ✓

Contoh 9.3.2 Sekarang setelah kita mengetahui yang merupakan elemen tak-tereduksi di $\mathbb{Z}[i]$, kita dapat memfaktorkan elemen $\mathbb{Z}[i]$ menjadi faktor tak-tereduksi. Sebagai contoh, misalkan kita ingin memfaktorkan $4 + 3i$ menjadi faktor yang tak-tereduksi. Pertama perhatikan bahwa jika $4 + 3i = (a + bi)(c + di)$ maka $25 = v(4 + 3z) = (a^2 + b^2)(c^2 + d^2)$. Oleh karena

itu $a^2 + b^2 = c^2 + d^2 = 5$ dan $a = \pm 2$ dan $b = \pm 1$ atau $a = \pm 1$ dan $b = \pm 2$. Oleh karena itu kita memperoleh $4 + 3i = (2 - i)(1 + 2i)$. Dengan Proposisi 9.3.2, bagian (3), maka $2 - i$ dan $1 + 2i$ adalah faktor-faktot yang tak-tereduksi di $\mathbb{Z}[i]$. ●

Latihan

Dalam Latihan 1 sampai 4 nyatakan bilangan prima yang ditunjukkan di $\mathbb{Z}$ sebagai jumlah dari dua kuadrat dan tulis faktorisasinya menjadi tak-tereduksi di $\mathbb{Z}[i]$.
1. 17 **2.** 29 **3.** 37 **4.** 41.

Dalam Latihan 5 hingga 8 faktorkan bilangan bulat Gaussian yang ditunjukkan ke dalam produk yang tak-tereduksi di $\mathbb{Z}[i]$.
5. 11 **6.** 13 **7.** $-1 + 5i$ **8.** $8 - i$.

9. Buktikan bahwa ada tak-berhingga banyak bilangan prima p di $\mathbb{Z}$ sehingga $p \equiv 3 \mod 4$.

10. (a) Buktikan bahwa ada tak-berhingga banyak elemen prima $a + bi$ di $\mathbb{Z}[i]$ dengan $a \neq 0$ dan $b \neq 0$.
(b) Buktikan bahwa ada tak-berhingga banyak bilangan prima p di $\mathbb{Z}$ sehingga $p \equiv 1 \mod 4$.

11. Misalkan n adalah suatu bilangan bulat positif dengan faktorisasi prima

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} q_1^{b_1} q_2^{b_2} \cdots q_s^{b_s},$$

dimana $p_i \equiv 1 \mod 4, 1 \leq i \leq r$ dan $q_j \equiv 3 \mod 4, 1 \leq j \leq s$. Tunjukkan bahwa n dapat ditulis sebagai jumlah dari dua kuadrat jika dan hanya jika b_j genap untuk semua $1 \leq j \leq s$.

12. Misalkan I adalah suatu ideal tak-trivial di $\mathbb{Z}[i]$. Tunjukkan bahwa $\mathbb{Z}[i]/I$ adalah suatu ring berhingga.

13. Misalkan z tak-tereduksi di $\mathbb{Z}[i]$. Tunjukkan bahwa $\mathbb{Z}[i]/\langle z \rangle$ adalah suatu lapangan.

Dalam Latihan 14 hingga 17 dapatkan order dan karakteristik lapangan yang diberikan.

14. $\mathbb{Z}[i]/\langle 3 \rangle$ **15.** $\mathbb{Z}[i]/\langle 7 \rangle$ **16.** $\mathbb{Z}[i]/\langle 1 + i \rangle$ **17.** $\mathbb{Z}[i]/\langle 2 + i \rangle$.

18. Misalkan q adalah suatu bilangan prima di $\mathbb{Z}$ sedemikian hingga $q \equiv 3 \mod 4$. Tunjukkan bahwa $\mathbb{Z}[i]/\langle q \rangle$ adalah suatu lapangan dengan order q^2.

19. Misalkan p adalah suatu bilangan prima di $\mathbb{Z}$ sehingga $p \equiv 1 \mod 4$. Tunjukkan bahwa

(a) $\mathbb{Z}[i]/\langle p \rangle$ adalah bukan suatu daerah integral.
(b) $\mathbb{Z}[i]/\langle p \rangle$ mempunyai order p^2.
(c) $\mathbb{Z}_p[i]/\langle p \rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

20. (**Teorema Sisa China**) Misalkan R adalah suatu ring komutatif dan K dan L dua ideal sejati dalam R sehingga $K + L = R$. Tunjukkan bahwa

$$R/(K \cap L) \cong R/K \times R/L.$$

21. Dalam $\mathbb{Z}[i]$ misalkan I adalah ideal dibangun oleh $3 + 11i$ and $7 + 4i$

(a) Dapatkan $d \in \mathbb{Z}[i]$ sedemikian hingga $I = \langle d \rangle$.

(b) Tulis d sebagai hasil perkalian dari elemen-elemen tak=terduksi di $\mathbb{Z}[i]$.

(c) Gunakan latihan sebelumnya untuk menunjukkan bahwa

$$\mathbb{Z}[i]/I \cong \mathbb{F}_1 \times \mathbb{F}_2,$$

untuk beberapa lapangan $\mathbb{F}_1$ dan $\mathbb{F}_2$.

(d) Jelaskan lapangan-lapangan $\mathbb{F}_1$ dan $\mathbb{F}_2$ ini.

Bab 10

Teori Lapangan

Setelah pengenalan singkat tentang **ruang vektor** atas suatu lapangan $\mathbb{F}$, kita memperkenalkan gagasan tentang **perluasan lapangan** $\mathbb{E}$ dari $\mathbb{F}$ merupakan lapangan yang lebih besar memuat $\mathbb{F}$. Perluasan lapangan $\mathbb{E}$ dapat dilihat baik sebagai lapangan maupun sebagai ruang vektor atas $\mathbb{F}$. Kita membuktikan teorema **Kronecker**, yang menyatakan bahwa setiap polinomial tak-konstan atas suatu lapangan $\mathbb{F}$ memiliki akar-akar di beberapa perluasan lapangan $\mathbb{E}$ dari $\mathbb{F}$. Kita kemudian mempelajari **perluasan terkecil** dari $\mathbb{F}$ yang berisi semua akar-akar dari polinomial yang diberikan, dan disebut **lapangan pemecah** (*splitting field*) dari polinomial. Pada bagian terakhir, kita menggunakan keberadaan dan ketunggalan lapangan pemecah dari polinomial tertentu untuk mendapatkan suatu teorema klasifikasi dari lapangan hingga.

10.1 Ruang Vektor

Aljabar linier adalah mata pelajaran dasar dalam matematika. Pada bagian ini kita hanya memberikan pengantar singkat untuk subjek ini untuk memperkenalkan beberapa pengertian dasar aljabar linier yang penting untuk studi lapangan di bagian selanjutnya. Gagasan penting adalah **ruang vektor** atas suatu lapangan, suatu **basis** dari suatu ruang vektor atas suatu lapangan, dan **dimensi** dari suatu ruang vektor atas suatu lapangan.

Contoh 10.1.1 Pertimbangkan lapangan $\mathbb{C}$ dari bilangan kompleks. Pada Bagian 1.4 kami menjelaskan bagaimana bilangan kompleks $z = a + bi \in \mathbb{C}$ dapat direpresentasikan dengan titik $(a, b) \in \mathbb{R}^2$

Elemen di $\mathbb{C}$	**Titik di $\mathbb{R}^2$**
$a + bi$	(a, b)
1	$(1, 0)$
i	$(0, 1)$
$(a + bi) + (c + di) = (a + c) + (b + d)i$	$(a, b) + (c, d) = (a + c, b + d)$
$c(a + bi) = ca + cbi$, untuk $c \in \mathbb{R}$	$c(a, b) = (ca, cb)$, untuk $c \in \mathbb{R}$
$a + bi = a \cdot 1 + b \cdot i$	$(a, b) = a(1, 0) + b(0, 1)$.

Kita telah memilih dalam contoh ini sifat-sifat elemen di $\mathbb{C}$ yang disajikan dengan titik yang sesuai pada lapangan $\mathbb{R}^2$. ●

Definisi 10.1.1 Misalkan $\mathbb{F}$ adalah suatu lapangan. Suatu himpunan V yang dilengkapi dengan dua operasi, ditulis sebagai **penjumlahan** dan **perkalian**, dikatakan sebagai ruang vektor atas $\mathbb{F}$ jika

(1) V adalah grup Abelian terhadap operasi penjumlahan. Untuk semua $a, b \in \mathbb{F}$ dan semua $u, v \in V$,

(2) Hasil perkalian $av \in V$ terdefinisi.

(3) $a(u + v) = au + av$

(4) $a(bv) = (ab)v$

(5) $1_{\mathbb{F}}v = v$.

Suatu elemen $v \in V$ disebut **vektor**. Elemen identitas di V terhadap penjumlahan disebut **vektor nol** dan ditulis 0_V. Suatu elemen $a \in \mathbb{F}$ disebut **skalar**, dan operasi hasil av disebut **perkalian skalar**.

Contoh 10.1.2 Himpunan $\mathbb{C}$ adalah suatu ruang vektor atas lapangan $\mathbb{R}$.

Contoh 10.1.3 Untuk sebarang lapangan $\mathbb{F}$ dan sebarang bilangan bulat positip n, misalkan

$$\mathbb{F}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{F} \text{ untuk } 1 \leq i \leq n\}.$$

Maka $\mathbb{F}^n$ adalah ruang vektor atas $\mathbb{F}$ dengan operasi penambahan komponen yang sesuai:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n)$$

dan perkalian skalar

$$c(a_1, a_2, \ldots, a_n) = (ca_1, ca_2, \ldots, ca_n), \text{ untuk sebarang } c \in \mathbb{F}.$$

Contoh 10.1.4 Untuk sembarang lapangan $\mathbb{F}$ ring polinomial $\mathbb{F}[x]$ adalah ruang vektor atas $\mathbb{F}$, karena

(1) $\mathbb{F}[x]$ adalah suatu ring, dan karenanya merupakan grup Abelian terhadap operasi penjumlahan.

(2) Untuk setiap konstanta $c \in \mathbb{F}$ dan setiap polinomial $f(x) \in \mathbb{F}[x]$, $cf(x) \in \mathbb{F}[x]$, dan dengan demikian kondisi (3) sampai (5) dari Definisi 10.1.1 dipenuhi.

Contoh 10.1.5 Untuk sembarang lapangan $\mathbb{F}$, himpunan $M(2, \mathbb{F})$ adalah ring dari semua matriks berukuran 2×2 dengan entri di $\mathbb{F}$ adalah ruang vektor atas $\mathbb{F}$ dengan operasi penjumlahan biasa pada matriks dan perkalian skalar:

$$c\begin{bmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{bmatrix} = \begin{bmatrix} ca_{1,1} & ca_{1,2} \\ ca_{2,1} & ca_{2,2} \end{bmatrix},$$

untuk sebarang $c \in \mathbb{F}$.

Beberapa contoh ruang vektor tersebut dapat digeneralisasikan sebagai berikut.

Proposisi 10.1.1 Diberikan $\mathbb{F} \subseteq R$ dimana $\mathbb{F}$ adalah suatu lapangan dan R adalah suatu ring yang memuat $\mathbb{F}$ sebagai subring, maka R adalah ruang vektor atas $\mathbb{F}$.

Bukti
Sebagai Latihan!

Untuk sebarang ruang vektor V atas suatu lapangan $\mathbb{F}$ ada dua elemen identitas terhadap penjumlahan yang terlibat, **vektor nol** $0_V \in V$ dan **skalar nol** $0_F \in \mathbb{F}$. Juga, setiap vektor $v \in V$ memiliki invers terhadap penjulahan $-v \in V$, sedangkan setiap skalar $c \in \mathbb{F}$ memiliki invers terhadap penjumlahan $-c \in \mathbb{F}$. Proposisi berikutnya menyatakan hubungan antara dua jenis **identitas** terhadap penjumlahan dan dua jenis **invers** terhadap penjumlahan menyiratkan, khususnya, bahwa $-v = (-1_F)v$.

Proposisi 10.1.2 Misalkan V adalah suatu ruang vektor atas suatu lapangan $\mathbb{F}$. Maka untuk sebarang skalar $c \in \mathbb{F}$ dan sebarang vektor $v \in V$

(1) $cv = 0_V$ jika dan hanya jika $c = 0_{\mathbb{F}} \in \mathbb{F}$ atau $v = 0_V \in V$.

(2) $-cv = -(cv) = c(-v)$

Bukti
(1) ($\Leftarrow$) Jika $c = 0_{\mathbb{F}} \in \mathbb{F}$, maka menurut Definisi 10.1.1 bagian (3), $0_{\mathbb{F}}v = (0_{\mathbb{F}} + 0_{\mathbb{F}})v = 0_{\mathbb{F}}v + 0_{\mathbb{F}}v$. Oleh karena itu $0_{\mathbb{F}}v = 0_V$. Demikian pula, jika $v = 0_V \in V$, maka $c0_V = c(0_V + 0_V) = c0_V + c0_V$, dan $c0_V = 0_V$.
($\Rightarrow$) Jika $cv = 0_V$ dan $c \neq 0_{\mathbb{F}} \in \mathbb{F}$, maka c adalah unit di $\mathbb{F}$. Kita memiliki $c^{-1}0_V = 0_V$ dengan apa yang telah kita buktikan. Tetapi menggunakan Definisi 10.1.1 bagian (4) dan (5) kita juga memiliki $c^{-1}0_V = c^{-1}(cv) = (c^{-1}c)v = 1_{\mathbb{F}}v = v$. Oleh karena itu $v = c^{-1}0_V = 0_V$.
(2) Menggunakan bagian (1), kita memiliki $(-c)v + cv = (-c + c)v = 0_{\mathbb{F}}v = 0_V$. Oleh karena itu, $(-c)v = -(cv)$. Demikian pula, $c(-v) + cv = c(-v + v) = c0_V = 0_V$, hal ini berakibat $c(-v) = -(cv)$.

Dengan setiap struktur aljabar yang telah kita perkenalkan (grup, ring, lapangan) kita telah mendefinisikan gagasan tentang substruktur (subgrup, subring, sublapangan). Dengan cara yang sama, kita mendefinisikan subruang dari ruang vektor dan menyatakan pengujian subruang yang pembuktiannya diberikan sebagai latihan.

Definisi 10.1.2 Himpunan bagian tak kosong U dari ruang vektor V atas suatu lapangan $\mathbb{F}$ adalah **subruang** dari V jika U adalah ruang vektor atas $\mathbb{F}$ pada operasi penjumlahan dan perkalian skalar yang sama sebagaimana di V.

Teorema 10.1.1 ***(Pengujian Subruang)*** Himpunan bagian tak kosong U dari suatu ruang vektor V atas suatu lapangan $\mathbb{F}$ adalah subruang dari V jika dan hanya jika untuk semua $c \in \mathbb{F}$ dan $u, v \in U$ kita memiliki

(1) $u - v \in U$

(2) $cu \in U$.

Bukti
Sebagai Latihan!

Contoh 10.1.6 Seperti yang kita lihat pada Contoh 10.1.4, untuk sebarang lapangan $\mathbb{F}$ ring $\mathbb{F}[x]$ adalah ruang vektor atas $\mathbb{F}$. Misalkan

$$\mathbb{F}^n[x] = \{f(x) \in \mathbb{F}[x] \mid \deg f(x) < n \text{ atau } f(x) = 0\}.$$

Maka $\mathbb{F}^n[x]$ adalah subruang dari $\mathbb{F}[x]$, sebab untuk sebarang $c \in \mathbb{F}$ dan sebarang fx dan $g(x)$ di $\mathbb{F}^n[x]$ kita mempunyai

(1) $\deg f(x) - g(x)) < n$ dan karenanya $f(x) - g(x) \in \mathbb{F}^n[x]$ atau $f(x) - g(x)) = 0 \in \mathbb{F}^n[x]$.

(2) $\deg(cf(x) = \deg f(x) < n$, dan karenanya $cf(x) \in \mathbb{F}^n[x]$, atau $cf(x) = 0 \in \mathbb{F}^n[x]$ dan pengujian subruang berlaku. ●

Proposisi 10.1.3 Dalam $\mathbb{F}[x]$, dimana $\mathbb{F}$ adalah suatu lapangan, maka sebarang ideal I dalam $\mathbb{F}[x]$ adalah subruang dari dari $\mathbb{F}[x]$.

Bukti
Sebagai Latihan! ✓

Contoh 10.1.7 Dalam $\mathbb{F}^n$ seperti yang didefinisikan dalam Contoh 10.1.3, dan $s \leq n$, misalkan

$$U^s = \{(a_1, a_2, \ldots, a_s, 0, 0, \ldots, 0) \mid a_i \in \mathbb{F} \text{ untuk } 1 \leq i \leq s\},$$

maka U^s adalah subruang dari $\mathbb{F}^n$. ●

Contoh 10.1.8 Pertimbangkan sistem persamaan linier:

$$\begin{aligned} c_{1,1}x_1 + c_{1,2}x_2 + \cdots c_{1,m}x_m &= 0_{\mathbb{F}} \\ c_{2,1}x_1 + c_{2,2}x_2 + \cdots c_{2,m}x_m &= 0_{\mathbb{F}} \\ &\vdots \\ c_{n,1}x_1 + c_{n,2}x_2 + \cdots c_{n,m}x_m &= 0_{\mathbb{F}} \end{aligned}$$

dengan $c_{i,j} \in \mathbb{F}$ dimana $\mathbb{F}$ adalah suatu lapangan. Misalkan U adalah himpunan bagian dari ruang vektor

$$\mathbb{F}^m = \{(a_1, a_2, \ldots, a_m) \mid a_i \in \mathbb{F} \text{ untuk } 1 \leq i \leq m\}$$

terdiri dari semua solusi dari sistem ini. Maka U adalah subruang dari $\mathbb{F}^m$. Karena jika $(a_1, a_2, \ldots, a_m)$ dan $(b_1, b_2, \ldots, b_m)$ ada di U, maka

$$\begin{aligned} (1)\ c_{i,1}(a_1 - b_1) + \cdots + c_{i,m}(a_m - b_m) &= (c_{i,1}a_1 + \cdots c_{i,n}a_m) + (c_{i,1}b_1 + \cdots c_{i,n}b_m) \\ &= 0_{\mathbb{F}} - 0_{\mathbb{F}} \\ &= 0_{\mathbb{F}}, \end{aligned}$$

untuk semua i, $\leq i \leq n$, maka $(a_1 - b_1, \ldots, a_m - b_m) \in U$.

$$\begin{aligned} (2)\ c_{i,1}(da_1) + \cdots + c_{i,m}(da_m) &= d(c_{i,1}a_1 + \cdots c_{i,n}a_m) \\ &= d0_{\mathbb{F}} \\ &= 0_{\mathbb{F}}, \end{aligned}$$

untuk sebarang $d \in \mathbb{F}$, maka $(da_1, \ldots, da_m) \in U$. ●

Contoh 10.1.9 Misalkan V adalah suatu ruang vektor atas suatu lapangan $\mathbb{F}$ dan misalkan v_1, v_2 adalah dua vektor di V. Misalkan

$$U = \{c_1v_1 + c_2v_2 \mid c_1, c_2 \in \mathbb{F}\}.$$

Maka U adalah subruang dari V. Karena jika $u = a_1v_1 + a_2v_2 \in U$ dan $w = b_1v_1 + b_2v_2 \in U$, maka

(1) $u - w = (a_1 - b_1)v_1 + (a_2 - b_2)v_2 \in U$,

(2) $cu = (ca_1)v_1 + (ca_2)v_2 \in U$,

untuk sebarang $c \in \mathbb{F}$. ●

Contoh terakhir ini memperkenalkan kita pada gagasan penting berikut.

Definisi 10.1.3 Misalkan V adalah suatu ruang vektor atas suatu lapangan $\mathbb{F}$ dan misalkan $v_1, v_2, \ldots, v_n$ adalah vektor di V. Maka

(1) vektor $c_1v_1 + c_1v_2 + \cdots + c_nv_n$ dimana $c_i \in \mathbb{F}$ untuk semua i disebut **kombinasi linier dari vektor** v_i.

(2) **Himpunan bentangan** dari vektor-vektor v_i dinotasikan sebagai himpunan

$$\text{span}\{v_1, v_2, \ldots, v_n\} = \{c_1v_1 + c_2v_2 + \cdots + c_nv_n \mid c_i \in \mathbb{F} \text{ untuk semua } i\}$$

adalah himpunan dari semua kombinasi linier dari vektor-vektor v_i. ✓

Konsekuensi langsung dari Definisi 10.1.3 adalah proposisi berikut, yang dua bagiannya bersama-sama mengatakan bahwa $\text{span}\{v_1, v_2, \ldots, v_n\}$ adalah subruang terkecil dari V yang memuat semua v_i.

Proposisi 10.1.4 Misalkan V adalah suatu ruang vektor atas suatu lapangan $\mathbb{F}$ dan vektor $v_1, \ldots, v_n$ di V. Maka

(1) $\text{span}\{v_1, v_2, \ldots, v_n\}$ adalah suatu subruang dari V.

(2) Jika U adalah subruang dari V dan $v_1, \ldots, v_n \in U$ maka $\text{span}\{v_1, \ldots, v_n\} \subseteq U$.

Bukti

(1) Kasus $n = 2$ dibuktikan dalam Contoh 10.1.9, dan bukti dalam kasus umum adalah sama.

(2) Menurut Definisi 10.1.3, $\text{span}\{v_1, \ldots, v_n\}$ terdiri dari semua kombinasi linier dari v_i, dan menurut pengujian subruang (Teorema 10.1.1), maka subruang U berisi semua kombinasi linier dari elemen-elemennya. ✓

Contoh 10.1.10 Dalam ruang vektor $\mathbb{F}[x]$ vektor $1, x, x^2, \ldots, x^{n-1}$ membentang subruang $\mathbb{F}^n[x] = \{f(x) \in \mathbb{F}[x] \mid \deg f(x) < 0 \text{ atau } f(x) = 0\}$. Dengan demikian himpunan bentangan $\text{span}\{1, x, x^2, \ldots, x^{n-1}\} = \mathbb{F}^n[x]$. ●

Contoh 10.1.11 Dalam $\mathbb{R}^3$ vektor $v_1 = (-3, 0, 1)$ dan $v_2 = (2, 1, 0)$ membentang subruang

$$\text{span}\{v_1, v_2\} = \{(2s - 3t, s, t) \mid s, t \in \mathbb{R}\}$$

yang merupakan suatu bidang di ruang $\mathbb{R}^3$ melalui titik asal dan didefinisikan oleh persamaan $x - 2y + 3z = 0$. ●

Contoh 10.1.12 Dalam ruang vektor V sebuah vektor tak-nol w berada dalam bentangan dua vektor tertentu $v_1, v_2 \in V$ jika ada skalar $c_1, c_2 \in \mathbb{F}$ sehingga $w = c_1v_1 + c_2v_2$ atau , ekuivalen, $w + (-c_1)v_1 + (-c_2)v_2 = 0_V$. Sebaliknya, jika ada skalar d_0, d_1, d_2 di lapangan $\mathbb{F}$ dengan $d_0 \neq 0_{\mathbb{F}}$ sedemikian rupa sehingga $d_0w + d_1v_1 + d_2v_2 = 0_V$, maka vektor w dapat ditulis sebagai kombinasi linier $w = (-d_1d_0^{-1})v_1 + (-d_2d_0^{-1})v_2$ dengan demikian $w \in \text{span}\{v_1, v_2\}$. ●

Definisi 10.1.4 Misalkan $v_1, v_2 \ldots, v_n$ adalah vektor di ruang vektor V atas suatu lapangan $\mathbb{F}$.

(1) Himpunan $v_1, v_2 \ldots, v_n$ disebut **bebas linier** atas $\mathbb{F}$ jika kombinasi linier

$$c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0_V$$

untuk $c_i \in \mathbb{F}$, menyiratkan bahwa $c_i = 0_{\mathbb{F}}$ untuk semua $1 \leq i \leq n$.

(2) Himpunan $v_1, v_2 \ldots, v_n$ disebut **bergantungan linier** atas $\mathbb{F}$ jika kombinasi linier

$$c_1v_1 + c_2v_2 + \cdots + c_nv_n = 0_V$$

untuk beberapa $c_i \in \mathbb{F}$, $1 \leq i \leq n$ dengan tidak semua $c_i = 0_{\mathbb{F}}$. ✓

Perhatikan bahwa himpunan $\{v_1, v_2, \ldots, v_n\}$ bergantung linier atas $\mathbb{F}$ jika dan hanya jika paling sedikit salah satu vektor v_i berada dalam himpunan bentangan $n - 1$ vektor yang lainnya.

Contoh 10.1.13 Dalam $\mathbb{F}[x]$ himpunan vektor $\{1, x, x^2, \ldots, x^n\}$ untuk setiap $n \geq 1$ bebas linier atas $\mathbb{F}$ karena

$$c_0 1 + c_1x + c_2x^2 + \cdots + c_nx^n = 0_{\mathbb{F}[x]}$$

jika dan hanya jika $c_i = 0_{\mathbb{F}}$ untuk semua i. ●

Contoh 10.1.14 Dalam $\mathbb{C}$ himpunan $\{1, i\}$ bebas linier atas $\mathbb{R}$ karena

$$a \cdot 1 + b \cdot i = 0$$

jika dan hanya jika $a = b = 0$. ●

Definisi 10.1.5 Dalam ruang vektor V, himpunan vektor $\{v_1, \ldots, v_n\}$ disebut **basis** untuk V atas $\mathbb{F}$ jika
(l) $\text{span}\{v_1, \ldots, v_n\} = V$
(2) $\{v_1, \ldots, v_n\}$ bebas linier atas $\mathbb{F}$. ✓

Contoh 10.1.15
(1) Himpunan $\{1, i\}$ adalah suatu basis untuk $\mathbb{C}$ atas $\mathbb{R}$.
(2) Himpunan $\{1, \sqrt{2}\}$ adalah suatu basis untuk $\mathbb{Q}(\sqrt{2})$ atas $\mathbb{Q}$. ●

Contoh 10.1.16 Himpunan $\{1, x, x^2, \ldots, x^{n-1}\}$ adalah suatu basis untuk

$$\mathbb{F}^n[x] = \{f(x) \in \mathbb{F}[x] \mid \deg f(x) < n \text{ atau } f(x) = 0\}$$

atas $\mathbb{F}$. ●

Contoh 10.1.17 Untuk sebarang lapangan $\mathbb{F}$, ruang vektor

$$\mathbb{F}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{F} \text{ untuk } 1 \leq i \leq n\},$$

salah satu basisnya adalah vektor-vektor:

$$\begin{aligned} e_1 &= (1_\mathbb{F}, 0_\mathbb{F}, \ldots, 0_\mathbb{F}) \\ e_2 &= (0_\mathbb{F}, 1_\mathbb{F}, \ldots, 0_\mathbb{F}) \\ &\vdots \\ e_n &= (0_\mathbb{F}, 0_\mathbb{F}, \ldots, 1_\mathbb{F}). \end{aligned}$$

Basis $\{e_1, e_2, \ldots, e_n\}$ ini disebut **basis baku** untuk $\mathbb{F}^n$ atas $\mathbb{F}$. ●

Contoh 10.1.18 Untuk sebarang lapangan $\mathbb{F}$, dalam ruang vektor $M(2, \mathbb{F})$ himpunan matriks berukuran 2×2 dengan elemen-elemen di $\mathbb{F}$, matriks

$$E_1 = \begin{bmatrix} 1_\mathbb{F} & 0_\mathbb{F} \\ 0_\mathbb{F} & 0_\mathbb{F} \end{bmatrix}, \; E_2 = \begin{bmatrix} 0_\mathbb{F} & 1_\mathbb{F} \\ 0_\mathbb{F} & 0_\mathbb{F} \end{bmatrix}, \; E_3 = \begin{bmatrix} 0_\mathbb{F} & 0_\mathbb{F} \\ 1_\mathbb{F} & 0_\mathbb{F} \end{bmatrix}, \; E_4 = \begin{bmatrix} 0_\mathbb{F} & 0_\mathbb{F} \\ 0_\mathbb{F} & 1_\mathbb{F} \end{bmatrix},$$

membentuk suatu basis dari $M(2, \mathbb{F})$ atas $\mathbb{F}$. ●

Konsep yang sangat penting dalam arti tertentu menggambarkan ruang vektor adalah **dimensi**nya. Kita mendefinisikan dimensi ruang vektor dalam hal banyaknya anggota himpunan suatu basis yang diberikan dalam ruang vektor. Tetapi pertama-tama kita harus menunjukkan bahwa semua basis untuk ruang vektor yang diberikan memiliki banyaknya elemen-elemen sama, yang merupakan teorema kita berikutnya.

Teorema 10.1.2 Misalkan V adalah suatu ruang vektor atas suatu lapangan $\mathbb{F}$ dan misalkan $\{v_1, \ldots, v_n\}$ dan $\{u_1, \ldots, u_m\}$ adalah dua basis untuk V atas $\mathbb{F}$. Maka $n = m$.

Bukti
Andaikankan $n \neq m$ dan misalkan $n < m$. Pertimbangkan himpunan $\{u_1, v_1, \ldots, v_n\}$. Karena $u_1 \in \text{span}\{v_1, v_2, \ldots, v_n\}$, terdapat skalar $a_i \in \mathbb{F}$ sehingga

$$u_1 = a_1 v_1 + a_2 v_2 + \cdots + a_n v_n$$

dan a_i, $1 \leq i \leq n$ tidak semuanya nol. Katakanlah (indeks ulang v_i jika perlu) bahwa $a_1 \neq 0_\mathbb{F}$. Maka

$$v_1 = (a_1^{-1})u_1 + (-a_2 a_1^{-1})v_2 + \cdots + (-a_n a_1^{-1})v_n.$$

Jadi $v_1 \in \text{span}\{u_1, v2, \ldots, v_n\}$ dan karena jelas $v_i \in \text{span}\{u_1, v_2, \ldots, v_n\}$ untuk $2 \leq i \leq n$, maka menurut Proposisi 10.1.4 $\text{span}\{v_1, v_2, \ldots, v_n\} \subseteq \text{span}\{u_1, v_2, \ldots, v_n\}$ akibatnya, kita mempunyai $V = \text{span}\{u_1, v_2, \ldots, v_n\}$. Sekarang pertimbangkan $u_2 \in V = \text{span}\{u_1, v_2, \ldots, v_n\}$. Kita mempunyai

$$u_2 = b_1 u_1 + b_2 v_2 + \cdots + b_n v_n$$

untuk beberapa $b_i \in \mathbb{F}$ dan karena u_1 dan u_2 bebas linier, maka b_i untuk $2 \leq i \leq n$ tidak semuanya nol. Katakanlah $b_2 \neq 0_{\mathbb{F}}$. Maka

$$v_2 = (-b_2^{-1}b_1)u_1 + (b_2^{-1})u_2 + (-b_2^{-1}b_3)v_3 \cdots + (-b_2^{-1}b_n)v_n$$

dan $V = \text{span}\{u_1, u_2, v_3 \ldots, v_n\}$. Melanjutkan dengan cara ini, kita memperoleh

$$V = \text{span}\{u_1, u_2, u_3 \ldots, u_n\}.$$

Kita membuat asumsi bahwa $n < m$. Oleh karena itu, untuk $u_{n+1} \in V$ adalah kombinasi linier dari vektor $\{u_1, u_2, u_3, \ldots, u_n\}$, dengan demikian himpunan $\{u_1, u_2, u_3, \ ldotsu_n, u_{n+1}, \ldots, u_m\}$ bergantung linier dan bukan basis. Ini adalah kontradiksi, maka haruslah $n = m$ dan buktinya lengkap.

Definisi 10.1.6 Misalkan V adalah suatu ruang vektor atas suatu lapangan $\mathbb{F}$. Jika terdapat himpunan berhingga yang membentuk basis untuk V atas $\mathbb{F}$ maka bilangan n yang merupakan banyaknya vektor-vektor dalam basis $\{v_1, \ldots, v_n\}$ (yang sama untuk semua basis seperti itu oleh teorema sebelumnya) disebut **dimensi** dari V atas $\mathbb{F}$ ditulis $\dim_{\mathbb{F}} V$. Jika tidak ada basis berhingga untuk ruang vektor V atas $\mathbb{F}$ maka V dikatakan **berdimensi tak hingga** atas $\mathbb{F}$.

Contoh 10.1.19 Berikut contoh dimensi ruang vektor:

(1) $\dim_{\mathbb{R}} \mathbb{C} = 2$.

(2) $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = 2$.

(3) $\dim_{\mathbb{R}} M(2, \mathbb{R}) = 4$.

(4) $\dim_{\mathbb{R}} \mathbb{R}^n = n$.

(5) $\dim_{\mathbb{F}} \mathbb{F}^n[x] = n$.

(6) $\mathbb{F}[x]$ berdimensi tak-hingga atas $\mathbb{F}$ ($\dim_{\mathbb{F}} \mathbb{F}[x] = \infty$.)

Kita menyimpulkan bagian ini dengan fakta yang berguna tentang himpunan bebas linier dalam ruang vektor berdimensi hingga.

Teorema 10.1.3 Misalkan V adalah suatu ruang vektor atas suatu lapangan $\mathbb{F}$ dengan $\dim_{\mathbb{F}} V = n$, dan misalkan $\{u_1, \ldots, u_r\}$ adalah himpunan vektor yang bebas linier di V. Maka

(1) $r \leq n$.

(2) Jika $r < n$ maka ada vektor $u_{r+1}, \ldots, u_n$ di V sedemikian rupa sehingga $\{u_1, u_2, \ldots, u_n\}$ membentuk basis untuk V atas $\mathbb{F}$.

Bukti
Jika $\text{span}\{u_1, \ldots, u_r\} = V$, maka $\{u_1, \ldots, u_r\}$ adalah basis untuk V, dan menurut Teorema 10.1.2 didapat $r = n$. Jika tidak, misalkan $\{v_1, \ldots, v_n\}$ adalah suatu basis untuk V atas $\mathbb{F}$. Maka

$$V = \text{span}\{v_1, \ldots, v_n\} \neq \text{span}\{u_1, \ldots, u_r\}$$

pasti ada $v_i \notin \text{span}\{u_1, \ldots, u_r\}$. Katakanlah (lakukan indeks ulang v_i jika perlu) dalam hal ini adalah v_1. Maka himpunan $\{u_1, \ldots, u_r, v_1\}$ adalah himpunan vektor yang bebas linier. Jika $\text{span}\{u_1, \ldots, u_r, v_1\} = V$, maka $\{u_1, \ldots, u_r, v_1\}$ adalah basis, dan $r = n - 1 < n$. Jika tidak, menggunakan argumen yang sama seperti sebelumnya, harus ada beberapa vektor $v_i \notin \text{span}\{u_1, \ldots, u_r, v_1\}$, misalkan v_2. Maka $\{u_1, \ldots, u_r, v_1, v_2\}$ adalah himpunan vektor yang bebas linier. Mengulangi proses ini, itu harus diakhiri untuk beberapa $k < n$ sedemikian rupa sehingga

$$\{u_1, \ldots, u_r, v_1, v_2, \ldots v_k\} = \{u_1, \ldots, u_r, v_1, v_2, \ldots v_{n-r}\},$$

adalah suatu basis untuk V, dan $r = n - k < n$ ◩

Akibat 10.1.1 Misalkan V adalah suatu ruang vektor atas suatu lapangan $\mathbb{F}$ dengan $\dim_{\mathbb{F}} V = n$ dan U subruang dari V. Maka

(1) Setiap basis untuk U dapat diperluas menjadi basis untuk V.

(2) $\dim_{\mathbb{F}} U \leq \dim_{\mathbb{F}} V$.

(3) $\dim_{\mathbb{F}} U = \dim_{\mathbb{F}} V$ jika dan hanya jika $U = V$.

Bukti
Sebagai Latihan! ◩

Latihan

Dalam Latihan 1 sampai 6 tentukan apakah himpunan vektor yang ditunjukkan merupakan basis untuk ruang vektor yang ditunjukkan V atas lapangan yang ditunjukkan $\mathbb{F}$.

1. $\{(1,1,1),(0,0,1),(1,1,0)\}$ $V = \mathbb{R}^3$ $\mathbb{F} = \mathbb{R}$
2. $\{2+3i, -5\}$ $V = \mathbb{C}$ $\mathbb{F} = \mathbb{R}$
3. $\{1+i, 2+i, 3i\}$ $V = \mathbb{C}$ $\mathbb{F} = \mathbb{R}$
5. $\{2+3x, -x^2+x, x^2+5\}$ $V = \mathbb{Q}^3[x]$ $\mathbb{F} = \mathbb{Q}$
6. $\{1+3\sqrt{2}, 2+5\sqrt{2}\}$ $V = \mathbb{Q}(\sqrt{2})$ $\mathbb{F} = \mathbb{Q}$.

7. Buktikan uji subruang, Teorema 10.1.1.

8. Misalkan $\mathbb{F}$ adalah suatu lapangan dan R adalah suatu ring sedemikian rupa sehingga $\mathbb{F} \subseteq R$ adalah subring dari R. Tunjukkan bahwa R adalah ruang vektor atas $\mathbb{F}$.

9. Buktikan Proposition 10.1.3.

Dalam Latihan 10 hingga 17 tentukan apakah subset yang ditunjukkan U adalah subruang dari ruang vektor yang ditunjukkan V atas lapangan yang ditunjukkan $\mathbb{F}$.

10. $U = \mathbb{Q}$ $V = \mathbb{Q}(\sqrt{3})$ $\mathbb{F} = \mathbb{Q}$
11. $U = \mathbb{R}$ $V = \mathbb{C}$ $\mathbb{F} = \mathbb{Q}$
12. $U = \{f(x) \in \mathbb{Q}[x] \mid f(1) = 0\}$ $V = \mathbb{Q}[x]$ $\mathbb{F} = \mathbb{Q}$
13. $U = \{f(x) \in \mathbb{Q}[x] \mid f(2) = 0\}$ $V = \mathbb{Q}[x]$ $\mathbb{F} = \mathbb{Q}$
14. $U = \{(x,0,z) \mid x,z \in \mathbb{R}\}$ $V = \mathbb{R}^3$ $\mathbb{F} = \mathbb{R}$
15. $U = \{(x,1,z) \mid x,z \in \mathbb{R}\}$ $V = \mathbb{R}^3$ $\mathbb{F} = \mathbb{R}$
16. $U = \{(a,b,2b-3a) \mid a,b \in \mathbb{R}\}$ $V = \mathbb{R}^3$ $\mathbb{F} = \mathbb{R}$
17. $U = \left\{ \begin{bmatrix} a & 2a \\ 0 & 3a \end{bmatrix} \middle| a \in \mathbb{R} \right\}$ $V = M(2,\mathbb{R})$ $\mathbb{F} = \mathbb{R}$.

18. Jelaskan semua subruang dari $\mathbb{R}^3$.

Dalam Latihan 19 dan 20 dapatkan basis dari ruang vektor yang ditunjukkan V datas lapangan yang ditunjukkan $\mathbb{F}$.
19. $V = \mathbb{R}[x]/\langle x^2+1\rangle$, $\mathbb{F} = \mathbb{R}$ **20.** $V = \mathbb{Q}[x]/\langle x^2-5\rangle$, $\mathbb{F} = \mathbb{Q}$.

21. Misalkan c adalah sebarang elemen di suatu lapangan $\mathbb{F}$. Tunjukkan bahwa

$$\{1, (x-c), (x-c)^2, \ldots, (x-c)^{n-1}\}$$

adalah suatu basis untuk $\mathbb{F}^n[x] = \{f(x) \in \mathbb{F}[x] \mid \deg f(x) < n \text{ atau } f(x) = 0\}$ atas $\mathbb{F}$.

22. Misalkan V adalah suatu ruang vektor berdimensi hingga atas suatu lapangan $\mathbb{F}$. Tunjukkan bahwa subset $\{v_1, \ldots, v_n\}$ dari V adalah basis untuk V atas $\mathbb{F}$ jika dan hanya jika untuk setiap $w \in V$ terdapat tunggal elemen-elemen $c_i \in \mathbb{F}$, $1 \le i \le n$ sedemikian rupa sehingga $w = c_1v_1 + \cdots + c_nv_n$.

23. Buktikan Kesimpulanr 10.1.1.

24. Misalkan V adalah suatu ruang vektor atas suatu lapangan $\mathbb{F}$ dengan $\dim_{\mathbb{F}} V = n$, dan subruang U dan W dari V dengan $\dim_{\mathbb{F}} U = m$ dan $\dim_{\mathbb{F}} W = k$. Tunjukkan bahwa jika $m + k > n$ maka $U \cap W \neq \{0_V\}$.

25. Tentukan apakah himpunan bagian dari $\mathbb{Q}[x]$ yang ditunjukkan bebas linier atas $\mathbb{Q}$:
(a) $S = \{x^2-1, x^2-4\}$ (b) $T = \{x^2-1, x^2-4, x^2-9\}$ (c) $U = \{x^2-1, x^3-4, x^4-9\}$.

26. Misalkan V dan W adalah ruang vektor pada suatu lapangan yang sama $\mathbb{F}$. Suatu fungsi $T : V \to W$ dikatakan sebagai **transformasi linier** dari V ke W jika untuk semua $c, d \in \mathbb{F}$ dan semua $u, v \in V$ kita miliki

$$T(cu + dv) = cT(u) + dT(v).$$

Misalkan T adalah suatu transformasi linier.

(a) Tunjukkan bahwa $\mathrm{Im}(T)$, ***image*** dari T, adalah suatu subruang dari W.

(b) Tunjukkan bahwa $\ker(T) = \{v \in V \mid T(v) = 0_W\}$ adalah suatu subruang dari V.

27. Misalkan V dan W adalah ruang vektor atas lapangan yang sama F dan misalkan $T : V \to W$ merupakan transformasi linier. Tunjukkan bahwa

(a) Untuk sebarang himpunan bagian $\{v_1, \ldots, v_n\}$ dari V dengan $\mathrm{span}\{v_1, \ldots, v_n\} = V$, kita memiliki $\mathrm{span}\{T(v_1), \ldots, T(v_n)\} = W$ jika dan hanya jika T **pada**.

(b) T adalah **satu-satu** jika dan hanya jika untuk setiap himpunan bagian $\{v_1, \ldots, v_n\}$ dari V yang bebas linier dalam V atas $\mathbb{F}$; $\{T(v_1), \ldots, T(v_n)\}$ bebas linier dalam W atas $\mathbb{F}$.

28. Misalkan V dan W adalah suatu ruang vektor atas lapangan yang sama $\mathbb{F}$. Suatu **isomorpisma** dari V ke W adalah transformasi linier $T : V \to W$ yang **satu-satu** dan **pada**. Misalkan $\dim_{\mathbb{F}} V = n$ dan misalkan $T : V \to W$ merupakan transformasi linier. Tunjukkan bahwa

(a) Jika ada basis $\{v_1, \ldots, v_n\}$ untuk V atas $\mathbb{F}$ sehingga $\{T(v_1), \ldots, T(v_n)\}$ adalah basis untuk W atas $\mathbb{F}$ maka T adalah isomorpisma.

(b) Jika T adalah isomorpisma, maka untuk sebarang basis $\{v_1, \ldots, v_n\}$ dari V atas $\mathbb{F}$ himpunan $\{T(v_1), \ldots, T(v_n)\}$ adalah basis untuk W atas $\mathbb{F}$.

29. Dua ruang vektor berdimensi hingga V dan W atas lapangan yang sama $\mathbb{F}$ adalah **isomorpik** jika terdapat isomorpisma dari V ke W. Tunjukkan bahwa dua ruang vektor berdimensi hingga pada lapangan yang sama $\mathbb{F}$ isomorpik jika dan hanya jika memiliki dimensi yang sama.

30. Misalkan V dan W adalah suatu ruang vektor atas lapangan yang sama $\mathbb{F}$. Misalkan $\dim_{\mathbb{F}} V = n$ dan misalkan $T : V \to W$ merupakan transformasi linier. Tunjukkan bahw

$$\dim_{\mathbb{F}} \ker(T) + \dim_{\mathbb{F}} \mathrm{Im}(T) = n.$$

10.2 Perluasan Aljabar

Pertanyaan paling mendasar dalam studi polinomial adalah menemukan **akar-akar**nya. Pada bagian ini pertama-tama kita tunjukkan bahwa setiap polinomial dengan koefisien di sembarang lapangan $\mathbb{F}$ selalu memiliki **akar-akar**, meskipun tidak harus di $\mathbb{F}$. Maka kita mempelajari struktur dari lapangan terkecil yang memuat $\mathbb{F}$ dan **akar-akar** dari polinomial yang diberikan. Di sinilah pengertian **ruang vektor**, **basis**, dan **dimensi** berperan. Dalam Bagian 8.7 kita mulai mempelajari contoh-contoh ring pecahan dari ring polinomial $\mathbb{F}[x]$. Pada bagian ini kita melanjutkan studi tentang ring pecahan dan melengkapi pembahasan dengan menunjukkan bahwa ring pecahan ini memberi kita lapangan yang berisi akar-akar dari polinomial yang diberikan.

Contoh 10.2.1 (2) Polinomial $x^2 - 2 \in \mathbb{Q}[xl$ tidak memiliki akar di $\mathbb{Q}$ tetapi memiliki akar $\sqrt{2}$ di $\mathbb{R}$. Namun, ada sublapangan yang lebih kecil dari $\mathbb{R}$ yang memuat $\mathbb{Q}$ serta akar ini yaitu $Q(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in Q\}$.
(2) Polinomial $x^2 + 1$ tidak memiliki akar di $\mathbb{R}$ tetapi memiliki akar i di $\mathbb{C}$. Dalam hal ini tidak ada sublapangan yang lebih kecil dari $\mathbb{C}$ yang memuat $\mathbb{R}$ dan i, karena kita telah memiliki $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$. ●

Proposisi pertama kita menjamin, untuk sebarang lapangan $\mathbb{F}$ dan polinomial tak nol $f(x) \in \mathbb{F}[x]$, bahwa jika kita dapat menemukan lapangan $\mathbb{E}$ di mana $\mathbb{F}$ adalah sublapangan yang berisi elemen α yang merupakan akar dari $f(x)$ maka akan ada sublapangan terkecil dari $\mathbb{E}$ yang memuat $\mathbb{F}$ dan α. Kemudian kita beralih ke pertanyaan menemukan lapangan seperti $\mathbb{E}$ ini.

Proposisi 10.2.1 Misalkankan $\mathbb{E}$ adalah suatu lapangan, $\mathbb{F} \subseteq \mathbb{E}$ sublapangan dari $\mathbb{E}$, dan $\alpha \in \mathbb{E}$ elemen di $\mathbb{E}$. Dalam $\mathbb{E}$ misalkan

$$\mathbb{F}[\alpha] = \{f(\alpha) \mid f(x) \in \mathbb{F}[x]\},$$

$$\mathbb{F}(\alpha) = \{f(\alpha)/g(\alpha) \mid f(x), g(x) \in \mathbb{F}[x], g(\alpha) \neq 0\}.$$

Maka

(1) $\mathbb{F}[\alpha]$ adalah suatu subring dari $\mathbb{E}$ yang memuat $\mathbb{F}$ and α.

(2) $\mathbb{F}[\alpha]$ adalah subring terkecil dari $\mathbb{E}$.

(3) $\mathbb{F}(\alpha)$ adalah sublapangan dari $\mathbb{E}$ yang memuat $\mathbb{F}$ dan α.

(4) $\mathbb{F}(\alpha)$ adalah sublapangan terkecil dari $\mathbb{E}$.

Bukti

(1) $\mathbb{F}[\alpha]$ memuat setiap elemen $a \in \mathbb{F}$, karena $a = f(\alpha)$, dimana $f(x)$ adalah polinomial konstanta $f(x) = a \in \mathbb{F}[x]$. Perhatikan bahwa $\mathbb{F}[\alpha]$ memuat α, karena $\alpha = f(\alpha)$ di mana $f(x)$ adalah polinomial $f(x) = x \in \mathbb{F}[x]$. Pertimbangkan sekarang dua elemen $f_1(\alpha), f_2(\alpha) \in \mathbb{F}[\alpha]$, dimana $f_1(x), f_2(x) \in \mathbb{F}[x]$. Maka $f_1(\alpha) - f_2(\alpha) = g(\alpha) \in \mathbb{F}[\alpha]$ dan $f_1(\alpha)f_2(\alpha) = h(\alpha) \in \mathbb{F}[\alpha]$, dimana $g(x) = f_1(x) - f_2(x) \in \mathbb{F}[x]$ dan $h(x) = f_1(x)f_2(x) \in \mathbb{F}[x]$. Dengan pengujian subring, maka $F[\alpha]$ adalah subring dari $\mathbb{E}$.

(2) Apa yang akan kita tunjukkan adalah bahwa jika R adalah subring dari $\mathbb{E}$ dengan $\mathbb{F} \subseteq R$ dan $\alpha \in R$, maka $\mathbb{F}[\alpha] \subseteq R$. Tetapi sebarang subring R dari $\mathbb{E}$ akan berisi pangkat α^i dari α dan kombinasi linear $a_0 + a_1\alpha + \cdots + a_n\alpha^n$ dari pangkat tersebut, dimana $a_i \in \mathbb{F}$. Dan setiap elemen $f(\alpha) \in \mathbb{F}[\alpha]$ dimana

$$f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{F}[x]$$

adalah suatu kombinasi linier.

(3) dan **(4)** langsung dari **(1)** dan **(2)**, karena $\mathbb{F}[\alpha] \subseteq \mathbb{E}$ dan $\mathbb{E}$ adalah lapangan, maka $\mathbb{F}[\alpha]$ adalah daerah integral, dengan demikian $\mathbb{F}(\alpha)$ merupakan lapangan pecahan dari daerah integral $\mathbb{F}[\alpha]$. ✓

Perhatikan bahwa jika $\mathbb{F}[\alpha]$ sudah merupakan suatu lapangan, maka $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$. Ini terjadi dalam kedua kasus dalam Contoh 10.2.1, dimana

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},$$

$$\mathbb{R}(i) = \mathbb{R}[i] = \{a + bi \mid a, b \in \mathbb{R}\} = \mathbb{C}.$$

Definisi 10.2.1 Misalkan $\mathbb{F}$ dan $\mathbb{E}$ adalah lapangan. Maka, jika $\mathbb{F} \subseteq \mathbb{E}$ dan $\mathbb{F}$ adalah sublapangan dari $\mathbb{E}$ kita juga mengatakan bahwa $\mathbb{E}$ adalah **perluasan** dari $\mathbb{F}$. Perluasan lapangan $\mathbb{F}(\alpha)$ pada Proposisi 10.2.1 adalah dikatakan diperoleh dengan **menghubungkan** α ke $\mathbb{F}$, dan notasi $\mathbb{F}(\alpha)$ dibaca "$\mathbb{F}$ menghubungkan α." ✓

Kita sekarang beralih ke pertanyaan tentang keberadaan lapangan perluasan yang berisi akar dari suatu polinomial.

Contoh 10.2.2 Pertimbangkan $f(x) = x^3 + x + 1 \in \mathbb{Q}[x]$. Dengan Teorema 8.4.3 dan 8.4.4, $f(x)$ tak-tereduksi atas $\mathbb{Q}$. Kita dapat mencari nol dari $f(x)$ dalam $\mathbb{R}$ menggunakan metode Bagian 8.5, karena $f(x)$ adalah polinomial kubik. Tetapi metode Bagian 8.7 memberikan cara yang berbeda untuk mendapatkan lapangan perluasan $\mathbb{Q}$ yang memuat akar dari $f(x)$, yang berfungsi lebih umum daripada hanya untuk polinomial kubik.

Mari kita tinjau metode-metode tersebut. Karena $f(x)$ tak-tereduksi di $\mathbb{Q}$, maka $I = \langle f(x) \rangle$ adalah ideal maksimal menurut Teorema 8.6.2, dan $\mathbb{E} = \mathbb{Q}[x]/I$ adalah suatu lapangan.

Elemen $\mathbb{E}$ dapat ditulis sebagai koset dari I. Ingat bahwa I adalah elemen nol dalam $\mathbb{E}$ dan bahwa $1 + I$ adalah elemen satuan di $\mathbb{E}$. Sekarang perhatikan elemen di $\mathbb{E}$ berikut

$$\alpha = x + I$$

Karena I adalah ideal, maka $\alpha^2 = (x + I)(x + I) = x^2 + I$ dan $\alpha^3 = x^3 + I$. Oleh karena itu dalam lapangan $\mathbb{E}$

$$\alpha^3 + \alpha + 1 = (x^3 + I) + (x + I) + (1 + I) = (x^3 + x + 1) + I.$$

Tetapi karena $I = \langle x^3 + x + 1 \rangle$, maka $\alpha^3 + \alpha + 1 = 0$ di $\mathbb{E}$. Dengan kata lain, $f(\alpha) = 0$, dan lapangan $\mathbb{E}$ berisi akar dari polinomial $f(x) = x^3 + x + 1$, yaitu α. Perhatikan juga bahwa himpunan elemen $\{c + I \mid c \in \mathbb{Q}\}$ membentuk suatu sublapangan dari $\mathbb{E}$ isomorpik dengan $\mathbb{Q}$, sehingga kita dapat menganggap $\mathbb{E}$ sebagai perluasan lapangan dari $\mathbb{Q}$. ●

Teorema 10.2.1 ***(Kronecker)*** Misalkan $\mathbb{F}$ adalah suatu lapangan dan $p(x)$ polinomial bukan konstan di $\mathbb{F}[x]$. Maka ada suatu lapangan $\mathbb{E}$ dan elemen α di $\mathbb{E}$ sedemikian rupa sehingga $\mathbb{E}$ adalah suatu lapangan perluasan dari $\mathbb{F}$ dan α adalah suatu akar dari $p(x)$.

Bukti
Pertama, pertimbangkan kasus khusus dimana $p(x)$ tak-tereduksi atas $\mathbb{F}$. Maka dengan Teorema 8.6.2, $I = \langle p(x) \rangle$ adalah ideal maksimal dalam $\mathbb{F}[x]$, juga berdasarkan Teorema 8.6.2, maka $\mathbb{E} = \mathbb{F}[x]/I$ adalah suatu lapangan.

Kita pertama-tama mengklaim bahwa $\mathbb{F}' = \{c + I \mid c \in \mathbb{F}\}$ adalah sublapangan dari $\mathbb{E}$ isomorpik dengan $\mathbb{F}$. Karena I adalah ideal dalam $\mathbb{F}[x]$ untuk sebarang $c + I$ dan $d + I$ di $\mathbb{F}'$, kita memiliki

$$(c + I) - (d + I) = (c - d) + I$$

dan jika $d \neq 0$ di $\mathbb{F}$, maka

$$\begin{aligned} (d + I)^{-1} &= d^{-1} + I \\ (c + I)(d + I)^{-1} &= cd^{-1} + I. \end{aligned}$$

Oleh karena itu dengan pengujian sublapangan (Teorema 6.3.6), $\mathbb{F}'$ adalah suatu sublapangan dari $\mathbb{E}$. Pemetaan natural sebagaimana diketahui $\phi : \mathbb{F} \to \mathbb{F}'$ yang didefinisikan oleh $\phi(c) = c + I$ untuk semua $c \in \mathbb{F}$ adalah suatu isomorpisma. Jika kita mengidentifikasi $c \in \mathbb{F}$ dan $\phi(c) = +I$, kita dapat menganggap $\mathbb{E}$ sebagai suatu lapangan perluasan dari $\mathbb{F}$. Kita sekarang menunjukkan bahwa $\mathbb{E}$ memuat akar dari $p(x)$. Karena I adalah ideal dalam $\mathbb{F}[x]$ kita memiliki

$$\begin{aligned} (x + I)^i &= x^i + I \\ c(x^i + I) &= (c + I)(x^i + I) = cx^i + I \end{aligned}$$

dan lebih umum untuk sebarang polinomial

$$f(x) = c_0 + c_1 x + \cdots + c_m x^m \in \mathbb{F}[x]$$

kita mempunyai

$$\begin{aligned} f(x + I) &= c_0 + c_1(x + I) + \cdots + c_m(x^m + I) \\ &= (c_0 + c_1 x + \cdots + c_m x^m) + I \\ &= f(x) + I. \end{aligned}$$

Jadi jika kita menulis α untuk $x + I$, maka, khususnya, kita memiliki

$$p(\alpha) = p(x + I) = p(x) + I = I = 0 \text{ di } \mathbb{E}.$$

Jadi α adalah akar dari $p(x)$. Selain itu, setiap elemen $\mathbb{E}$ berbentuk $f(x) + I = f(\alpha)$ untuk beberapa $f(x) \in \mathbb{F}[x]$ sehingga dalam notasi Proposisi 10.2.1 kita memiliki $\mathbb{E} = \mathbb{F}[\alpha] = \mathbb{F}(\alpha)$. Kita telah menggunakan konstruksi ring kuasi untuk **menghubungkan** akar α dari polinomial tak-tereduksi $p(x)$ ke $\mathbb{F}$. Ini melengkapi bukti dalam kasus khusus di mana $p(x)$ tak-tereduksi. Dalam kasus umum dimana $p(x)$ tidak perlu tak-tereduksi, cukup terapkan kasus khusus ini ke faktor-faktor tak-tereduksi dari $p(x)$. ✓

Contoh 10.2.3 Pertimbangkan $p(x) = x^2 + 1 \in \mathbb{R}[x]$. Misalkan $\phi : \mathbb{R}[x] \to \mathbb{C}$ adalah suatu evaluasi homomorpisma $\phi(f(x)) = f(i)$ untuk semua $f(x) \in \mathbb{R}[x]$. Untuk sebarang bilangan kompleks $a + bi \in \mathbb{C}$ kita memiliki $a + bi = \phi(a + bx)$ dengan $a + bx \in \mathbb{R}[x]$· Oleh karena itu ϕ adalah **pada**. Selanjutnya, $\ker(\phi) = \{f(x) \in \mathbb{R}[x] \mid \phi(f(x)) = 0\}$. Jadi, $p(x) = x^2 + 1 \in \ker(\phi)$ dan

$$I = \langle p(x)\rangle \subseteq \ker(\phi) \subseteq \mathbb{R}[x].$$

Karena $I = \langle p(x)\rangle$ adalah ideal maksimal dalam $\mathbb{R}[x]$ maka salah satu $\ker(\phi) = \mathbb{R}[x]$ atau $\ker(\phi) = I = \langle p(x)\rangle$. Karena $\phi(1) = 1$, maka ϕ bukan pemetaan homomorpisma nol, dan $\ker(\phi) \neq \mathbb{R}[x]$. Dengan demikian haruslah $\ker(\phi) = I = \langle p(x)\rangle$. Dengan menggunakan teorema isomorpisma pertama untuk ring (Teorema 7.2.17) kita memiliki

$$\mathbb{R}[x]/\langle x^2 + 1\rangle \cong \mathbb{C} = \mathbb{R}(i).$$

Di bawah isomorpisma ini kita memiliki yang berikut:

$$\begin{aligned} I &\leftrightarrow 0, \\ x + I &\leftrightarrow i, \\ a + I &\leftrightarrow a \in \mathbb{R}, \\ (a + bx) + I &\leftrightarrow a + bi \in \mathbb{C}, \end{aligned}$$

yang sepenuhnya menggambarkan hubungan timbal balik antar elemen-elemen dari $\mathbb{R}[x]/I$ ke $\mathbb{C} = \mathbb{R}(i)$. ●

Contoh 10.2.4 Pertimbangkan bilangan kompleks $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$, yang telah kita temui beberapa kali. Ini adalah salah satu akar ketiga dari bilangan-bilangan komplek yang terletak pada lingkaran dengan jari-jari satu atau ekivalen dengan akar dari $x^3 - 1$. Dalam $\mathbb{Q}[x]$ kita memiliki faktorisasi $x^3 - 1 = (x - 1)(x^2 + x + 1)$, dan ω adalah akar dari faktor tak-tereduksi $(x^2 + x + 1)$. Misalkan $\phi : \mathbb{Q}[x] \to \mathbb{C}$ adalah suatu homomorpisma evaluasi $\phi(f(x)) = f(\omega)$. Maka ***image*** dari ϕ

$$\text{Im}(\phi) = \{f(\omega) \mid f(x) \in \mathbb{Q}[x]\} = \mathbb{Q}[\omega]$$

sebagaimana didefinisikan dalam Proposisi 10.2.1. Mari kita tentukan kernel dari ϕ. Karena ω adalah akar dari $x^2 + x + 1$, kita memiliki $x^2 + x + 1 \in \ker(\phi)$ dan oleh karena itu $\langle x^2 + x + 1\rangle \subseteq \ker(\phi)$. Karena $x^2 + x + 1$ tak-tereduksi pada $\mathbb{Q}$, $\langle x^2 + x + 1\rangle$ ideal adalah ideal maksimal dalam $\mathbb{Q}[x]$. Oleh karena itu, $\ker(\phi) = \mathbb{Q}[x]$ atau $\ker(\phi) = \langle x^2 + x + 1\rangle$. Sekarang karena $\phi(1) = 1$, maka ϕ bukan pemetaan homomorpisma nol, maka $\ker(\phi) \neq \mathbb{Q}[x]$. Oleh karena itu, $\ker(\phi) = \langle x^2 + x + 1\rangle$.

Sekarang mari kita perhatikan *image* dari ϕ. Dengan teorema isomorpisma pertama untuk ring kita mempunyai

$$\text{Im}(\phi) \cong \mathbb{Q}[x]/\langle x^2 + x + 1\rangle.$$

Karena ideal $\langle x^2 + x + 1\rangle$ adalah maksimal, maka $\mathbb{Q}[x]/\langle x^2 + x + 1\rangle$ adalah suatu lapangan, dan $\text{Im}(\phi) = \mathbb{Q}[\omega]$ adalah suatu lapangan. Jadi $\text{Im}(\phi) = \mathbb{Q}[\omega] = \mathbb{Q}(\omega)$ dan kita memiliki

$$\mathbb{Q}(\omega) \cong \mathbb{Q}[x]/\langle x^2 + x + 1\rangle.$$

Kita dapat melanjutkan untuk memberikan deskripsi yang lebih eksplisit tentang elemen $\mathbb{Q}(\omega)$. Setiap elemen tersebut adalah kombinasi linier

$$c_0 + c_1\omega + \cdots + c_m\omega^m$$

atas $\mathbb{Q}$ dari pangkat ω, dimana

$$c_0 + c_1x + \cdots + c_mx^m \in \mathbb{Q}[x].$$

Tetapi karena ω adalah akar dari $x^2 + x + 1$ dan akar dari pangkat tiga lingkaran satuan, kita dapatkan

$$\begin{aligned} \omega^2 &= -1 - \omega \\ \omega^3 &= 1 \\ \omega^4 &= \omega \\ &\vdots \end{aligned}$$

Jadi setiap pangkat ω adalah kombinasi linier dari 1 dan ω atas $\mathbb{Q}$. Karenanya setiap elemen $\mathbb{Q}(\omega)$ adalah kombinasi linier tsb. dan

$$\mathbb{Q}(\omega) = \{a + b\omega \mid a, b \in \mathbb{Q}\}.$$

Perhatikan bahwa kita memiliki

$$\begin{aligned} (a + b\omega)(c + d\omega) &= ac + (bc + ad)\omega + bd\omega^2 \\ &= ac + (bc + ad)\omega + bd(-1 - \omega) \\ &= (ac - bd) + (bc + ad - bd)\omega \end{aligned}$$

sebagai aturan untuk hasil perkalian di $\mathbb{Q}(\omega)$. ●

Definisi 10.2.2 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $\mathbb{E}$ lapangan perluasan dengan $\mathbb{F} \subseteq \mathbb{E}$. Maka suatu elemen $\alpha \in \mathbb{E}$ dikatakan **aljabar** atas $\mathbb{F}$ jika terdapat polinomial bukan-nol $0 \neq f(x) \in \mathbb{F}[x]$ yang memenuhi $f(\alpha) = 0$. Jika tidak, α dikatakan **transendental** atas $\mathbb{F}$. ✓

Teorema 10.2.2 Misalkan $\mathbb{F} \subseteq \mathbb{F}$ adalah lapangan, dan misalkan $\alpha \in \mathbb{E}$ adalah aljabar atas $\mathbb{F}$. Maka terdapat tunggal polinomial monik $p(x) \in \mathbb{F}[x]$ sedemikian sehingga

(1) $p(\alpha) = 0$,

(2) $p(x)$ tak-tereduksi atas $\mathbb{F}$.

(3) Jika $f(x) \in \mathbb{F}[x]$ sedemikian rupa sehingga $f(\alpha) = 0$, maka $p(x)$ membagi $f(x)$.

Bukti
Pertimbangkan $I = \{f(x) \in \mathbb{F}[x] \mid f(\alpha) = 0\}$. Maka I adalah ideal sejati di $\mathbb{F}[x]$. Oleh karena itu dengan Teorema 8.6.1, $I = \langle p(x) \rangle \subset F[x]$, dimana $p(x)$ adalah derajat minimal dalam I. Kita juga dapat memilih $p(x)$ untuk menjadi monik dengan mengalikannya dengan unit yang sesuai. Selanjutnya kita tunjukkan bahwa $p(x)$ tak-tereduksi. Misalkan $p(x) = g(x)h(x)$. Maka $g(\alpha)h(\alpha) = p(\alpha) = 0$. Oleh karena itu $g(\alpha) = 0$ atau $h(\alpha) = 0$, dan $g(x) \in I$ atau $h(x) \in I$. Karena $p(x)$ memiliki derajat minimal dalam I, faktor mana pun yang $g(x)$ atau $h(x)$ termasuk dalam I harus merupakan kelipatan unit dari $p(x)$ dan faktor lain harus berupa unit, seperti yang diperlukan untuk menunjukkan $p(x)$ tidak dapat direduksi. Ini membuktikan sifat (2) dari teorema, dan sifat (1) dan (3) langsung dari definisi I. Terakhir, untuk membuktikan ketunggalan, misalkan $q(x)$ adalah polinomial monik lainnya yang memenuhi sifat (1) sampai (3). Maka dengan sifat (3) kita memiliki $p(x) \mid q(x)$ dan $q(x) \mid p(x)$. Oleh karena itu $q(x) = up(x)$ untuk beberapa unit u. Tetapi karena $p(x)$ dan $q(x)$ keduanya monik, kita harus memiliki $u = 1$ dan $q(x) = p(x)$. ✓

Keberadaan polinomial tak-tereduksi $p(x)$ untuk setiap elemen aljabar α membantu kita memahami perluasan lapangan $\mathbb{F}(\alpha)$.

Definisi 10.2.3 Misalkan $\mathbb{F} \subseteq \mathbb{E}$ adalah lapangan dan misalkan $\alpha \in \mathbb{E}$ adalah aljabar atas $\mathbb{F}$. Maka polinomial tunggal tak-tereduksi monik $p(x) \in \mathbb{F}[x]$ sedemikian hingga $p(\alpha) = 0$ disebut **polinomial minimal** dari α atas $\mathbb{F}$. **Derajat** α **atas** $\mathbb{F}$ didefinisikan sebagai derajat polinomial minimal $p(x)$ dan ditulis sebagai $\deg_{\mathbb{F}}(\alpha)$. ✓

Perhatikan bahwa $a \in \mathbb{F}$ dihitung sebagai aljabar atas $\mathbb{F}$ derajat 1, polinomial minimal dalam hal ini adalah polinomial linier $p(x) = x - a$. Contoh 10.2.3 menunjukkan bahwa i adalah aljabar atas $\mathbb{R}$ dan $\deg_{\mathbb{R}}(i) = 2$. Contoh 10.2.4 menunjukkan bahwa ω adalah aljabar atas $\mathbb{Q}$ dan $\deg_{\mathbb{Q}}(\omega) = 2$. Kedua contoh ini menggambarkan teorema dasar berikut.

Teorema 10.2.3 Misalkan $\mathbb{F} \subseteq \mathbb{E}$ adalah lapangan, misalkan $\alpha \in \mathbb{E}$ adalah aljabar atas $\mathbb{F}$ dengan $\deg_{\mathbb{F}}(\alpha) = n$, dan $p(x)$ adalah polinomial minimal dari α atas $\mathbb{F}$. Maka

(1) $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/\langle p(x) \rangle$.

(2) $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ adalah basis untuk ruang vektor $\mathbb{F}(\alpha)$ atas $\mathbb{F}$.

(3) $\dim_{\mathbb{F}} \mathbb{F}(\alpha) = \deg_{\mathbb{F}}(\alpha) = \deg p(x)$.

Bukti

(1) Pertimbangkan evaluasi homomorpisma $\phi : \mathbb{F}[x] \to \mathbb{E}$ yang didefinisikan oleh $\phi(f(x)) = f(\alpha)$. $\text{Im}(\phi) = \{f(\alpha) \mid f(x) \in \mathbb{F}[x]\} = \mathbb{F}[\alpha]$ seperti yang didefinisikan dalam Proposisi 10.2.1. $\ker(\phi) = \{f(x) \in \mathbb{F}[x] \mid f(\alpha) = 0\}$. Berdasarkan Teorema 10.2.2, bagian (1), $p(\alpha) = 0$ dan $f(\alpha) = 0$ untuk $f(x) \in \mathbb{F}[x]$ sehingga $p(x)$ membagi $f(x)$ dan dengan Teorema 10.2.2, bagian (3), jika $f(x) \in \mathbb{F}[x]$ dan $f(\alpha) = 0$, maka $p(x)$ membagi $f(x)$. Jadi

$$\ker(\phi) = \{f(x) \in \mathbb{F}[x] \mid p(x) \text{ membagi } f(x)\} = \langle p(x) \rangle.$$

Berdasarkan Teorema 10.2.2, bagian (2), $p(x)$ tak-tereduksi dan karenanya $\langle p(x)\rangle$ adalah ideal maksimal dengan demikian $\mathbb{F}[x]/\langle p(x)\rangle$ adalah suatu lapangan. Selanjutnya, dengan teorema isomorpisma pertama kita mempunyai

$$\text{Im}(\phi) \cong \mathbb{F}[x]/\langle p(x)\rangle.$$

Jadi $\text{Im}(\phi) = \mathbb{F}[\alpha]$ adalah lapangan, dan $\text{Im}(\phi) = \mathbb{F}[\alpha] = \mathbb{F}(\alpha)$, dengan demikian **(1)** terbukti.

(2) Pertimbangkan $S = \text{span}_{\mathbb{F}}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Kita melihat dalam bukti (1) bahwa

$$\mathbb{F}(\alpha) = \mathbb{F}[\alpha] = \{f(\alpha) \mid f(x) \in \mathbb{F}[x]\}.$$

Jadi $\mathbb{F}(\alpha)$ terdiri dari semua elemen bentuk

$$a_m\alpha^m + \cdots + a_2\alpha^2 + a_1\alpha + a_0$$

atau, dengan kata lain, semua kombinasi linier dari pangkat α atas $\mathbb{F}$. Karena setiap elemen S adalah kombinasi linier yang semacam itu (dengan $m < n$), kita memiliki $S \subseteq \mathbb{F}(\alpha)$. Untuk inklusi yang sebaliknya, misalkan polinomial minimal $p(x)$ adalah

$$p(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_2x^2 + b_1x + b_0.$$

Karena $p(\alpha) = 0$, kita mempunyai

$$\alpha^n = (-b_0) + (-b_1)\alpha + (-b_2)\alpha^2 + \cdots + (-b_{n-1})\alpha^{n-1} \in S.$$

Ini menunjukkan bahwa α^n adalah kombinasi linier dari α^i untuk $i < n$, dan termuat dalam S. Sehingga kita mempunyai yang berikut ini

$$\begin{aligned}
\alpha^{n+1} &= \alpha \cdot \alpha^n \\
&= (-b_0)\alpha + (-b_1)\alpha^2 + \cdots + (-b_{n-1})\alpha^n \\
&= (-b_0)\alpha + (-b_1)\alpha^2 + \cdots + (-b_{n-1})\left((-b_0) + (-b_1)\alpha + (-b_2)\alpha^2 + \cdots + (-b_{n-1})\alpha^{n-1}\right) \\
&= (b_{n-1}b_0) + (b_{n-1}b_1 - b_0)\alpha + (b_{n-1}b_2 - b_1)\alpha^2 + \cdots + (b_{n-1}^2 - b_{n-2})\alpha^{n-1} \in S
\end{aligned}$$

dan ini menunjukkan bahwa α^{n+1} adalah kombinasi linier dari elemen-elemen S dan juga termuat di S. Dengan melanjutkan cara ini, setiap pangkat dari α adalah termuat di S, demikian juga setiap kombinasi linear pangkat dari α. Ini menunjukkan bahwa $\mathbb{F}(\alpha) \subseteq S$. Jadi

$$\text{span}_{\mathbb{F}}\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\} = \mathbb{F}(\alpha).$$

Di sisi lain, jika ada elemen $d_i \in \mathbb{F}$ sedemikian rupa sehingga

$$d_0 + d_1\alpha + d_2\alpha^2 + \cdots + d_{n-1}\alpha^{n-1} = 0$$

maka

$$g(x) = d_0 + d_1x + d_2x^2 + \cdots + d_{n-1}x^{n-1} \in \mathbb{F}[x]$$

adalah polinomial dengan $\deg g(x) \leq n - 1 < n = \deg p(x)$ dan $g(\alpha) = 0$. Menurut Teorema 10.2.2, bagian (3), maka $p(x)$ membagi $g(x)$ ini tidak mungkin kecuali semua $d_i = 0$. Ini menunjukkan bahwa himpunan $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ bebas linier, dan kita telah membuktikan **(2)**.

(3) Mengikuti langsung dari **(2)**.

Contoh 10.2.5 (1) $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}\left(5^{\frac{1}{2}}\right)$ adalah suatu lapangan perluasan dari $\mathbb{Q}$ dan juga ruang vektor atas $\mathbb{Q}$ dengan basis $\left\{1, 5^{\frac{1}{2}}\right\}$. Setiap elemen $\mathbb{Q}\left(5^{\frac{1}{2}}\right)$ berbentuk $c_0 + c_1 5^{\frac{1}{2}}$ untuk beberapa $c_i \in \mathbb{Q}$.
(2) Begitu juga $\mathbb{Q}\left(2^{\frac{2}{3}}\right)$ adalah suatu lapangan perluasan dari $\mathbb{Q}$ dan merupakan ruang vektor atas $\mathbb{Q}$ dengan basis $\left\{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}\right\}$. Setiap elemen $\mathbb{Q}\left(2^{\frac{2}{3}}\right)$ berbentuk $c_0 + c_1 2^{\frac{1}{3}} + c_2 2^{\frac{2}{3}}$ untuk beberapa $c_i \in \mathbb{Q}$.

Contoh 10.2.6 Kita dapat dengan mudah melihat bahwa $3^{\frac{1}{5}}$ adalah elemen aljabar atas $\mathbb{Q}$ karena $3^{\frac{1}{5}}$ adalah suatu akar dari $x^5 - 3 \in \mathbb{Q}[x]$. Dengan **kriteria *Eisenstein***, $x^5 - 3$ takтereduksi atas $\mathbb{Q}$. Jadi $3^{\frac{1}{5}}$ adalah elemen aljabar derajat lima. Sekarang perhatikan beberapa elemen dari $\mathbb{Q}\left(3^{\frac{1}{5}}\right)$, misalnya

$$\alpha = 3^{\frac{1}{5}} - 4 \cdot 3^{\frac{2}{5}} + 7 \cdot 3^{\frac{3}{5}}.$$

Apakah α elemen aljabar atas $\mathbb{Q}$? Kita dapat mencoba menunjukkan bahwa itu adalah dengan menghitung berbagai pangkat dan mencoba berbagai kombinasi linier dari pangkat ini untuk melihat apakah kita bisa mendapatkan akar dari $x^5 - 3 \in \mathbb{Q}[x]$. Apapun hal ini, teorema kita berikutnya segera menyiratkan bahwa α adalah elemen aljabar, tanpa kita harus melakukan perhitungan seperti itu.

Sebelum kita dapat menyajikan teorema berikutnya, kita perlu beberapa definisi.

Definisi 10.2.4 Misalkan $\mathbb{E}$ adalah suatu lapangan perluasan dari suatu lapangan $\mathbb{F}$. Maka

(1) $\mathbb{E}$ dikatakan sebagai **perluasan aljabar** dari $\mathbb{F}$ jika setiap elemen $\alpha \in \mathbb{E}$ aljabar atas $\mathbb{F}$.

(2) $\mathbb{E}$ dikatakan sebagai **perluasan berhingga** dari $\mathbb{F}$ jika $\mathbb{E}$ adalah ruang vektor berdimensi hingga atas $\mathbb{F}$. Dalam hal ini, kita menyatakan dimensi n dari $\mathbb{E}$ atas $\mathbb{F}$ dengan $[\mathbb{E} : \mathbb{F}] = n$ dan kita menyebut n sebagai **derajat** dari $\mathbb{E}$ atas $\mathbb{F}$.

Contoh 10.2.7
(1) $\left[\mathbb{Q}\left(2^{\frac{1}{3}}\right) : \mathbb{Q}\right] = 3$,
(2) $[\mathbb{C} : \mathbb{R}] = 2$,
(3) $[\mathbb{F} : \mathbb{F}] = 1$, untuk sebarang lapangan $\mathbb{F}$,
(4) $[\mathbb{F}(\alpha) : \mathbb{F}] = \deg_{\mathbb{F}}(\alpha)$ menggunakan Teorema 10.2.3.

Teorema berikutnya menunjukkan bahwa dua jenis perluasan lapangan yang baru saja kita perkenalkan terkait erat.

Teorema 10.2.4 Misalkan $\mathbb{E}$ adalah suatu perluasan berhingga dari suatu lapangan $\mathbb{F}$. Maka

(1) $\mathbb{E}$ adalah suatu perluasan aljabar dari $\mathbb{F}$,

(2) $\deg_{\mathbb{F}}(\alpha) \leq [\mathbb{E} : \mathbb{F}]$ untuk setiap $\alpha \in \mathbb{E}$.

Bukti
Misalkan $\mathbb{E}$ adalah suatu perluasan berhingga dari $\mathbb{F}$ dengan $[\mathbb{E} : \mathbb{F}] = n$. Misalkan sebarang $\alpha \in \mathbb{E}$ dan pertimbangkan himpunan $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}, \alpha^n\}$. Karena banyaknya elemen himpunan ini adalah $n+1$ sedangkan $\mathbb{E}$ adalah ruang vektor berdimensi n atas $\mathbb{F}$, maka elemen-elemen ini harus bergantung secara linier dengan Teorema 10.1.3. Ini berarti ada $c_i \in \mathbb{F}$ tidak semuanya nol, sehingga

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1} + c_n\alpha^n = 0.$$

Maka

$$g(x) = c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1} + c_nx^n$$

adalah polinomial bukan nol $g(x) \in \mathbb{F}[x]$ dengan $g(\alpha) = 0$. Oleh karena itu α adalah elemen aljabar atas $\mathbb{F}$ dan $\deg_{\mathbb{F}}(\alpha) \leq \deg g(x) = n$. Karena ini berlaku untuk setiap elemen $\alpha \in \mathbb{E}$, maka $\mathbb{E}$ adalah suatu perluasan aljabar dari $\mathbb{F}$.

Contoh 10.2.8 Dengan Teorema 10.2.4, karena

$$\left[\mathbb{Q}\left(3^{\frac{1}{5}}\right) : \mathbb{Q}\right] = \deg_{\mathbb{Q}} 3^{\frac{1}{5}} = 5$$

elemen

$$\alpha = 3^{\frac{1}{5}} - 4 \cdot 3^{\frac{2}{5}} + 7 \cdot 3^{\frac{3}{5}} \in \mathbb{Q}\left(3^{\frac{1}{5}}\right)$$

disebutkan dalam Contoh 10.2.6 memang elemen aljabar atas $\mathbb{Q}$ berderajat ≤ 5.

Contoh 10.2.9 Polinomial $x^2 - 5$ tak-tereduksi atas $\mathbb{Q}$, akar kuadrat $5^{\frac{1}{2}}$ adalah elemen aljabar berderajat 2 atas $\mathbb{Q}$, dan $\mathbb{Q}(5^{\frac{1}{2}})$ adalah perluasan aljabar dari $\mathbb{Q}$ berderajat 2, dan $\{1, 5^{\frac{1}{2}}\}$ membentuk basis untuk $\mathbb{Q}(5^{\frac{1}{2}})$ atas $\mathbb{Q}$. Polinomial $x^3 - 2$ tak-tereduksi atas $\mathbb{Q}$, akar pangkat tiga $2^{\frac{1}{3}}$ adalah elemen aljabar bederajat 3 atas $\mathbb{Q}$, dan $\mathbb{Q}(2^{\frac{1}{3}})$ adalah perluasan aljabar dari $\mathbb{Q}$ berderajat 3, dan $\{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}\}$ membentuk basis untuk $\mathbb{Q}(2^{\frac{1}{3}})$ atas $\mathbb{Q}$. Sekarang perhatikan $\mathbb{Q}(5^{\frac{1}{2}}, 2^{\frac{1}{3}}) = (\mathbb{Q}(5^{\frac{1}{2}}))(2^{\frac{1}{3}})$, perluasan diperoleh dengan menghubungkan $2^{\frac{1}{3}}$ ke $\mathbb{Q}(5^{\frac{1}{2}})$. Karena setiap elemen $\mathbb{Q}(5^{\frac{1}{2}})$ berderajat ≤ 2 atas $\mathbb{Q}$, sedangkan $2^{\frac{1}{3}}$ berderajat 3 atas $\mathbb{Q}$, maka $2^{\frac{1}{3}} \notin \mathbb{Q}(5^{\frac{1}{2}})$. Oleh karena itu polinomial $x^3 - 2$ masih tak-tereduksi atas $\mathbb{Q}(5^{\frac{1}{2}})$, dan $\mathbb{Q}(5^{\frac{1}{2}}, 2^{\frac{1}{3}})$ adalah perluasan aljabar dari $\mathbb{Q}(5^{\frac{1}{2}})$ berderajat 3, dan $\{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}\}$ membentuk basis untuk $\mathbb{Q}(5^{\frac{1}{2}}, 2^{\frac{1}{3}})$ atas $\mathbb{Q}(5^{\frac{1}{2}})$. Suatu elemen dari $Q(5^{\frac{1}{2}}, 2^{\frac{1}{3}})$ memiliki bentuk

$$\alpha = c_0 + c_1 2^{\frac{1}{3}} + c_2 2^{\frac{2}{3}},$$

dimana $c_i \in \mathbb{Q}(5^{\frac{1}{2}})$, karena itu memiliki bentuk

$$c_0 = d_{0,0} + d_{0,1}5^{\frac{1}{2}} \quad c_1 = d_{1,0} + d_{1,1}5^{\frac{1}{2}} \quad c_2 = d_{2,0} + d_{2,1}5^{\frac{1}{2}}.$$

Jadi

$$\begin{aligned} \alpha &= (d_{0,0} + d_{0,1}5^{\frac{1}{2}}) + (d_{1,0} + d_{1,1}5^{\frac{1}{2}})2^{\frac{1}{3}} + (d_{2,0} + d_{2,1}5^{\frac{1}{2}})2^{\frac{2}{3}} \\ &= d_{0,0} + d_{0,1}5^{\frac{1}{2}} + d_{1,0}2^{\frac{1}{3}} + d_{1,1}5^{\frac{1}{2}}2^{\frac{1}{3}} + d_{2,0}2^{\frac{2}{3}} + d_{2,1}5^{\frac{1}{2}}2^{\frac{2}{3}}. \end{aligned}$$

Karena itu himpunan

$$S = \{1, 5^{\frac{1}{2}}, 2^{\frac{1}{3}}, 5^{\frac{1}{2}}2^{\frac{1}{3}}, 2^{\frac{2}{3}}, 5^{\frac{1}{2}}2^{\frac{2}{3}}\}$$

membentang $\mathbb{Q}(5^{\frac{1}{2}}, 2^{\frac{1}{3}})$ atas $\mathbb{Q}$. Himpunan S sebenarnya adalah basis, karena jika

$$b_{0,0} + b_{0,1}5^{\frac{1}{2}} + b_{1,0}2^{\frac{1}{3}} + b_{1,1}5^{\frac{1}{2}}2^{\frac{1}{3}} + b_{2,0}2^{\frac{2}{3}} + b_{2,1}5^{\frac{1}{2}}2^{\frac{2}{3}} = 0,$$

maka, karena $\{1, 2^{\frac{1}{3}}, 2^{\frac{2}{3}}\}$ adalah suatu basis untuk $\mathbb{Q}(5^{\frac{1}{2}})(2^{\frac{1}{3}})$ atas $\mathbb{Q}(5^{\frac{1}{2}})$, maka kita harus mempunyai

$$b_{0,0} + b_{0,1}5^{\frac{1}{2}} = 0, \quad b_{1,0} + b_{1,1}5^{\frac{1}{2}}, \quad b_{2,0} + b_{2,1}5^{\frac{1}{2}} = 0.$$

Karena $\{1, 5^{\frac{1}{2}}\}$ adalah suatu basis untuk $\mathbb{Q}(5^{\frac{1}{2}})$ atas $\mathbb{Q}$, maka kita harus mempunyai semua $b_{i,j} = 0$. Jadi

$$[\mathbb{Q}(5^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}] = 6 = 3 \cdot 2 = [\mathbb{Q}(5^{\frac{1}{2}}, 2^{\frac{1}{3}}) : \mathbb{Q}(2^{\frac{1}{3}})] \cdot [\mathbb{Q}(5^{\frac{1}{2}}) : \mathbb{Q}]$$

dan kita telah memperoleh basis untuk $\mathbb{Q}(5^{\frac{1}{2}}, 2^{\frac{1}{3}})$ atas $\mathbb{Q}$ melalui "menggandakan" suatu basis untuk $\mathbb{Q}(5^{\frac{1}{2}})$ atas $\mathbb{Q}$ dan suatu basis untuk $\mathbb{Q}(5^{\frac{1}{2}}, 2^{\frac{1}{3}})$ atas $\mathbb{Q}(5^{\frac{1}{2}})$. ●

Contoh 10.2.10 Polinomial $x^2 - 2$ tidak dapat direduksi pada $\mathbb{Q}$, akar kuadrat $2^{\frac{1}{2}}$ adalah elemen aljabar derajat 2 terhadap $\mathbb{Q}$, dan $\mathbb{Q}(2^{\frac{1}{2}})$ adalah perluasan aljabar dari $\mathbb{Q}$ derajat 2, dan $\{1, 2^{\frac{1}{2}}\}$ membentuk basis untuk $\mathbb{Q}(2^{\frac{1}{2}})$ atas $\mathbb{Q}$. Polinomial $x^4 - 2$ tak-tereduksi atas $\mathbb{Q}$, akar pangkat empat $2^{\frac{1}{4}}$ adalah elemen aljabar berderajat 4 atas $\mathbb{Q}$, dan $\mathbb{Q}(2^{\frac{1}{4}})$ adalah perluasan aljabar dari $\mathbb{Q}$ berderajat 4, dan $\{1, 2^{\frac{1}{4}}, 2^{\frac{2}{4}}, 2^{\frac{3}{4}}\}$ membentuk basis untuk $\mathbb{Q}(2^{\frac{1}{4}})$ atas $\mathbb{Q}$. Tetapi atas $\mathbb{Q}(2^{\frac{1}{2}})$ polinomial $x^4 - 2$ difaktorkan sebagai $(x^2 + 2^{\frac{1}{2}})(x^2 - 2^{\frac{1}{2}})$. Akar pangkat empat $2^{\frac{1}{4}}$ adalah akar dari faktor kedua $x^2 - 2^{\frac{1}{2}}$. Karena setiap elemen $\mathbb{Q}(2^{\frac{1}{2}})$ memiliki derajat ≤ 2 atas $\mathbb{Q}$, sedangkan $2^{\frac{1}{4}}$ adalah berderajat 4 atas $\mathbb{Q}$, jadi $2^{\frac{1}{4}} \notin \mathbb{Q}(2^{\frac{1}{2}})$. Oleh karena itu polinomial $x^2 - 2^{\frac{1}{2}}$ tak-tereduksi atas $\mathbb{Q}(2^{\frac{1}{2}})$, dan $2\ ^{frac14}$ adalah elemen aljabar berderajat 2 atas $\mathbb{Q}(2^{\frac{1}{2}})$. Karena $2^{\frac{1}{2}} = (2^{\frac{1}{4}})^2 \in \mathbb{Q}(2^{\frac{1}{4}})$, maka $\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{4}})$ perluasan yang diperoleh dengan menghubungkan $2^{\frac{1}{4}}$ ke $\mathbb{Q}(2^{\frac{1}{2}})$ adalah $\mathbb{Q}(2^{\frac{1}{4}})$. Perhatikan, bagaimanapun, bahwa kita masih memiliki hubungan

$$[\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{4}}) : \mathbb{Q}] = 4 = 2 \cdot 2 = [\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{4}}) : Q(2^{\frac{1}{2}})] \cdot [Q(2^{\frac{1}{2}}) : \mathbb{Q}],$$

Apalagi, karena

$$\{1, 2^{\frac{1}{4}}, 2^{\frac{2}{4}}, 2^{\frac{3}{4}}\} = \{1, 2^{\frac{1}{4}}, 2^{\frac{1}{2}}, 2^{\frac{1}{4}} \cdot 2^{\frac{1}{2}}\}$$

kita masih memperoleh basis untuk $\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{4}})$ atas $\mathbb{Q}$ ketika kita "menggandakan" basis untuk $Q(2^{\frac{1}{2}})$ atas $\mathbb{Q}$ dan basis untuk $\mathbb{Q}(2^{\frac{1}{2}}, 2^{\frac{1}{4}})$ atas $\mathbb{Q}(2^{\frac{1}{2}})$. ●

Teorema 10.2.5 Misalkan $\mathbb{E}$ adalah suatu lapangan perluasan berhingga dari suatu lapangan $\mathbb{F}$ dan $\mathbb{K}$ suatu lapangan perluasan berhingga dari $\mathbb{E}$. Maka $\mathbb{K}$ adalah suatu lapangan perluasan berhingga dari $\mathbb{F}$ dan

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{F}].$$

Bukti
Kita memiliki $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$. Misalkan $[\mathbb{K} : \mathbb{E}] = m$ dan misalkan $\{v_1, \ldots, v_m\}$ adalah suatu basis untuk $\mathbb{K}$ atas $\mathbb{E}$. Misalkan $[\mathbb{E} : \mathbb{F}] = n$ dan $\{w_1, \ldots, w_n\}$ adalah suatu basis untuk $\mathbb{E}$ atas $\mathbb{F}$. Kita membuktikan teorema dengan membuktikan bahwa himpunan $m \cdot n$ elemen

$$\{v_i w_j \mid 1 \leq i \leq m,\ 1 \leq j \leq n\}$$

merupakan basis untuk $\mathbb{K}$ atas $\mathbb{F}$. Pertama kita tunjukkan bahwa $v_i w_j$ **membentang** $\mathbb{K}$ atas $\mathbb{F}$. Misalkan α adalah sebarang elemen di $\mathbb{K}$. Karena v_i **membentang** $\mathbb{K}$ atas $\mathbb{F}$, kita memiliki

$$\alpha = \beta_1 v_1 + \beta_1 v_1 + \beta_m v_m$$

untuk beberapa $\beta_i \in \mathbb{E}$. Karena w_j **membentang** $\mathbb{E}$ atas $\mathbb{F}$, kita memiliki

$$\begin{aligned} \beta_1 &= c_{1,1}w_1 + \cdots + c_{1,n}w_n \\ \beta_2 &= c_{2,1}w_1 + \cdots + c_{2,n}w_n \\ &\vdots \\ \beta_m &= c_{m,1}w_1 + \cdots + c_{m,n}w_n \end{aligned}$$

untuk beberapa $c_{i,j} \in \mathbb{F}$. Dari sini dapat disimpulkan bahwa

$$\begin{aligned} \alpha &= (c_{1,1}w_1 + \cdots + c_{1,n}w_n)v_1 + (c_{2,1}w_1 + \cdots + c_{2,n}w_n)v_2 + \cdots + (c_{m,1}w_1 + \cdots + c_{m,n}w_n)v_m \\ &= \sum_{i,j} c_{i,j}(v_i w_j) \in \text{span}\{v_i w_j \mid 1 \le i \le m,\ 1 \le j \le n\}. \end{aligned}$$

Jadi $v_i w_j$ membentang $\mathbb{K}$ atas $\mathbb{F}$. Selanjutnya kita tunjukkan bahwa $v_i w_j$ bebas linier atas $\mathbb{F}$. Misalkan kita punya

$$\sum_{i,j} d_{i,j}(v_i w_j) = 0$$

dimana $d_{i,j} \in \mathbb{F}$ untuk $1 \le i \le m$ dan $1 \le j \le n$. Maka

$$(d_{1,1}w_1 + \cdots + d_{1,n}w_n)v_1 + (d_{2,1}w_1 + \cdots + d_{2,n}w_n)v_2 + \cdots + (d_{m,1}w_1 + \cdots + d_{m,n}w_n)v_m = 0.$$

Karena v_i bebas linier atas $\mathbb{E}$ kita harus memiliki

$$\begin{aligned} d_{1,1}w_1 + \cdots + d_{1,n}w_n &= 0, \\ d_{2,1}w_1 + \cdots + d_{2,n}w_n &= 0, \\ &\vdots \\ d_{m,1}w_1 + \cdots + d_{m,n}w_n &= 0. \end{aligned}$$

Karena w_j bebas linier atas $\mathbb{F}$, kita harus memiliki $d_{i,j} = 0$ untuk semua i dan j.

Akibat 10.2.1 Misalkan

$$\mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq\subseteq \cdots \mathbb{F}_i \subseteq \mathbb{F}_r,$$

adalah lapangan dengan $[\mathbb{F}_{i+1} : \mathbb{F}_i] = n_{i+1},\ 1 \le i \le r-1$. Maka

$$[\mathbb{F}_r : \mathbb{F}_1] = n_2 n_3 \cdots n_r.$$

Bukti
Langsung dari Teorema 10.2.5.

Akibat 10.2.2 Misalkan $\mathbb{E}$ adalah suatu perluasan berhingga dari suatu lapangan $\mathbb{F}$ dan misalkan sebarang $\alpha \in \mathbb{E}$. Maka $\deg_{\mathbb{F}}(\alpha)$ membagi $[\mathbb{E} : \mathbb{F}]$.

Bukti
Kita memiliki $\mathbb{F} \subseteq \mathbb{F}(\alpha) \subseteq \mathbb{E}$. Dengan Kedimpulan 10.2.1, kita memiliki

$$[\mathbb{E} : \mathbb{F}] = [\mathbb{E} : F(\alpha)] \cdot [\mathbb{F}(\alpha) : \mathbb{F}] = [\mathbb{E} : F(\alpha)] \cdot \deg_{\mathbb{F}}(\alpha),$$

jadi $\deg_{\mathbb{F}}(\alpha) \mid [\mathbb{E} : \mathbb{F}]$ seperti yang diinginkan.

Definisi 10.2.5 Misalkan $\mathbb{F} \subseteq \mathbb{E}$ keduanya adalah lapangan dan $\alpha_1, \alpha_2, \ldots, \alpha_r$ adalah elemen-elemen di $\mathbb{E}$. Misalkan $\mathbb{F}_0 = \mathbb{F}$, dan $\mathbb{F}_{i+1} = \mathbb{F}_i(\alpha_{i+1})$ untuk $0 \leq i < r$. Maka kita menamakan $\mathbb{F}_r$ lapangan yang diperoleh dengan **menghubungkan secara berurutan** elemen-elemen $\alpha_1, \alpha_2, \ldots, \alpha_r$ di $\mathbb{E}$ ke $\mathbb{F}$, dan kita menulis $F(\alpha_1, \alpha_2, \ldots, \alpha_r)$ untuk $\mathbb{F}_r$.

Kita telah memperkenalkan notasi ini dalam kasus khusus $r = 2$ dalam Contoh 10.2.9 dan 10.2.10.

Akibat 10.2.3 Misalkan $\mathbb{F} \subseteq \mathbb{E}$ keduanya adalah lapangan, α dan β adalah elemen-elemen di $\mathbb{E}$ yang merupakan aljabar atas $\mathbb{F}$ dengan $\deg_{\mathbb{F}}(\alpha) = n$ dan $\deg_{\mathbb{F}}(\beta) = m$. Maka $[\mathbb{F}(\alpha, \beta) : \mathbb{F}] \leq n \cdot m$.

Bukti
Dengan Teorema 10.2.5 kita memiliki

$$[\mathbb{F}(\alpha, \beta) : \mathbb{F}] = [\mathbb{F}(\alpha, \beta) : \mathbb{F}(a)] \cdot [F(\alpha) : \mathbb{F}].$$

Dengan Teorema 10.2.3, kita memiliki

$$\begin{aligned} [\mathbb{F}(\alpha) : \mathbb{F}] &= \deg_{\mathbb{F}}(\alpha) \\ [\mathbb{F}(\alpha, \beta) : \mathbb{F}(\alpha)] &= \deg_{\mathbb{F}(\alpha)}(\beta). \end{aligned}$$

Tinggal menunjukkan bahwa $\deg_{\mathbb{F}(\alpha)}(\beta) \leq \deg_{\mathbb{F}}(\beta) = m$. Kita tahu bahwa β adalah akar dari suatu polinomial $p(x) \in \mathbb{F}[x]$ berderajat m yang tak-tereduksi atas $\mathbb{F}$. Jika $p(x)$ masih tetap tak-tereduksi atas $\mathbb{F}(\alpha)$, maka $\deg_{\mathbb{F}(\alpha)}(\beta) = m$. Jika tidak, $p(x)$ dapat difaktorkan atas $\mathbb{F}(\alpha)$ menjadi hasil perkalian polinomial derajat $< m$ dan β adalah suatu akar dari salah satu faktor ini. Oleh karena itu $\deg_{\mathbb{F}(\alpha)}(\beta) < m$. Ini melengkapi buktinya.

Akibat 10.2.4 Misalkan $\mathbb{F} \subseteq \mathbb{E}$ keduanya adalah lapangan, α dan β adalah elemen-elemen di $\mathbb{E}$ yang merupakan aljabar atas $\mathbb{F}$. Maka $\alpha \pm \beta, \alpha\beta$, dan (jika $\beta \neq 0$) α/β semuanya merupakan elemen-elemen aljabar atas $\mathbb{F}$.

Bukti
Dengan menggunakan Akibat 10.2.3, maka $\mathbb{F}(\alpha, \beta)$ adalah perluasan berhingga dari $\mathbb{F}$ dengan demikian menurut Teorema 10.2.4 $F(\alpha, \beta)$ adalah perluasan aljabar dari $\mathbb{F}$. Tetapi $\alpha \pm \beta, \alpha\beta$, dan (jika $\beta \neq 0$) α/β adalah semuanya elemen-elemen di $\mathbb{F}(\alpha, \beta)$, maka elemen-elemen tsb. aljabar atas $\mathbb{F}$.

Akibat 10.2.5 Misalkan $\mathbb{F} \subseteq \mathbb{E}$ keduanya adalah lapangan dan misalkan S adalah suatu himpunan dengan elemen-elemen di $\mathbb{E}$ yang merupakan aljabar atas $\mathbb{F}$. Maka S adalah sublapangan dari $\mathbb{E}$ dan lapangan perluasan dari $\mathbb{F}$.

Bukti
Langsung dari Akibat 10.2.4 ✓

Definisi 10.2.6 Misalkan $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ adalah aljabar atas } \mathbb{Q}\}$. Maka $\overline{\mathbb{Q}}$ disebut lapangan dari **bilangan-bilangan aljabar**. ✓

Contoh 10.2.11 Lapangan $\overline{\mathbb{Q}}$ dari bilangan-bilangan aljabar adalah contoh dari suatu perluasan aljabar tak-berhingga dari $\mathbb{Q}$. Menurut definisi, $\overline{\mathbb{Q}}$ adalah perluasan aljabar dari $\mathbb{Q}$. Sekarang pertimbangkan untuk sebarang bilangan bulat positif n elemen $2^{\frac{1}{n}}$. Elemen-elemen ini aljabar atas $\mathbb{Q}$, maka elemen-elemen tsb. berada di $\overline{\mathbb{Q}}$. Karena $[\mathbb{Q}(2^{\frac{1}{n}}) : \mathbb{Q}] = n$, maka $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$ untuk semua $n > 0$. ●

Teorema 10.2.6 Misalkan $\mathbb{K}$ adalah suatu perluasan aljabar dari dari suatu lapangan $\mathbb{E}$, dan $\mathbb{E}$ merupakan perluasan aljabar dari dari suatu lapangan $\mathbb{F}$. Maka $\mathbb{K}$ adalah suatu perluasan aljabar dari $\mathbb{F}$.

Bukti
Misalkan α adalah sebarang elemen di $\mathbb{K}$. Maka α adalah elemen aljabar atas $\mathbb{E}$. Karena itu,

$$c_n\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0, \tag{10.1}$$

untuk beberapa $c_i \in \mathbb{E}$, $0 \leq i \leq n$. Karena $\mathbb{E}$ adalah aljabar atas $\mathbb{F}$, maka semua $c_i \in \mathbb{E}$ adalah elemen aljabar atas $\mathbb{F}$. Oleh karena itu, menurut Akibat 10.2.3, maka $\mathbb{L} = \mathbb{F}(c_0, c_1, \ldots, c_n)$ adalah perluasan berhingga dari $\mathbb{F}$. Dari (10.1) α adalah elemen aljabar atas $\mathbb{L}$, jadi $\mathbb{L}(\alpha)$ adalah perluasan berhingga dari $\mathbb{L}$. Dengan Teorema 10.2.5, maka $\mathbb{L}(\alpha)$ adalah perluasan berhingga dari $\mathbb{F}$. Dengan demikian menurut Teorema 10.2.4 $\mathbb{L}(\alpha)$ merupakan perluasan aljabar dari $\mathbb{F}$ dan adalah aljabar atas $\mathbb{F}$. ✓

Memang ada elemen $\alpha \in \mathbb{R}$ yang transendental atas $\mathbb{Q}$. (Suatu bukti diuraikan dalam tiga latihan terakhir untuk bagian ini.) Jauh lebih mudah untuk membuktikan bahwa ada bilangan real transendental daripada membuktikan bahwa bilangan real **penting tertentu** yang ditemui dalam kalkulus dan cabang matematika lainnya, seperti e dan π, bersifat transendental. Memang benar, tetapi pembuktiannya memerlukan metode kalkulus dan tidak termasuk dalam aljabar.

Latihan

Dalam Latihan 1 sampai 5 tunjukkan bahwa $\alpha \in \mathbb{C}$ yang ditunjukkan adalah aljabar atas $\mathbb{Q}$

1. $1 - \sqrt{5}$ **2.** $\sqrt{2} + \sqrt{3}$ **3.** $1 + i$ **4.** $\sqrt{1 + \sqrt{3}}$ **5.** $2^{\frac{1}{3}} + 1$.

6. Tunjukkan bahwa pemetaan ϕ yang didefinisikan dalam pembuktian Teorema 10.2.1 adalah suatu isomorpisma.

7. Misalkan $\mathbb{F} \subseteq \mathbb{E}$ keduanya adalah lapangan dan sebarang $\alpha \in \mathbb{E}$ adalah aljabar atas $\mathbb{F}$. Tunjukkan bahwa

$$I = \{f(x) \in \mathbb{F}[x] \mid f(\alpha) = 0\}$$

adalah suatu ideal sejati dalam $\mathbb{F}[x]$.

Dalam Latihan 8 hingga 10 tunjukkan bahwa $\alpha \in \mathbb{C}$ yang ditunjukkan adalah aljabar atas $\mathbb{Q}$, dan tentukan $\deg_{\mathbb{Q}}(\alpha)$

8. $\sqrt{3} - i$ **9.** $\sqrt{3} - \sqrt{3}i$ **10.** $\sqrt{2} + \sqrt{2}\,i$.

11. Dapatkan $\deg_{\mathbb{F}}(\sqrt{2} + \sqrt{3})$ untuk lapangan yang ditunjukkan $\mathbb{F}$:
(a) $\mathbb{F} = \mathbb{Q}$ (b) $\mathbb{F} = \mathbb{Q}(\sqrt{6})$ (c) $\mathbb{F} = \mathbb{Q}(\sqrt{5})$ (d) $\mathbb{F} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

12. Dapatkan polinomial minimal dari $\dfrac{\sqrt{2} + \sqrt{2}\,i}{2}$ atas lapangan $\mathbb{F}$ yang diberikan:
(a) $\mathbb{F} = \mathbb{Q}$ (b) $\mathbb{F} = \mathbb{R}$ (c) $\mathbb{F} = \mathbb{Q}(i)$.

Dalam Latihan 13 sampai 17 dapatkan basis untuk lapangan perluasan dari $\mathbb{Q}$ yang diberikan atas $\mathbb{Q}$.
13. $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ **14.** $\mathbb{Q}(\sqrt{2}, i)$ **15.** $\mathbb{Q}(\sqrt{2}\,i)$ **16.** $\mathbb{Q}(2^{\frac{1}{3}}, 7^{\frac{1}{2}})$ **17.** $\mathbb{Q}(\sqrt{2} + i)$.

18. Misalkan $\mathbb{F}$ adalah suatu lapangan, $\mathbb{F} \subseteq \mathbb{E}$ sublapangan dari $\mathbb{E}$, dan $\alpha \in \mathbb{E}$. Tunjukkan bahwa $\mathbb{F}(\alpha)$ adalah suatu ruang vektor berdimensi hingga atas $\mathbb{F}$ jika dan hanya jika α adalah aljabar atas $\mathbb{F}$.

19. Misalkan $\mathbb{E}$ adalah suatu lapangan, $\mathbb{F} \subseteq \mathbb{E}$ sublapangan dari $\mathbb{E}$, dan $\alpha \in \mathbb{E}$. Tunjukkan bahwa α adalah aljabar atas $\mathbb{F}$ jika dan hanya jika $F[\alpha] = \{f(\alpha) \mid f(x) \in \mathbb{F}[x]\}$ adalah suatu lapangan.

20. Misalkan $\mathbb{E}$ adalah suatu lapangan, $\mathbb{F} \subseteq \mathbb{E}$ sublapangan dari $\mathbb{E}$, dan $\alpha \in \mathbb{E}$. Tunjukkan bahwa α adalah transendental atas $\mathbb{F}$ jika dan hanya jika $F[\alpha] = \{f(\alpha) \mid f(x) \in \mathbb{F}[x]\}$ isomorpik dengan $\mathbb{F}[x]$.

21. Misalkan $\mathbb{E}$ adalah suatu lapangan, $\mathbb{F} \subseteq \mathbb{E}$ sublapangan dari $\mathbb{E}$, dan $\alpha \in \mathbb{E}$. Jika α adalah aljabar atas $\mathbb{F}$ berderajat 15 dan $\beta \in \mathbb{F}(\alpha)$, berapakah nilai yang mungkin dari $[\mathbb{F}(\beta) : \mathbb{F}]$?

22. Misalkan $f(x)$ dan $g(x)$ adalah polinomial tak-tereduksi atas suatu lapangan $\mathbb{F}$ dengan $\deg f(x) = 15$ dan $\deg g(x) = 14$. Misalkan α adalah suatu akar dari $f(x)$ di beberapa lapangan perluasan dari $\mathbb{F}$. Tunjukkan bahwa $g(x)$ masih tetap tak-tereduksi atas $\mathbb{F}(\alpha)$.

23. Misalkan $\mathbb{E}$ adalah suatu lapangan, $\mathbb{F} \subseteq \mathbb{E}$ suatu sublapangan dari $\mathbb{E}$, dan $\alpha, \beta \in \mathbb{E}$. Jika α dan β adalah aljabar atas $\mathbb{F}$ dengan $\deg_{\mathbb{F}} \alpha = n$ dan $\deg_{\mathbb{F}} \beta = m$ dengan $\text{fpb}(n, m) = 1$, maka tunjukkan bahwa $[\mathbb{F}(\alpha, \beta) : \mathbb{F}] = n \cdot m$.

24. Jika $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_r)$, dimana masing-masing α_i aljabar atas $\mathbb{F}$ dengan derajat $\deg_{\mathbb{F}} \alpha_i = n_i$, maka tunjukkan bahwa $[\mathbb{E} : \mathbb{F}] \leq n_1 \cdots n_r$.

25. Misalkan $\mathbb{E}$ adalah suatu lapangan, dan $\mathbb{F} \subseteq \mathbb{E}$ suatu sublapangan dari $\mathbb{E}$. Tunjukkan bahwa $\mathbb{E}$ adalah perluasan berhingga dari $\mathbb{F}$ jika dan hanya jika ada elemen-elemen $\alpha_i \in \mathbb{E}$, $1 \leq i \leq r$ dengan masing-masing α_i aljabar atas $\mathbb{F}$ dan $\mathbb{E} = \mathbb{F}(\alpha_1, \ldots, \alpha_r)$.

26. Misalkan $\mathbb{E}$ adalah suatu lapangan, $\mathbb{F} \subseteq \mathbb{E}$ suatu sublapangan dari $\mathbb{E}$ dan $\alpha \in \mathbb{E}$, suatu polinomial taknol $f(x) \in \mathbb{F}[x]$. Tunjukkan bahwa jika $f(\alpha)$ aljabar atas $\mathbb{F}$, maka α aljabar atas $\mathbb{F}$.

27. Misalkan p dan q adalah dua bilangan bulat prima yang berbeda.

(a) Tunjukkan bahwa $\mathbb{Q}(\sqrt{p} + \sqrt{q}) = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

(b) Dapatkan polinomial minimal dari $\sqrt{p} + \sqrt{q}$ atas $\mathbb{Q}$.

28. Misalkan $\mathbb{E}$ adalah suatu lapangan, $\mathbb{F} \subseteq \mathbb{E}$ satu sublapangan dari $\mathbb{E}$, dan $\alpha, \beta \in \mathbb{E}$. Tunjukkan bahwa bila $\alpha + \beta$ dan $\alpha\beta$ keduanya adalah aljabar atas $\mathbb{F}$, maka α dan β aljabar atas $\mathbb{F}$.

Keberadaan Bilangan Transendental

Latihan 29 hingga 31 menguraikan bukti keberadaan bilangan real transendental atas $\mathbb{Q}$.

29. Tulis $\mathbb{N}$ untuk himpunan $\{n \in \mathbb{Z} \mid n > 0\}$ bilangan bulat positif. Suatu himpunan X **dapat dihitung** (***countable***) jika ada pemetaan $\phi : \mathbb{N} \to X$ dari $\mathbb{N}$ ke X yang **pada**.

(a) Tunjukkan bahwa himpunan $\mathbb{N}^2 = \{(i, j) \mid i, j \in \mathbb{N}\}$ adalah **dapat dihitung** dengan mendefinisikan pemetaan $\phi_2 : \mathbb{N} \to \mathbb{N}^2$ adalah **pada**. (**Petunjuk**: Setiap bilangan bulat positif n dapat ditulis secara tunggal sebagai hasil perkalian $2^{i-1}(2j-1)$ dari pangkat 2 dan bilangan ganjil.)

(b) Tunjukkan bahwa himpunan dari 3-pasangan bilangan bulat positif $\mathbb{N}^3$ adalah **dapat dihitung** dengan mendefinisikan pemetaan dari himpunan $\mathbb{N}$ ke $\mathbb{N}^3$. (**Petunjuk**: Pertama-tama gunakan ϕ_2 untuk mendefinisikan suatu pemetaan **pada** dari himpunan $\mathbb{N}^2$ ke himpunan $\mathbb{N}^3$.)

(c) Tunjukkan bahwa untuk setiap bilangan bulat positif r himpunan $\mathbb{N}^r$ dari r-pasangan bilangan bulat positif adalah **dapat dihitung** dengan menunjukkan cara mendefinisikan pemetaan **pada** ϕ_r dari $\mathbb{N}$ ke $\mathbb{N}^r$.

(d) Misalkan $\mathbb{N}^{<\infty}$ adalah himpunan semua barisan berhingga bilangan bulat positif atau, dengan kata lain, $\mathbb{N}^{<\infty} = \bigcup_{r \in \mathbb{N}} \mathbb{N}^r$. Tunjukkan bahwa $\mathbb{N}^{<\infty}$ adalah **dapat dihitung** dengan menunjukkan cara mendefinisikan pemetaan **pada** ϕ dari $\mathbb{N}$ ke $\mathbb{N}^{<\infty}$. (**Petunjuk**: Tunjukkan bahwa pemetaan $\psi(r, n) = \phi_r(n)$ dari $\mathbb{N}^2$ ke $\mathbb{N}^{<\infty}$ adalah **pada**.)

30. Dengan menggunakan hasil dari soal sebelumnya, tunjukkan bahwa himpunan berikut **dapat dihitung**:

(a) Himpunan semua bilangan rasional $\mathbb{Q}$ (**Petunjuk**: Setiap bilangan rasional dapat direpresentasikan sebagai hasil pembagian $(i - j)/k$ di mana i, j dan k adalah bilangan bulat positif.)

(b) Ring polinomial atas lapangan bilangan rasional $\mathbb{Q}[x]$. (**Petunjuk**: Pertama tunjukkan bahwa himpunan $\mathbb{Q}^{<\infty}$ dari barisan berhingga bilangan rasional **dapat dihitung**.)

(c) Lapangan dari bilangan-bilangan aljabar $\overline{\mathbb{Q}}$.

31. Misalkan $\phi : \mathbb{N} \to I$, di mana I adalah **interval satuan** $\{a \in \mathbb{R} \mid 0 < a < 1\}$. Untuk setiap $n \in \mathbb{N}$, tulis $\phi(n)$ dalam notasi desimal:

$$\phi(n) = 0, c_{n,1}c_{n,2}c_{n,3}\cdots$$

dimana setiap $0 \leq c_{n,i} \leq 9$ untuk semua n dan i. **Bilangan diagonal** $\delta(\phi)$ dari ϕ adalah bilangan real $b \in I$ dengan representasi desimal

$$\delta(\phi) = 0, d_{n,1}d_{n,2}d_{n,3}\cdots$$

dimana $d_{n,i} = 1$ jika $c_{n,i} \neq 1$, dan $d_{n,i} = 2$ jika $c_{n,i} = 1$.

(a) Tunjukkan bahwa $\delta(\phi) \neq \phi(n)$ untuk setiap n.

(b) Tunjukkan bahwa I tak-terhitung.

Menggunakan fakta-fakta ini dan hasil dari masalah sebelumnya

(c) Tunjukkan bahwa himpunan bilangan real transendental bukan himpunan kosong.

(d) Tunjukkan bahwa himpunan bilangan real transendental tak-terhitung.

10.3 Lapangan Pemecah

Seperti yang ditunjukkan pada bagian sebelumnya, setiap polinomial $f(x) \in \mathbb{F}[x]$ memiliki akar α di beberapa lapangan perluasan dari $\mathbb{F}$ (Teorema Kronecker). Kita telah mempelajari struktur $\mathbb{F}(\alpha)$, lapangan perluasan terkecil dari $\mathbb{F}$ yang berisi α. Di bagian ini kita membangun **lapangan pemecah** dari $f(x)$ atas $\mathbb{F}$ yang merupakan lapangan perluasan terkecil dari $\mathbb{F}$ yang berisi semua akar dari $f(x)$. Teorema Kronecker digunakan untuk menunjukkan bahwa lapangan perluasan seperti itu ada untuk setiap polinomial $f(x)$.

Contoh 10.3.1 Hubungkan ke $\mathbb{Q}$ satu akar $\sqrt{2} = 2^{\frac{1}{2}}$ dari polinomial tak-tereduksi $x^2-2 \in \mathbb{Q}[x]$ juga memberi kita akar lainnya $-2^{\frac{1}{2}}$, dan atas $\mathbb{Q}(2^{\frac{1}{2}})$ kita memiliki suatu faktorisasi lengkap menjadi suatu hasil perkalian dari faktor-faktor linier:

$$x^2 - 2 = (x - 2^{\frac{1}{2}})(x + 2^{\frac{1}{2}})$$

Demikian pula, menghubungkan ke $\mathbb{Q}$ satu akar $\sqrt{3}\,i = 3^{\frac{1}{2}}i \in \mathbb{C}$ dari polinomial tak-tereduksi $x^2 + 3 \in \mathbb{Q}[x]$ juga memberi kita $-3^{\frac{1}{2}}$ akar lainnya, dan atas $\mathbb{Q}(3^{\frac{1}{2}})$ kita memiliki faktorisasi menjadi hasil perkalian faktor-faktor linier:

$$x^2 + 3 = (x - 3^{\frac{1}{2}}i)(x + 3^{\frac{1}{2}}i).$$

Demikian pula, menghubungkan ke $\mathbb{Q}$ satu akar $\omega \in \mathbb{C}$ dari polinomial tak-tereduksi x^2+x+1 juga memberi kita akar lainnya ω^2, dan atas $\mathbb{Q}(\omega)$ kita memiliki faktorisasi lengkap menjadi hasil perkalian faktor-faktor linier:

$$x^2 + x + 1 = (x - \omega)(x - \omega^2).$$

Sebenarnya, karena $\omega = \frac{1}{2}(-1 + 3^{\frac{1}{2}}i)$ dan $3^{\frac{1}{2}}i = 2\omega + 1$, lapangan-lapangannya sama dalam dua kasus terakhir ini, $\mathbb{Q}(3^{\frac{1}{2}}i) = \mathbb{Q}(\omega)$. ●

Contoh 10.3.2 Berbeda dengan sebelumnya, hubungkan ke $\mathbb{Q}$ satu akar $\sqrt[3]{2} = 2^{\frac{1}{3}}$ dari polinomial tak-tereduksi $x^3 - 2 \in \mathbb{Q}[x]$ tidak memberi kita dua akar lainnya dari polinomial ini di $\mathbb{C}$, yaitu $\omega 2^{\frac{1}{3}}$ dan $\omega^2 2^{\frac{1}{3}}$. Atas $\mathbb{Q}(2^{\frac{1}{3}})$ kita memiliki faktorisasi

$$x^3 - 2 = (x - 2^{\frac{1}{3}})(x^2 + 2^{\frac{1}{3}}x + 2^{\frac{2}{3}}),$$

tetapi faktor kedua, yang akarnya di $\mathbb{C}$ adalah $\omega 2^{\frac{1}{3}}$ dan $\omega^2 2^{\frac{1}{3}}$, tak-tereduksi. Lebih lanjut, hubungkan ke $\mathbb{Q}(2^{\frac{1}{3}})$ salah satu dari akar ini memberikan yang lain, dan atas $\mathbb{Q}(2^{\frac{1}{3}}, \omega 2^{\frac{1}{3}})$ kita memiliki faktorisasi lengkap menjadi hasil perkalian faktor-faktor linier:

$$x^3 - 2 = (x - 2^{\frac{1}{3}})(x - \omega 2^{\frac{1}{3}})(x - \omega^2 2^{\frac{1}{3}}).$$

Menghubungkan $\omega 2^{\frac{1}{3}}$ ke $\mathbb{Q}(2^{\frac{1}{3}})$ jelas menghasilkan hasil yang sama seperti menghubungkan ω, yang telah kita sebutkan dalam contoh sebelumnya menghasilkan hasil yang sama seperti menghubungkan $3^{\frac{1}{2}}i$. Artinya, kita memiliki

$$\mathbb{Q}(2^{\frac{1}{3}}, \omega 2^{\frac{1}{3}}) = \mathbb{Q}(2^{\frac{1}{3}}, \omega) = \mathbb{Q}(2^{\frac{1}{3}}, 3^{\frac{1}{2}}i).$$

Perhatikan bahwa ω dan $3^{\frac{1}{2}}i$ memiliki derajat 2 atas $\mathbb{Q}$, sedangkan menurut Kesimpula 10.2.2, derajat dari setiap elemen-elemen di $\mathbb{Q}(2^{\frac{1}{3}})$ atas $\mathbb{Q}$ harus membagi 3. Jadi ω dan $3^{\frac{1}{2}}i$ tidak berada di $\mathbb{Q}(2^{\frac{1}{3}})$. ●

Beberapa definisi dan proposisi berikutnya memperkenalkan beberapa terminologi untuk menggambarkan jenis situasi yang dihadapi dalam contoh sebelumnya dan menyatakan beberapa fakta dasar tentang gagasan yang diperkenalkan.

Definisi 10.3.1 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x) \in \mathbb{F}[x]$ polinomial tidak konstan, dan $\mathbb{E}$ suatu lapangan perluasan dari $\mathbb{F}$. Maka kita katakan $f(x)$ **terpecah** atas $\mathbb{E}$ jika dalam $\mathbb{E}[x]$ kita memiliki faktorisasi $f(x)$ ke dalam hasil perkalian suatu unit dikalikan faktor linier monik:

$$f(x) = u(x - \alpha_1) \cdots (x - \alpha_n).$$

Perhatikan bahwa dalam faktorisasi seperti itu, karena u adalah koefisien utama dari $f(x)$, kita memiliki $u \in \mathbb{F}$. ✓

Proposisi 10.3.1 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x) \in \mathbb{F}[x]$ polinomial tidak konstan, dan $\mathbb{E}$ suatu lapangan perluasan dari $\mathbb{F}$.

(1) Jika dalam $\mathbb{E}[x]$ kita memiliki faktorisasi lengkap dari $f(x)$ menjadi hasil perkalian faktor-faktor linier:

$$f(x) = (a_1 x + b_1) \cdots (a_n x + b_n),$$

maka $f(x)$ **memisah** atas $\mathbb{E}$.

(2) Jika $\mathbb{E}$ memuat n akar-akar yang berbeda $\alpha_1, \ldots, \alpha_n$ dari $f(x)$, dimana n adalah derajat $f(x)$, maka $f(x)$ memisah atas $\mathbb{E}$.

Bukti

(1) Diberikan faktorisasi seperti pada (1), kita memperoleh pemecaham seperti pada Definisi 10.3.1 dengan menetapkan $u = a_1 \cdots a_n$ dan $\alpha_i = -a_i^{-1} b_i$.

(2) Jika α_1 adalah suatu akar dari $f(x)$, maka

$$f(x) = (x - \alpha_1)q_1(x) \in \mathbb{E}[x]$$

di mana $\deg q_1(x) = n - 1$. Jika α_2 adalah akar dari $f(x)$ yang berbeda dengan α_1, maka $x - \alpha_2$ membagi $q_1(x)$ dan

$$f(x) = (x - \alpha_1)(x - \alpha_2)q_2(x) \in \mathbb{E}[x],$$

dimana $\deg q_2(x) = n - 2$. Melanjutkan cara ini dan karena semua $x - \alpha_i$ berbeda, maka kita memiliki

$$f(x) = (x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)q_n(x) \in \mathbb{E}[x],$$

dimana $\deg q_n(x) = 0$, sehingga $q_n(x) = u \neq 0$ adalah suatu konstanta bukan nol, dan karenanya merupakan unit.

Definisi 10.3.2 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x) \in \mathbb{F}[x]$ suatu polinomial tak-konstan, dan $\mathbb{E}$ suatu lapangan perluasan dari $\mathbb{F}$ dimana $f(x)$ terpecah atas $\mathbb{E}$. Sublapangan $\mathbb{K}$ dari $\mathbb{E}$ yang memuat $\mathbb{F}$ disebut **lapangan pemecah** dalam $\mathbb{E}$ dari $f(x)$ atas $\mathbb{F}$ jika

(1) $f(x)$ memisah atas $\mathbb{K}$,

(2) sublapangan $\mathbb{K}$ adalah **sublapangan terkecil** dari $\mathbb{E}$ yang memuat $\mathbb{F}$ dimana $f(x)$ memisah atas $\mathbb{K}$.

Proposisi 10.3.2 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x) \in \mathbb{F}[x]$ suatu polinomial bukan konstan, dan $\mathbb{E}$ suatu lapangan perluasan dari $\mathbb{F}$ dimana $f(x)$ terpecah atas $\mathbb{E}$ sebagai

$$f(x) = u(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

Maka $\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ adalah lapangan pemecah di $\mathbb{E}$ dari $f(x)$ atas $\mathbb{F}$.

Bukti
(1) Karena $f(x) = u(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \in \mathbb{K}[x]$ dan $\alpha_i \in \mathbb{K}$, maka $f(x)$ terpecah atas $\mathbb{K}$.
(2) Untuk menunjukkan bahwa $\mathbb{K}$ adalah sublapangan terkecil dari $\mathbb{E}$ yang memuat $\mathbb{F}$ dimana $f(x)$ memisah, kita harus menunjukkan bahwa jika $\mathbb{L}$ adalah sublapangan yang lain dari $\mathbb{E}$ memuat $\mathbb{F}$ dimana $f(x)$ memisah, maka $\mathbb{K} \subseteq \mathbb{L}$. Jadi misalkan $\mathbb{L}$ adalah suatu sublapangan seperti itu. Atas $\mathbb{L}$ kita memiliki pemecah dari:

$$f(x) = v(x - \beta_1)(x - \beta_2)\cdots(x - \beta_n) \in \mathbb{L}[x] \subseteq \mathbb{E}[x].$$

Tetapi dengan faktorisasi tunggal untuk $\mathbb{E}[x]$ faktor-faktor $(x - \beta_j)$ harus sama dengan faktor-faktor $(x - \alpha_i)$ kecuali untuk urutannya. Jadi setiap α_i sama dengan salah satu dari $\beta_j \in \mathbb{L}$. Oleh karena itu $\alpha_i \in \mathbb{L}$ untuk semua i, dan karena juga $\mathbb{L}$ diasumsikan memuat $\mathbb{F}$ kita dapatkan

$$\mathbb{K} = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq \mathbb{L}$$

sebagaimana yang dibutuhan.

Perhatikan bahwa jika penghubungan dengan beberapa α_i memberi kita yang lain, katakan

$$\alpha_{m+1}, \ldots, \alpha_n \in \mathbb{F}(\alpha_1, \ldots, \alpha_m),$$

maka

$$\mathbb{F}(\alpha_1, \ldots, \alpha_m) = \mathbb{F}(\alpha_1, \ldots, \alpha_n)$$

yang merupakan lapangan pemecah. Ini adalah situasi dengan lapangan

$$\mathbb{Q}(2^{\frac{1}{3}}, \omega 2^{\frac{1}{3}}) = \mathbb{Q}(2^{\frac{1}{3}}, \omega) = \mathbb{Q}(2^{\frac{1}{3}}, 3^{\frac{1}{2}} i).$$

dalam Contoh10.3.2, yang menurut Proposis 10.3.2 adalah lapangan pemecah di $\mathbb{C}$ dari $x^3 - 2$ atas $\mathbb{Q}$.

Contoh 10.3.3 Pertimbangkan $f(x) = x^4 - 7x^2 + 1 \in \mathbb{Q}[x]$. Kita mulai dengan memeriksa kerekduksian. Jika kita mencari suatu faktorisasi

$$x^4 - 7x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$$

dalam $\mathbb{Z}[x]$ kita memperoleh koondisi

$$\begin{aligned} bd &= 1 \\ ad + bc = &= 0 \\ b + d + ac &= -7 \\ a + c &= 0, \end{aligned}$$

dan $b = d = 1, a = -c = 3$ adalah suatu penyelesaian. Karena itu

$$x^4 - 7x^2 + 1 = (x^2 + 3x + 1)(x^2 - 3x + 1).$$

Sekarang kita dapat menggunakan rumus persamaan kuadrat untuk menemukan bahwa akar-akar dari $f(x)$ dalam $\mathbb{C}$ adalah empat bilangan real sebagai berikut:

$$\frac{\pm 3 \pm \sqrt{5}}{2}.$$

Jelas, jika r adalah sebarang salah satu dari empat akar-akar ini, maka $\sqrt{5} = 5^{\frac{1}{2}} \in \mathbb{Q}(r)$. Semua keempat akar-akar ini berada di $Q(5^{\frac{1}{2}})$ yang merupakan lapangan pemecah di $\mathbb{C}$ dari $f(x)$ atas $\mathbb{Q}$. ●

Contoh 10.3.4 Pertimbangkan $f(x) = x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$. Kita memiliki faktorisasi

$$x^4 + 2x^2 + 1 = (x^2 + 1)^2.$$

Akar-akar dari $f(x)$ di $\mathbb{C}$ hanyalah $\pm i$. Lapangan pemecah di $\mathbb{C}$ dari $f(x)$ atas $\mathbb{Q}$ hanya $\mathbb{Q}(i)$, dimana kita memiliki pemecahan

$$(x - i)^2 (x + i)^2.$$

Ini menggambarkan kasus dimana banyaknya akar yang berbeda kurang dari derajat polinomial. ●

Proposisi 10.3.2 memberi tahu kita bahwa lapangan pemecah $\mathbb{K}$ untuk polinomial $f(x) \in \mathbb{F}[x]$ ada asalkan ada lapangan perluasan $\mathbb{E}$ dari $\mathbb{F}$ dimana $f(x)$ dipecah. Dalam contoh yang dipertimbangkan sejauh ini, $\mathbb{F}$ adalah bilangan rasional $\mathbb{Q}$ dan $f(x)$ paling buruk adalah polinomial kuartik, dan polinomial tersebut telah dipecah atas $\mathbb{C}$. Teorema berikutnya memberi tahu kita bahwa untuk $\mathbb{F}$ dan $f(x) \in \mathbb{F}[x]$ sebarang polinomial bukan konstanta, akan ada beberapa lapangan perluasan $\mathbb{E}$ dimana polinomial dipecah, dan oleh karena itu ada lapangan pemecah.

Teorema 10.3.1 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $f(x) \in \mathbb{F}[x]$ polinomial bukan konstan. Maka ada lapangan perluasan $\mathbb{E}$ dari $\mathbb{F}$ dimana $f(x)$ dipecah.

Bukti
Kita membuktikan teorema dengan induksi pada $n = \deg f(x)$. Jika $n = 1$, maka $f(x)$ sudah linier, dan kita dapat mengambil $\mathbb{E} = \mathbb{F}$. Jika tidak, asumsikan sebagai hipotesis induksi bahwa teorema berlaku untuk $n-1$ pada sebarang lapangan, dan pertimbangkan $f(x)$ berderajat n. Dengan teorema Kronecker (Teorema 10.2.5) ada suatu lapangan perluasan $\mathbb{K}$ dari $\mathbb{F}$ dimana $f(x)$ memiliki akar β. Selanjutnya, atas $\mathbb{K}$ kita memiliki faktorisasi: $f(x) = (x-\beta)g(x)$, dimana $g(x)$ memiliki derajat $n-1$. Dengan hipotesis induksi ada lapangan perluasan $\mathbb{E}$ dari $\mathbb{K}$ dimana ada pemecahan:

$$g(x) = u(x-\alpha_1)\cdots(x-\alpha_{n-1}).$$

Maka atas $\mathbb{E}$ kita mempunyai

$$f(x) = u(x-\alpha_1)\cdots(x-\alpha_{n-1})(x-\beta)$$

yang merupakan pemecahan. ∎

Proposisi 10.3.2 dan Teorema 10.3.1 menyiratkan keberadaan polinomial bukan konstan $f(x) \in \mathbb{F}[x]$ dari lapangan perluasan berhingga $\mathbb{K}$ dari $\mathbb{F}$ yang merupakan lapangan pemecah dari $f(x)$. Apa yang dapat kita katakan tentang derajat $[\mathbb{K} : \mathbb{F}]$ dari $\mathbb{K}$ atas $\mathbb{F}$? Tentu saja, jika $f(x)$ sudah dipecah di $\mathbb{F}$ kita dapat mengambil $\mathbb{K} = \mathbb{F}$ sehingga $[\mathbb{K} : \mathbb{F}]$ dapat menjadi sekecil 1. Seberapa besar itu bisa? Argumen induktif seperti yang digunakan untuk membuktikan Teorema 10.3.1 dapat digunakan untuk membuktikan berikut ini.

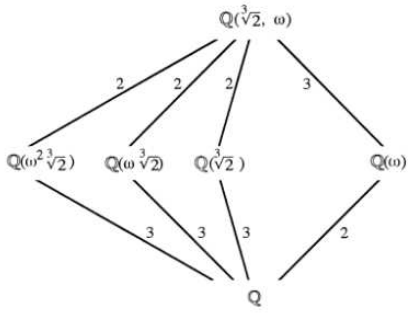
Proposisi 10.3.3 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $f(x) \in \mathbb{F}[x]$ polinomial berderajat $n > 1$. Maka ada perluasan berhingga $\mathbb{E}$ dari $\mathbb{F}$ berderajat $[\mathbb{E} : \mathbb{F}] \leq n!$ dimana $f(x)$ dipecah.

Bukti
Sebagai Latihan! ∎

Bahkan jika tidak ada akar dari $f(x)$ yang berada di $\mathbb{F}$, derajat $[\mathbb{K} : \mathbb{F}]$ dari suatu lapangan pemecah $\mathbb{K}$ mungkin jauh lebih kecil dari $n!$ sebagaimana dalam proposisi sebelumnya. Misalnya, dalam Contoh 10.3.3 dan 10.3.4 kita memiliki

$$[\mathbb{K} : \mathbb{F}] = 2 \leq 4 = \deg f(x).$$

Dalam contoh ini, $f(x)$ dapat direduksi. Jika $f(x)$ adalah polinomial tak-tereduksi berderajat n maka bahkan hanya menghubungkan ke satu akar dari polinomial $f(x)$ menghasilkan suatu perluasan derajat n jadi kita memiliki batas bawah $n \leq [\mathbb{K} : \mathbb{F}]$ untuk menuju batas atas $[\mathbb{K} : \mathbb{F}] \leq n!$ tersirat oleh proposisi sebelumnya. Dua contoh berikutnya menggambarkan kemungkinan.



Gambar 10.1: ***Lattice*** dari Contoh 10.3.5

Contoh 10.3.5 Kita lihat lagi Contoh 10.3.2, dimana kita mempertimbangkan lapangan pemecah $\mathbb{Q}(2^{\frac{1}{3}}, \omega)$ dari $x^3 - 2$ atas $\mathbb{Q}$. Gambar 10.1 menunjukkan ***lattice*** dari sublapangan dari lapangan pemecah ini. Angka 2 atau 3 di samping garis yang menghubungkan lapangan dan lapangan perluasannya menunjukkan derajad perluasan. Dengan demikian kita dapat memperoleh lapangan pemecah dengan menghubungkan ke $\mathbb{Q}$ salah satu dari akar dari $x^3 - 2$ dan kemudian menghubungkan suatu akar dari $x^2 + x + 1$, atau dengan melakukan kebalikannya. Dari derajad tsb., kita memiliki

$$\begin{aligned}\left[\mathbb{Q}(2^{\frac{1}{3}}, \omega) : \mathbb{Q}\right] &= \left[\mathbb{Q}(2^{\frac{1}{3}}, \omega) : \mathbb{Q}(2^{\frac{1}{3}})\right] \cdot \left[\mathbb{Q}(2^{\frac{1}{3}}) : \mathbb{Q}\right] = 2 \cdot 3 = 6 = 3! \\ \left[\mathbb{Q}(2^{\frac{1}{3}}, \omega) : \mathbb{Q}\right] &= \left[\mathbb{Q}(2^{\frac{1}{3}}, \omega) : \mathbb{Q}(\omega)\right] \cdot [\mathbb{Q}(\omega) : \mathbb{Q}] = 2 \cdot 3 = 6 = 3!.\end{aligned}$$

Bagaimanapun kita sampai di sana, derajat lapangan pemecah adalah maksimum yang mungkin untuk polinomial derajat 3. ●

Contoh 10.3.6 Akar-akar dari polinomial $x^n - 1 \in \mathbb{Q}[x]$ adalah apa yang kita sebut akar-akar tingkat-n dari satuan yaitu lingkaran dengan jari-jari satu pusat di titik asal $(0, 0)$. Akar-akar ini adalah bilangan kompleks

$$\begin{aligned}\xi_n &= \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) \\ \xi_n^k &= \cos(k\frac{2\pi}{n}) + i\sin(k\frac{2\pi}{n}),\end{aligned}$$

dimana $0 \leq k \leq n - 1$. Akar-akar tsb. membentuk suatu grup siklik

$$\{1, \xi_n, \xi_n^2, \ldots, \xi_n^{n-1}\}$$

berorder n terhadap perkalian. Karenanya semua n akar-akar yang berbeda ini berada di $\mathbb{Q}(\xi_n)$, oleh karena itu merupakan lapangan pemecah dari $x^n - 1 \in \mathbb{Q}[x]$ atas $\mathbb{Q}$. Perhatikan bahwa jika $n = p$ suatu bilangan prima, maka

$$x^p - 1 = (x - 1)(x^{p-1} + \cdots + x^2 + x + 1)$$

dan polinomial

$$\Phi_p(x) = x^{p-1} + \cdots + x^2 + x + 1$$

menurut Akibat 8.4.2 tak-tereduksi. Oleh karena itu lapangan pemecah $\mathbb{Q}(\xi_p)$ dari $x^p - 1$ memiliki derajat $[\mathbb{Q}(\xi_p) : \mathbb{Q}] = p - 1$.

Untuk mengilustrasikan kasus dimana n bukan bilangan prima, pertimbangkan $n = 6$. Maka

$$x^6 - 1 = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1)$$

mempunyai akar-akar 1 dan

$$\begin{aligned}
\xi_6 &= \cos(\frac{2\pi}{6}) + i\sin(\frac{2\pi}{6}) = \frac{1 + \sqrt{3}i}{2} = -\omega^2 \\
\xi_6^2 &= \frac{-1 + \sqrt{3}i}{2} = \omega \\
\xi_6^3 &= -1 \\
\xi_6^4 &= \frac{-1 - \sqrt{3}i}{2} = \omega^2 \\
\xi_6^5 &= \frac{1 - \sqrt{3}i}{2} = -\omega.
\end{aligned}$$

Perhatikan bahwa $1, \xi_6^2$ dan ξ_6^4 adalah akar-akar dari $x^3 - 1$, tetapi juga ξ_6^2 dan ξ_6^4 adalah akar-akar dari $x^2 + x + 1$, sedangkan $-1, \xi_6$ dan ξ_6^5 adalah adalah akar-akar dari $x^3 + 1$, tetapi juga ξ_6 dan ξ_6^5 adalah akar-akar dari $x^2 - x + 1$.

Lapangan $\mathbb{Q}(\xi_6) = \mathbb{Q}(\sqrt{3}i)$ memuat keenam akar-akar tsb dan merupakan lapangan pemecah dari $x^6 - 1$ atas $\mathbb{Q}$, jadi dalam hal ini lapangan pemecah ini memiliki derajat $[Q(\xi_6) : \mathbb{Q}] = 2$.

Definisi 10.3.3 Suatu generator dari grup siklik dari akar-akar tingkat-n dari satuan disebut suatu **akar primitif tingkat-n dari satuan**. Ada sebanyak $\phi(n)$ akar-akar primitif tingkat-n dari satuan, dimana ϕ adalah fungsi Euler.

Definisi 10.3.4 Untuk setiap $n > 0$ **polinomial siklotomik tingkat-n**, $\Phi_n(x)$ adalah polinomial monik yang akar-akarnya adalah akar-akar primitif tingkat-n dari satuan:

$$\Phi_n(x) = (x - \xi_1) \cdots (x - \xi_{\phi(n)})$$

dimana $\xi_1, \ldots, \xi_{\phi(n)}$ adalah $\phi(n)$ akar-akar primitif tingkat-n dari satuan.

Contoh 10.3.7 Dalam notasi Contoh 10.3.6, akar-akar primitif tingkat-6 dari satuan adalah ξ_6 dan ξ_6^5. Oleh karena itu $\Phi_6(x) = x^2 - x + 1$. Perhatikan bahwa $\Phi_6(x) \in \mathbb{Z}[x]$ dan

$$\begin{aligned}
\deg \Phi_6(x) &= [\mathbb{Q}(\xi_6) : \mathbb{Q}] = 2 = \phi(6) \\
x^6 - 1 &= (x^3 - 1)(x^3 + 1) \\
&= (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1) \\
&= \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x) \\
&= \prod_{d|6} \Phi_d(x).
\end{aligned}$$

Proposisi kita selanjutnya menyatakan bahwa hubungan terakhir hasil ini berlaku secara umum.

Proposisi 10.3.4 Untuk setiap $n > 0$, kita mempunyai

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

Bukti
Sebagai Latihan! ∅

Contoh 10.3.8 Mari kita pertimbangkan apa Definisi 10.3.3 dan 10.3.4 dalam kasus khusus $n = p$ prima. Karena setiap elemen kecuali identitas dalam grup siklik orde prima adalah generator, maka semua akar-akar tingkat-p dari satuan kecuali akar trivial 1 adalah akar-akar primitif tingkat-p dari satuan. Dalam Definisi 8.4.3 kita mendefinisikan polinomial siklotomik $\Phi_p(x)$ dalam kasus khusus suatu bilangan prima p. Definisi 10.3.4 berlaku untuk sebarang n tetapi sesuai dengan Definisi 8.4.3 kita sebelumnya untuk bilangan-bilangan prima. Karena dengan Proposisi 10.3.4, maka

$$x^p - 1 = \Phi_1(x)\Phi_p(x) = (x-1)\Phi_p(x),$$

tetapi

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1)$$

dan, juga

$$\Phi_p(x) = (x^{p-1} + x^{p-2} + \cdots + x^2 + x + 1)$$

yang merupakan definisi kita sebelumnya dalam kasus khusus suatu bilangan prima. Menurut Akibat 8.4.2, polinomial ini terbukti tak-tereduksi atas $\mathbb{Q}$. Dalam kasus p suatu bilangan prima, semua akar-akar tingkat-p dari satuan kecuali akar trivial 1 itu sendiri adalah akar dari polinomial tak-tereduksi $\Phi_p(x)$ berderajat $p-1$ atas $\mathbb{Q}$, dan karenanya semua akar-akar tak-trivial tingkat-p memiliki derajat $p-1$ atas $\mathbb{Q}$. ●

Contoh 10.3.9 Misalkan p adalah suatu bilangan prima dan pertimbangkan lapangan pemecah di $\mathbb{C}$ dari $f(x) = x^p - 3$ atas $\mathbb{Q}$. Jika α adalah akar dari $f(x)$, maka $\alpha^p = 3$ dan karenanya $(\alpha\xi)^p = 3$ dimana ξ adalah akar tingkat-p dari satuan. Jadi, lapangan pemecah dalam kasus ini adalah $\mathbb{Q}(3^{\frac{1}{p}}, \xi)$ dimana ξ adalah sembarang akar tak-trivial tingkat-p dari satuan. Perhatikan bahwa $3^{\frac{1}{p}}$ masih memiliki derajat p atas $\mathbb{Q}(\xi)$, karena jika memiliki derajat $m < p$ kita akan memiliki

$$[\mathbb{Q}(3^{\frac{1}{p}}, \xi) : \mathbb{Q}] = [\mathbb{Q}(3^{\frac{1}{p}}, \xi) : \mathbb{Q}(\xi)] \cdot [\mathbb{Q}(\xi) : \mathbb{Q}] = m(p-1)$$

yang tidak mungkin karena menurut Akibat 10.2.2, $p = \deg_{\mathbb{Q}}(3^{\frac{1}{p}})$ membagi $[\mathbb{Q}(3^{\frac{1}{p}}, \xi) : \mathbb{Q}]$, tetapi bilangan prima p tidak dapat membagi suatu hasil perkalian $m(p-1)$. Jadi dalam hal ini kita memiliki lapangan pemecah

$$[\mathbb{Q}(3^{\frac{1}{p}}, \xi) : \mathbb{Q}] = [\mathbb{Q}(3^{\frac{1}{p}}, \xi) : \mathbb{Q}(\xi)] \cdot [\mathbb{Q}(\xi) : \mathbb{Q}] = p(p-1)$$

dan derajat lapapangan pemecahan ini adalah $p(p-1)$, yaitu $< p!$ untuk semua bilangan prima $p > 3$. ●

Contoh 10.3.10 Kita mendapatkan lapangan pemecah dari polinomial $x^5 - 1$ atas $\mathbb{Q}$ dengan dua metode berbeda.

Metode Pertama: Misalkan

$$\xi = \cos(\frac{2\pi}{5}) + i\sin(\frac{2\pi}{5}) = a + bi$$

Maka $(a + bi)^5 = 1$. Mengambil bagian real dan imajiner, kita memperoleh

$$a^5 - 10b^2a^3 + 5b^4a = l.$$

Karena

$$a^2 + b^2 = \cos^2(\frac{2\pi}{5}) + \sin^2(\frac{2\pi}{5}) = 1,$$

maka kita mempunyai

$$a^5 - 10(1 - a^2)a^3 + 5(1 - a^2)a = 1 \Rightarrow 16a^5 - 20a^3 + 5a - 1 = 0.$$

Oleh karena itu $a = \cos(\frac{2\pi}{5})$ adalah suatu akar dari polinomial

$$f(x) = 16x^5 - 20x^3 + 5x - 1.$$

Tetapi kita punya faktorisasinya

$$f(x) = (x - 1)(4x^2 + 2x - 1)^2.$$

Dengan menggunakan rumus persamaan kuadrat, kita peroleh

$$\begin{aligned} \cos(\frac{2\pi}{5}) &= \frac{-1 + \sqrt{5}}{2} \\ \sin(\frac{2\pi}{5}) &= \frac{\sqrt{10 + 2\sqrt{5}}}{4}. \end{aligned}$$

Karena itu,

$$\xi = \frac{-1 + \sqrt{5}}{2} + i\frac{\sqrt{10 + 2\sqrt{5}}}{4}$$

dan lapangan pemecah dari $x^5 - 1$ adalah $\mathbb{K} = \mathbb{Q}\left(\sqrt{5}, i\sqrt{10 + 2\sqrt{5}}\right)$. Perhatikan bahwa $[\mathbb{K} : \mathbb{Q}] = 4$, sesuai dengan Contoh 10.3.8.

Metode Kedua: Kita mempunyai

$$x^5 - 1 = (x - 1)\Phi_5(x) = (x - 1)(x^4 + x^3 + x^2 + x + 1)$$

dan kita ingin menyelesaikan kuartik $\Phi_5(x)$. Menggunakan notasi yang kita kembangkan di Bagian 8.5 untuk polinomial kuartik, kubik pembantu (sebagaimana diberikan dalam Definisi 8.5.2) dalam hal ini adalah

$$g(k) = 8k^3 - 4k^2 - 6k + 2$$

dan $k = 1$ adalah suatu akar dari $g(k)$. Karena itu

$$h = \frac{1}{2}, \quad u = \frac{\sqrt{5}}{2} \quad \text{dan} \quad v = 0,$$

dan

$$\begin{aligned}\Phi_5(x) &= \left(x^2+\frac{1}{2}x+1+\frac{\sqrt{5}}{2}x\right)\left(x^2+\frac{1}{2}x+1-\frac{\sqrt{5}}{2}x\right)\\ &= \left(x^2+\frac{1+\sqrt{5}}{2}x+1\right)\left(x^2+\frac{1-\sqrt{5}}{2}x+1\right)\end{aligned}$$

dan akhirnya, dengan menggunakan rumus persamaan kuadrat, kita memperoleh empat akar-akar dari $\Phi_5(x)$:

$$\xi = \frac{-1+\sqrt{5}}{2}+\frac{\sqrt{10+2\sqrt{5}}}{4}\,i$$

dan ξ^2, ξ^3, ξ^4. ●

Misalkan $\mathbb{F}$ suatu lapangan, $f(x) \in \mathbb{F}[x]$ suatu polinomial tak-konstan. Kita telah menunjukkan bahwa ada suatu lapangan perluasan dari $\mathbb{F}$ dimana $f(x)$ terpecah, dan bahwa dalam lapangan perluasan tersebut ada suatu lapangan pemecah untuk $f(x)$ atas $\mathbb{F}$. Jika kita memiliki dua lapangan perluasan dari $\mathbb{F}$ maka kita memiliki suatu lapangan pemecah dari $f(x)$ atas $\mathbb{F}$ di masing-masing lapangan. Selanjutnya kita buktikan bahwa kedua lapangan pemecah ini isomorpik: lapangan pemecah dari $f(x)$ atas $\mathbb{F}$ tunggal hingga isomorpisma.
Buktinya dibagi menjadi dua langkah.
Diberikan dua lapangan $\mathbb{F}$ dan $\mathbb{F}'$ dan suatu isomorpisma $\phi : F \to \mathbb{F}'$, isomorpisma yang diinduksi $\phi^* : \mathbb{F}[x] \to \mathbb{F}'[x]$, memetakan setiap elemen

$$f(x) = a_n x^n + \cdots + c_1 x + c_0 \in \mathbb{F}[x]$$

ke

$$\phi^*(f(x)) = \phi(a_n)x^n + \cdots + \phi(c_1)x + \phi(c_0) \in \mathbb{F}'[x].$$

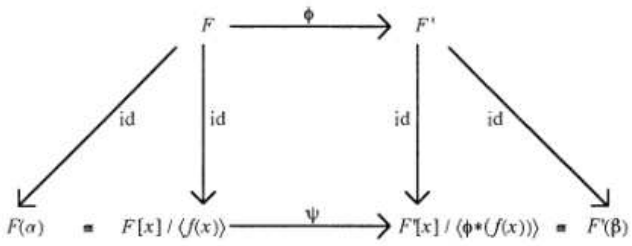
Teorema 10.3.2 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $f(x) \in \mathbb{F}[x]$ tak-tereduksi. Misalkan α adalah suatu akar dari $f(x)$ di beberapa lapangan perluasan dari $\mathbb{F}$. Jika $\mathbb{F}'$ adalah suatu lapangan lain dan $\phi : \mathbb{F} \to \mathbb{F}'$ adalah isomorpisma, dan jika β adalah suatu akar dari $\phi^*(f(x))$ *di*$\mathbb{F}'[x]$ di beberapa lapangan perluasan dari $\mathbb{F}'$ maka ada suatu isomorpisma $\phi^\dagger : \mathbb{F}(\alpha) \to \mathbb{F}'(\beta)$ sedemikian rupa sehingga

(1) $\phi^\dagger$ sesuai dengan ϕ adalah **pada** $\mathbb{F}$, yaitu, $\phi^\dagger(c) = \phi(c)$ untuk semua $c \in \mathbb{F}$.

(2) $\phi^\dagger(\alpha) = \beta$.

Bukti
Buktinya mengacu pada Gambar 10.2. Supaya lebih memudahkan, untuk $g(x) \in \mathbb{F}[x]$ tertentu kita menulis menulis $g'(x)$ sebagai notasi ringkas untuk $\phi^*(g(x)) \in \mathbb{F}'[x]$· Perhatikan bahwa karena ϕ^* adalah isomorpisma, $g(x)$ dan $g'(x)$ memiliki derajat yang sama. Pertama kita perhatikan bahwa $f'(x) = \phi^*(f(x))$ tak-tereduksi atas $\mathbb{F}'$. Karena jika kita memiliki faktorisasi $f'(x) = g'(x)h'(x) \in \mathbb{F}'[x]$, dimana kedua faktor memiliki derajat lebih kecil dari $f'(x)$, maka karena ϕ^* adalah isomorpisma kita miliki

$$\phi^*(f(x)) = f'(x) = g'(x)h'(x) = \phi^*(g(x))\phi^*(h(x)) = \phi^*(g(x)h(x))$$



Gambar 10.2: Diagram $F(\alpha) \cong \mathbb{F}'(\beta)$

maka kita akan memiliki faktorisasi $f(x) = g(x)h(x) \in \mathbb{F}[x]$ dimana kedua faktor memiliki derajat lebih kecil dari $f(x)$, yang tidak mungkin karena $f(x)$ tak-tereduksi atas $\mathbb{F}$. Oleh karena itu, $f'(x)$ tak-tereduksi atas $\mathbb{F}'$ dan $\mathbb{F}[x]/\langle f(x)\rangle$ serta $F'[x]/\langle f'(x)\rangle$ keduanya lapangan. Kita mendefinisikan pemetaan

$$\psi : \mathbb{F}[x]/\langle f(x)\rangle \to \mathbb{F}'[x]/\langle f'(x)\rangle$$

dengan

$$\psi(g(x) + \langle f(x)\rangle) = g'(x) + \langle f'(x)\rangle, \ \forall g(x) + \langle f(x)\rangle \in \mathbb{F}[x]/\langle f(x)\rangle.$$

Maka ψ adalah suatu isomorpisma. Berdasarkan Teorema 10.2.11, bagian (1), $\mathbb{F}(\alpha)$ dan $\mathbb{F}[x]/\langle f(x)\rangle$ isomorpik, begitu juga $F'(\beta)$ dan $\mathbb{F}'[x]/\langle f'(x)\rangle$. Ambil isomorpisma dalam arah dari $\mathbb{F}(\alpha)$ ke $\mathbb{F}[x]/\langle f(x)\rangle$ dan isomorpisma dalam arah dari $\mathbb{F}'[x]/\langle f'(x)\rangle$ to $\mathbb{F}'(\beta)$, dan tentukan $\phi^\dagger$ sebagai komposisinya, seperti di bagian bawah Gambar 10.2. Untuk sebarang elemen $h(\alpha) \in \mathbb{F}(\alpha)$, $h(\alpha)$ pertama dibawa ke $h(x) + \mathbb{F}[x]/\langle f(x)\rangle$ oleh isomorpisma dari $\mathbb{F}(\alpha)$ ke $\mathbb{F}[x]/\langle f(x)\rangle$ lalu ke $h'(x) + \langle f'(x)\rangle$ oleh ψ, lalu ke $h'(\beta)$ dengan isomorpisma dari $\mathbb{F}'[x]/\langle f'(x)\rangle$ ke $\mathbb{F}'(\beta)$ atau, dalam diagram

$$\phi^\dagger : h(\alpha) \to h(x) + \mathbb{F}[x]/\langle f(x)\rangle \to h'(x) + \langle f'(x)\rangle \to h'(\beta).$$

Menerapkan diagram ini ke polinomial konstan $h(x) = c \in \mathbb{F}$, dimana $h'(x) = \phi^*(h(x)) = \phi(c)$, kita mempunyai

$$\phi^\dagger : c \to c + \mathbb{F}[x]/\langle f(x)\rangle \to c + \langle f'(x)\rangle \to \phi(c).$$

Menerapkannya ke polinomial $h(x) = x$, dimana $h'(x) = \phi^*(h(x)) = x$, kita dapatkan

$$\phi^\dagger : \alpha \to x + \mathbb{F}[x]/\langle f(x)\rangle \to x + \langle f'(x)\rangle \to \beta.$$

Ini adalah kondisi (1) dan (2) yang diperlukan untuk $\phi^\dagger$ dalam pernyataan teorema. ✓

Teorema 10.3.3 Misalkan $\mathbb{F}$ suatu lapangan, $f(x) \in \mathbb{F}[x]$ suatu polinomial tak-konstan, dan $\mathbb{K}$ suatu lapangan pemecah untuk $f(x)$ atas $\mathbb{F}$. Jika $\mathbb{F}'$ adalah suatu lapangan lain dan $\phi : \mathbb{F} \to \mathbb{F}'$ adalah suatu isomorpisma, dan jika $\mathbb{K}'$ adalah suatu lapangan pemecah untuk $\phi^*(f(x))$ atas $\mathbb{F}'$, maka terdapat isomorpisma $\phi^\ddagger; \mathbb{K} \to \mathbb{K}'$ sedemikian rupa sehingga $\phi^\ddagger$ sesuai dengan ϕ **pada** $\mathbb{F}$.

Bukti
Kita menggunakan induksi pada derajat n dari $f(x)$. Jika $n = 1$, maka $\mathbb{K} = \mathbb{F}, \mathbb{K}' = \mathbb{F}'$ dan kita dapat mengambil $\phi^\ddagger = \phi$. Jadi asumsikan sebagai hipotesis induksi bahwa teorema

berlaku untuk polinomial derajat $n-1$. Misalkan $p(x)$ merupakan faktor tak-tereduksi dari $f(x)$. Dengan Teorema 10.3.2, jika $\alpha \in \mathbb{K}$ adalah suatu akar dari $p(x)$ dan $\beta \in \mathbb{K}'$ adalah suatu akar dari $\phi^*(p(x))$, maka ada isomorpisma $\phi^\dagger : \mathbb{F}(\alpha) \to \mathbb{F}'(\beta)$ yang sesuai dengan ϕ **pada** $\mathbb{F}$ dan memiliki $\phi^\dagger(\alpha) = \beta$. Isomorpisma ini menghasilkan isomorpisma induksi $\chi : \mathbb{F}(\alpha)[x] \to \mathbb{F}'(\beta)[x]$ yang sesuai dengan ϕ^* **pada** $\mathbb{F}[x]$. Sekarang perhatikan faktorisasinya

$$f(x) = (x-\alpha)g(x) \in \mathbb{F}(\alpha)[x]$$

dimana $g(x)$ memiliki derajat $n-1$. Ini besesuaian dengan suatu faktorisasi

$$\chi(f(x)) = \phi^*(f(x)) = (x-\beta)\chi(g(x)) \in \mathbb{F}'(\beta)[x].$$

Sekarang $\mathbb{K}$ adalah lapangan pemecah dari $g(x)$ atas $\mathbb{F}(\alpha)$ dan $\mathbb{K}'$ adalah suatu lapangan pemecah dari $\chi(g(x))$ atas $\mathbb{F}'(\beta)$. Jadi hipotesis induksi menyiratkan ada isomorpisma $\phi^\ddagger : \mathbb{K} \to \mathbb{K}'$ yang sesuai dengan $\phi^\dagger$ **pada** $\mathbb{F}(\alpha)$ dan karena itu sesuai dengan ϕ **pada** $\mathbb{F}$.

Ketunggalan lapangan pemecah hingga isomorpisma mengikuti kesimpulan berikut.

Akibat 10.3.1 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x) \in \mathbb{F}[x]$ suatu polinomial tak-konstan, $\mathbb{K}$ dan $\mathbb{K}'$ dua lapangan pemecah untuk $f(x)$ atas $\mathbb{F}$. Maka $\mathbb{K}$ dan $\mathbb{K}'$ isomorpik.

Bukti
Terapkan Teorema 10.3.3 dengan $\mathbb{F}' = \mathbb{F}$ dan ϕ = identitas.

Dengan menggunakan teorema Kronecker, kita dapat menunjukkan bahwa setiap polinomial memiliki suatu lapangan pemecah. Dalam semua contoh polinomial kita berada di $\mathbb{Q}[x]$ dan $\mathbb{R}[x]$, lapangan pemecah semuanya adalah sublapangan dari $\mathbb{C}$. Kita tidak menemukan perluasan aljabar $\mathbb{C}$ (selain $\mathbb{C}$ itu sendiri). Faktanya, tidak ada. Fakta ini, dikenal sebagai teorema dasar aljabar. Kita menyertakan pernyataan dan beberapa konsekuensi langsungnya di bagian ini karena hubungannya yang erat dengan teorema dan contoh di bagian ini.

Definisi 10.3.5 Suatu lapangan $\mathbb{F}$ **tertutup secara aljabar** jika setiap polinomial tak-konstan di $\mathbb{F}[x]$ memiliki suatu akar di $\mathbb{F}$.

Teorema berikut memungkinkan kita untuk menggunakan empat definisi ekivalen dari suatu lapangan tertutup secara aljabar.

Teorema 10.3.4 Misalkan $\mathbb{F}$ adalah sebarang lapangan. Maka pernyataan pernyataan berikut adalah ekivalen:

(1) $\mathbb{F}$ adalah tertutup secara aljabar.

(2) $f(x) \in \mathbb{F}[x]$ adalah tak-tereduksi jika dan hanya jika deg $f(x) = 1$.

(3) Setiap polinomial buka konstan di $\mathbb{F}[x]$ terpisah atas $\mathbb{F}$.

(4) Bila $\mathbb{E}$ adalah suatu perluasan aljabar dari $\mathbb{F}$ maka $\mathbb{E} = \mathbb{F}$.

Bukti

(1) (1) $\Rightarrow$ (2) Sebagai Latihan!

(2) (2) $\Rightarrow$ (3) Sebagai Latihan!

(3) (2) $\Rightarrow$ (4) Misalkan $\mathbb{E}$ adalah suatu perluasan aljabar dari $\mathbb{F}$ dan misalkan $\alpha \in \mathbb{E}$ Maka α adalah aljabar atas $\mathbb{F}$, jadi $f(\alpha) = 0$ untuk beberapa polinomial tak-nol $f(x) \in \mathbb{F}[x]$. Jadi $f(x)$ adalah polinomial bukan-konstan, dan dengan (3) kita memiliki suatu pemecahan atas $\mathbb{F}$:

$$f(x) = u(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n)$$

dimana setiap $\alpha_i \in \mathbb{F}$. Karena $f(\alpha) = 0$, maka $x - \alpha$ harus membagi $f(x)$ dan harus sama dengan salah satu faktor $(x - \alpha_i)$. Tapi ini berarti $\alpha = \alpha_i \in \mathbb{F}$. Ini menunjukkan $\mathbb{E} \subseteq \mathbb{F}$ dan oleh karena itu $\mathbb{F} = \mathbb{E}$.

(4) (4) $\Rightarrow$ (1) Misalkan $f(x)$ adalah suatu polinomial bukan konstan di $\mathbb{F}[x]$ dan misalkan α adalah suatu akar dari $f(x)$ di beberapa perluasan dari $\mathbb{F}$. Maka $\mathbb{F}(\alpha)$ adalah suatu perluasan aljabar dari $\mathbb{F}$, dengan (4) kita memiliki $\mathbb{F}(\alpha) = \mathbb{F}$ dan $\alpha \in \mathbb{F}$. ✓

Teorema 10.3.5 ***(Teorema dasar aljabar)*** Lapangan bilangan kompleks tertutup secara aljabar.

Bukti
Sebagai Latihan! ✓

Akibat 10.3.2 Untuk setiap polinomial bukan konstan $f(x) \in \mathbb{Q}[x]$ terdapat suatu lapangan pemecah $\mathbb{K} \subseteq \mathbb{C}$ untuk $f(x)$ atas $\mathbb{Q}$.

Bukti
Ini langsung dari Teorema 10.3.5, (menggunakan definisi (3) dari tertutup secara aljabar dan Teorema 10.3.4) bersama dengan Proposisi 10.3.2. ✓

Akibat 10.3.3 Jika $\mathbb{E}$ adalah suatu lapangan perluasan dari $\mathbb{C}$ dan $[\mathbb{E} : \mathbb{C}] > 1$, maka $\mathbb{E}$ bukan perluasan aljabar dari $\mathbb{C}$ dan $[\mathbb{E} : \mathbb{C}]$ tidak terbatas..

Bukti
Ini langsung dari Teorema 10.3.5, (menggunakan definisi (4) dari aljabar tertutup dari Teorema 10.3.4) bersama dengan Teorema 10.2.4. ✓

Akibat 10.3.4 Misalkan $f(x) \in \mathbb{R}[x]$ adalah suatu polinomial bukan konstan. Jika $f(x)$ takereduksi atas $\mathbb{E}$, maka $\deg f(x) = 1$ atau 2.
Bukti
Sebagai Latihan! ✓

Latihan

Dalam Latihan 1 hingga 11 dapatkan lapangan pemecah $\mathbb{K}$ dalam $\mathbb{C}$ dari polinomial yang ditunjukkan $f(x)$ atas $\mathbb{Q}$, dan tentukan $[\mathbb{K} : \mathbb{Q}]$.(Petunjuk untuk 8 hingga 11: Gunakan metode Bagian 8.5.)

1. $f(x) = x^4 - 1$. **2.** $f(x) = x^3 + 1$. **3.** $f(x) = x^4 - 4$.

4. $f(x) = x^4 + 1$. **5.** $f(x) = x^3 - 5$. **6.** $f(x) = x^4 - 2x^2 + 1$.

7. $f(x) = x^5 + x^4 + x^3 - x^2 - x - 1$. **8.** $f(x) = x^3 + x + 1$. **9.** $f(x) = x^3 - 3x + 2$.

10. $f(x) = x^4 - 4x^3 + 6x^2 - 4x + 1$. **11.** $f(x) = x^4 - 2x^3 - x + 2$.

12. Misalkan α adalah suatu akar dari $f(x) = x^3 + x^2 + 1$ atas $\mathbb{Z}_2$. Tunjukkan bahwa $f(x)$ terpecah atas $\mathbb{Z}_2(\alpha)$.

13. Buktikan Proposisi 10.3.3.

14. Biarkan $\mathbb{E} = \mathbb{Q}(\sqrt{3}, \sqrt[3]{2}, i)$. Konstruksi suatu ***lattice*** sublapangan untuk $\mathbb{E}$ seperti pada Contoh 10.3.5.

15. Tunjukkan bahwa banyaknya akar-akar primitif tingkat-n dari satuan adalah $\phi(n)$.

16. Hitung polinomial siklotomik $\Phi_n(x)$ untuk semua $\leq n \leq 8$.

17. Misalkan $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \in \mathbb{Z}$ dimana masing-masing p_i bilangan prima berbeda. Tunjukkan bahwa

$$\Phi(n) = \prod_{1 \leq i \leq k} p_i^{a_i - 1}(p_i - 1).$$

18. Dapatkan semua akar tingkat-8 dari satuan dan identifikasi mana yang merupakan akar primitif tingkat-8.

19. Tentukan suatu lapangan pemecah di $\mathbb{C}$ dari $f(x) = x^8 - 2$ atas $\mathbb{Q}$.

20. Misalkan n dan m merupakan bilangan bulat yang relatif prima, ξ_n suatu akar primitif tingkat-n dari satuan, dan ξ_m suatu akar primitif tingkat-m dari satuan. Tunjukkan bahwa $\xi_n \xi_m$ adalah akar primitif tingkat-(mn) dari satuan.

21. Misalkan ξ_n adalah suatu akar primitif tingkat-n dari satuan dan d merupakan pembagi dari n. Tunjukkan bahwa ξ_n^d adalah akar primitif tingkat-$(\frac{n}{d})$ dari satuan.

22. Buktikan Proposisi 10.3.4.

23. Tunjukkan bahwa pemetaan ψ yang didefinisikan dalam pembuktian Teorema 10.3.2 adalah suatu isomorpisma.

24. Buktikan (1) $\Rightarrow$ (2) dalam Teorema 10.3.4.

25. Buktikan (2) $\Rightarrow$ (3) dalam Teorema 10.3.4.

26. Buktikan Akibat 10.3.4.

27. Tunjukkan bahwa lapangan $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha$ adalah aljabar atas $\mathbb{Q}\}$ tertutup secara aljabar.

10.4 Lapangan Berhingga

Kita mengakhiri bab ini tentang teori medan dengan teorema yang indah tentang lapangan berhingga. Kita tunjukkan bahwa sembarang lapangan berhingga $\mathbb{F}$ berorder p^n untuk beberapa p prima dan bilangan bulat positif n dan bahwa lapangan tersebut adalah lapangan pemecah dari polinomial $x^{p^n} - x$ atas $\mathbb{Z}_p$. Kita menggunakan teorema tentang keberadaan dan ketunggalan lapangan pemmecah yang dibuktikan pada bagian sebelumnya untuk menunjukkan bahwa terdapat lapangan, tunggal hingga isomorpisma, dengan order p^n untuk setiap bilangan prima p dan bilangan bulat positif n.

Sebelum menerapkan pekerjaan ini pada lapangan pemecah dari bagian sebelumnya, kita tinjau apa yang kita ketahui tentang lapangan berhingga dari bab-bab sebelumnya dan meringkas apa yang berikut dengan hasil dasar dari dua bagian pertama bab ini.

Proposisi 10.4.1 Misalkan $\mathbb{F}$ adalah suatu lapangan berhingga. Maka

(1) Order dari $\mathbb{F}$ adalah pangkat prima $|\mathbb{F}| = p^n$ dimana = khar($\mathbb{F}$).

(2) $\mathbb{F}$ adalah suatu perluasan aljabar $\mathbb{Z}_p(\alpha)$, dimana α adalah suatu akar dari polinomial monik tak-tereduksi $q(x)$ derajat n atas $\mathbb{Z}_p$.

Bukti

(1) Misalkan $\mathbb{F}$ adalah suatu lapangan berhingga. Karena $\mathbb{F}$ berhingga, karakteristik dari $\mathbb{F}$ adalah prima p dan $\mathbb{Z}_p$ adalah sublapangan dari $\mathbb{F}$ menurut Teorema 7.3.4. Misalkan $n = [\mathbb{F} : \mathbb{Z}_p]$. Maka karena ruang vektor berdimensi n atas lapangan $\mathbb{Z}_p$ dari elemen p memiliki tepat p^n elemen (menjadi isomorpik sebagai ruang vektor dengan $\mathbb{Z}_p^n$ oleh **Latihan 29**, Bagian 10.1), kita memiliki $|\mathbb{F}| = p^n$.

(2) Grup perkalian $\mathbb{F}^*$ dari elemen bukan nol $\mathbb{F}$ adalah siklik menurut Teorema 8.3.4, dan jika α adalah generator, maka setiap elemen bukan nol dari $\mathbb{F}$ sama dengan beberapa pangkat α berada di $\mathbb{Z}_p(\alpha)$. Jadi $\mathbb{F} = \mathbb{Z}_p(a)$ suatu lapangan terkecil yang memuat $\mathbb{Z}_p$ dan α. Berdasarkan Teorema 10.2.2 terdapat dengan tunggal polinomial monik $q(x) \in \mathbb{Z}_p[x]$ tak-tereduksi atas $\mathbb{Z}_p$ dan berderajat n sedemikian rupa sehingga α adalah suatu akar dari $q(x)$ yaitu polinomial minimal dari α atas $\mathbb{Z}_p$. ●

Contoh 10.4.1 Misalkan $\mathbb{F}$ adalah suatu lapangan yang memiliki elemen antara 65 dan 124. Dengan Proposisi 10.4.1, karena satu-satunya pangkat prima dalam rentang ini adalah $81 = 3^4$, maka $\mathbb{F}$ memiliki karakteristik 3, dan $\mathbb{F}$ memiliki elemen 81, dan $\mathbb{F} = \mathbb{Z}_3(\alpha)$, dimana α adalah suatu akar dari polinomial monik tak-tereduksi $q(x) \in \mathbb{Z}_3[x]$ derajat 4. Perhatikan sekarang bahwa karena elemen bukan nol dari $\mathbb{F}$ membentuk grup dengan order 80, maka menurut teorema Lagrange $a^{80} = 1$ untuk semua $a \in \mathbb{F}$ bukan nol. Jadi setiap a tersebut adalah akar dari $x^{80} - 1$ dan $x^{81} - x$, juga 0 merupakan akar dari yang terakhir. Jadi setiap elemen $\mathbb{F}$ adalah akar dari $f(?) = x^{81} - x$, dan $\mathbb{F}$ memuat sebanyak $81 = \deg f(x)$ akar-akar berbeda dari $f(?)$. Oleh karena itu $\mathbb{F}$ adalah suatu lapangan pemecah dari $f(x)$ atas $\mathbb{Z}_3$. Jika sekarang $\mathbb{F}'$ adalah suatu lapangan lain yang mempunyai sebanyak 81 elemen, maka dengan argumen yang sama $\mathbb{F}'$ juga merupakan suatu lapangan pemecah dari $f(x)$ atas $\mathbb{Z}_3$. Dengan Akibat 10.3.1, kita memiliki $\mathbb{F} \cong \mathbb{F}'$. ●

Contoh ini menunjukkan bagaimana kita membuktikan bahwa dua lapangan berhingga dengan order yang sama adalah isomorpik, setengah dari teorema utama bagian ini yang merupakan ketunggalan. Untuk setengah yang lainnya tentang keberadaan, kita menunjukkan bahwa lapangan pemecah dari polinomial $x^{p^n} - x$ atas $\mathbb{Z}_p$ adalah suatu lapangan berorder p^n. Langkah kuncinya adalah menunjukkan bahwa akar dari polinomial ini semuanya berbeda, dan untuk langkah ini gagasan utama yang perlu kita perkenalkan adalah **turunan** dari suatu polinomial.

Definisi 10.4.1 Misalkan $\mathbb{F}$ adalah suatu lapangan dan $f(x) \in \mathbb{F}[x]$ suatu polinomial

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_i x^i + \cdots + a_1 x + a_0.$$

Maka **turunan** dari $f(x)$ adalah polinomial

$$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + ia_i x^{i-1} + \cdots + a_1 \in \mathbb{F}[x].$$

Perhatikan bahwa dalam kasus polinomial konstan $f(x) = a_0$ turunannya adalah polinomial nol $f'(x) = 0$.

Perhatikan bahwa sementara dalam kalkulus, turunan terdefinisi untuk fungsi polinomial dan fungsi lain dari $\mathbb{R}$ ke $\mathbb{R}$, definisi aljabar turunan berlaku untuk polinomial atas sebarang lapangan dan tidak melibatkan gagasan limit. Tentu saja, kita tidak dapat mengandalkan bukti dari kalkulus aturan dasar untuk menghitung turunan tetapi harus memberikan bukti baru berdasarkan definisi baru kita.

Proposisi 10.4.2 Misalkan $\mathbb{F}$ adalah suatu lapangan, $c \in \mathbb{F}$ suatu elemen di $\mathbb{F}$, dan $f(x), g(x) \in \mathbb{F}[x]$ polinomial atas $\mathbb{F}$. Maka

(1) $[cf(x)]' = cf'(x)$

(2) $[f(x) + g(x)]' = f'(x) + g'(x)$

(3) $[f(x)g(x)]' = f(x)g'(x) + f'(x)g(x)$

(4) $[(x-c)^n]' = n(x-c)^{n-1}$.

Bukti
(1) dan (2) Langsung dari Definisi 10.4.1.
(3) Untuk sembarang polinomial $h(x) = a_n x^n + \cdots + a_i x^i + + a_1 x + a_0$, kita definisikan

$$\begin{aligned} h_0(u,v) &= (h(u) - h(v))/(u-v) \\ &= \left(a_n(u^n - v^n) + \cdots + a^2(u^2 - v^2) + a_1(u-v)\right)/(u-v) \\ &= a_n[u^{n-1} + u^{n-2}v + \cdots + uv^{n-2} + v^{n-1}] + \cdots + a_2(u+v) + a_1. \end{aligned}$$

Maka $h'(x) = h(x,x)$. Sekarang kita terapkan ini pada $f(x), g(x)$ dan $h(x) = f(x)g(x)$. Kita mempunyai

$$\begin{aligned} h_0(u,v) &= (f(u)g(u) - f(v)g(v))/(u-v) \\ &= (f(u)g(u) - f(u)g(v) + f(u)g(v) - f(v)g(v))/(u-v) \\ &= f(u)[(g(u) - g(v))/(u-v)] + g(v)[(f(u) - f(v))/(u-v)] \\ &= f(u)g_0(u,v) + f_0(u,v)g(v). \end{aligned}$$

Dan karenanya

$$h'(x) = h_0(x,x) = f(x)g_0(x,x) + f_0(x,x)g(x) = f(x)g'(x) + f'(x)g(x).$$

(4) Kita melanjutkan dengan induksi pada n. Untuk $n = 1$, jika $f(x) = (x-c)^1 = x - c$, maka $f'(x) = 1 = 1 \cdot (x-c)^0$. Sekarang asumsikan (4) berlaku untuk $n-1$. Jika $f(x) = (x-c)^n = (x-c)(x-c)^{n-1}$ maka dengan (3) kita dapatkan

$$f'(x) = (n-1)(x-c)(x-c)^{n-2} + 1 \cdot (x-c)^{n-1} = n(x-c)^{n-1},$$

seperti yang dikehendaki. ✓

Contoh 10.4.2 Perhatikan polinomial

$$f(x) = (x-2)^3(x-1)^2(x+1) \in \mathbb{Q}[x].$$

Dalam terminologi Definisi 8.3.1, 2 adalah akar dari $f(x)$ rangkap 3, 1 adalah akar rangkap 2, dan -1 adalah akar rangkap 1. Kita hitung turunan dari $f(x)$ menggunakan bagian (3) dan (4) dari Proposisi 10.4.2.

$$\begin{aligned} f'(x) &= (x-2)^3[(x-1)^2 + 2(x-l)(x+1)] + 3(x-2)^2[(x-1)^2(x+1)] \\ &= (x-2)^2(x-1)[(x-2)(x-1) + 2(x-2)(x+1) + 3(x-1)(x-1)] \end{aligned}$$

Oleh karena itu $f'(2) = f'(1) = 0$, sedangkan $f'(-1) = -108 \neq 0$. Oleh karena itu, akar-akar dari $f(x)$ dengan rangkap yang lebih besar dari 1 adalah akar-akar dari $f(x)$ yang juga merupakan akar-akar dari $f'(x)$. ●

Teorema 10.4.1 Misalkan $\mathbb{F}$ adalah suatu lapangan, $f(x) \in \mathbb{F}[x]$ polinomial, dan α akar dari $f(x)$ di beberapa lapangan perluasan dari $\mathbb{F}$. Maka α adalah akar dari $f(x)$ dengan rangkap $s > 1$ jika dan hanya jika α adalah akar dari $f'(x)$.

Bukti
($\Rightarrow$) Jika α adalah elemen dari beberapa lapangan perluasan $\mathbb{E}$ dari $\mathbb{F}$ dan α adalah akar dari $f(x)$ dengan rangkap $s > 1$, maka menurut Definisi 8.3.1 ini berarti bahwa dalam $\mathbb{E}[x]$ kita memiliki

$$f(x) = (x-\alpha)^s g(x),$$

dimana $g(\alpha) \neq 0$. Maka

$$f'(x) = (x-\alpha)^s g'(x) + s(x-\alpha)^{s-1} g(x),$$

dan $f'(\alpha) = 0$.
($\Leftarrow$) Jika α adalah suatu akar dari $f(x)$ dengan multiplisitas $s = 1$, maka dalam $\mathbb{E}[x]$ kita memiliki faktorisasi

$$f(x) = (x-\alpha)g(x),$$

dimana $g(\alpha) \neq 0$. Maka

$$f'(x) = (x-\alpha)g'(x) + g(x)$$

dan $f'(\alpha) = g(\alpha) \neq 0$. ✓

Contoh 10.4.3 Pertimbangkan $f(x) = x^8 - 1 \in \mathbb{Z}_3[x]$. Maka $f'(x) = 8x^7$ dan $f'(\alpha) = 0$ jika dan hanya jika $\alpha = 0$. Tetapi $f(0) = -1 \neq 0$. Oleh karena itu $f(x)$ dan $f'(x)$ tidak memiliki akar secara bersama. Oleh karena itu dengan Proposisi sebelumnya, semua akar-akar dari $f(x)$ memiliki multiplisitas 1, dan $f(x)$ memiliki 8 akar-akar yang berbeda dalam lapangan pemecahnnya atas $\mathbb{Z}_3$, dan $g(x) = x^9 - x$ yang memiliki akar tambahan 0, oleh karena itu memiliki 9 akar-akar yang berbeda di lapangan pemecahnya atas $\mathbb{Z}_3$. ●

Contoh ini mengilustrasikan bagaimana kita membuktikan keberadaan perluasan dari $\mathbb{Z}_p$ yang memiliki setidaknya p^n elemen untuk setiap p prima dan bilangan bulat positif n. Untuk membuktikan keberadaan suatu lapangang dengan tepat mempunyai sebanyak p^n elemen, kita menggunakan suatu pemetaan penting. Ingat dari Bagian 7.1 (**Latihan 7.1.7**) bahwa jika $\mathbb{F}$ adalah suatu lapangan dengan karakteristik p maka pemeta $\phi : \mathbb{F} \to \mathbb{F}$ didefinisikan oleh $\phi(\alpha) = \alpha^p$ untuk semua $\alpha \in \mathbb{F}$ disebut **pemetaan Frobenius** adalah suatu homomorpisma.

Proposition 10.4.1 Misalkan $\mathbb{F}$ adalah suatu lapangan berhingga mempunyai karakteristik p. Maka pemetaan Frobenius $\phi : \mathbb{F} \to \mathbb{F}$ adalah automorpisma dari $\mathbb{F}$.

Bukti
Menurut **Latihan 7.1.7** dari Bagian 7.1, ϕ adalah homomorpisma. Untuk menunjukkan bahwa ϕ adalah isomorpisma, tinggal ditunjukkan bahwa ϕ adalah satu-satu (dan karena itu pada). Untuk ini lihat Latihan 21 di akhir bagian ini. ✓

Kita sekarang memiliki semua alat yang diperlukan untuk membuktikan teorema utama pada lapangan berhingga yang dijanjikan dalam diskusi sebelumnya.

Teorema 10.4.2 Misalkan p adalah suatu bilangan prima dan n bilangan bulat positif. Maka $\mathbb{F}$ adalah suatu lapangan berhingga berorder p^n jika dan hanya jika $\mathbb{F}$ adalah suatu lapangan pemecah dari $f(x) = x^{p^n} - x$ atas $\mathbb{Z}_p$.

Bukti
($\Rightarrow$) Jika $\mathbb{F}$ adalah suatu lapangan berhingga dengan $|\mathbb{F}| = p^n$ maka $\mathbb{F}^* = \mathbb{F} - \{0_\mathbb{F}\}$ adalah grup perkalian berorder $p^n - 1$, dan dengan teorema Lagrange, kita mempunyai $\alpha^{p^n-1} = 1_\mathbb{F}$ untuk semua $\alpha \in \mathbb{F}^*$. Oleh karena itu $\alpha^{p^n} - \alpha = 0_\mathbb{F}$ untuk semua $\alpha \in \mathbb{F}$, dan sebanyak p^n elemen-elemen di $\mathbb{F}$ semuanya adalah akar-akar yang berbeda dari $f(x) = x^{p^n} - x \in \mathbb{F}[x]$. Jadi $\mathbb{F}$ adalah suatu lapangan pemecah dari $f(x)$ atas $\mathbb{Z}_p$.
($\Leftarrow$) Misalkan $\mathbb{F}$ adalah suatu lapangan pemecah dari $f(x) = x^{p^n} - x$ atas $\mathbb{Z}_p$ dan misalkan

$$\mathbb{K} = \{\alpha \in \mathbb{F} \mid f(\alpha) = 0_\mathbb{F}\}$$

himpunan bagian dari $\mathbb{F}$ yang terdiri dari akar-akar dari $f(x)$. Perhatikan bahwa $f'(x) = -1_\mathbb{F} \neq 0_\mathbb{F}$; maka semua akar-akar dari $f(x)$ memiliki rangkap 1, dengan demikian $f(x)$ memiliki sebanyak p^n akar-akar yang berbeda. Jadi, $|\mathbb{K}| = p^n$. Jika kita dapat menunjukkan bahwa $\mathbb{K}$ adalah suatu lapangan, maka kita akan memiliki $\mathbb{F} = \mathbb{K}$ karena itu $\mathbb{K} \subseteq \mathbb{F}$ keduanya merupakan lapangan pemecah dari $f(x)$. Pertimbangkan automorpisma Frobenius $\phi : \mathbb{F} \to \mathbb{F}$. Maka karena $\phi^n(\alpha) = \alpha^{p^n}$ dan $\alpha \in \mathbb{K}$ jika dan hanya jika $f(\alpha) = \alpha^{p^n} - \alpha = 0_\mathbb{F}$, kita mempunyai

$$\mathbb{K} = \{\alpha \in \mathbb{F} \mid \phi^n(\alpha) = 0_\mathbb{F}\}.$$

Maka $\mathbb{K}$ adalah suatu sublapangan dari $\mathbb{F}$. (Lihat Latihan 22). Oleh karena itu, $\mathbb{K}$ adalah lapangan dan, seperti yang disebutkan sebelumnya, $\mathbb{F} = \mathbb{K}$ dengan demikian $|\mathbb{F}| = |\mathbb{K}| = p^n$ seperti yang diperlukan. ✓

Akibat 10.4.1 Diberikan sembarang p prima dan sembarang bilangan bulat positif n

(1) Ada suatu lapangan berhingga $\mathbb{F}$ yang berorder p^n.

(2) Sebarang dua lapangan yang berorder p^n isomorpik.

Bukti
Langsung dari Teorema 10.4.2 dan Teorema 10.3.10 dan Akibat 10.3.23 tentang keberadaan dan ketunggalan dalam arti isomorpisma pada lapangan pemecahnya.

Akibat 10.4.2 Diberikan bilangan bulat positif k

(1) Terdapat suatu lapangan berhingga $\mathbb{F}$ berorder k jika dan hanya jika k adalah pangkat dari bilangan prima p^n.

(2) Setiap dua lapangan berorder k adalah isomorpik.

Bukti
Langsung dari Akibat 10.4.1 dan Proposisi 10.4.1, bagian (1).

Akibat 10.4.3 Diberikan p prima dan sebarang bilangan bulat positif n, maka terdapat polinomial monik $q(x) \in \mathbb{Z}_p[x]$ derajat n yang tak-tereduksi atas $\mathbb{Z}_p$.
Bukti
Langsung dari Akibat 10.4.1 dan Proposisi 10.4.1 bagian (2).

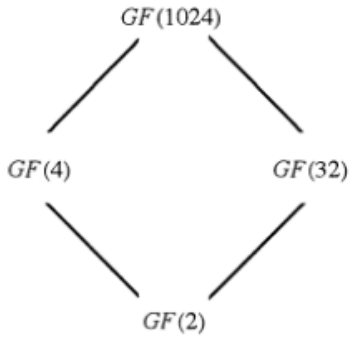
Definisi 10.4.2 Diberikan p prima dan sebarang bilangan bulat positif n, lapangan tunggal (dalam arti isomorpik) berorder p^n dinotasikan sebagai GF(p^n) dan disebut **lapangan Galois** berorder p^n.

Definisi 10.4.3 Diberikan suatu lapangan berhingga $\mathbb{F}$, generator dari grup siklik $\mathbb{F}^*$ disebut **elemen primitif** dari $\mathbb{F}$.

Contoh 10.4.4 (1) Dalam $\mathbb{F} = \text{GF}(7) = \mathbb{Z}_7$, maka $\mathbb{F}^* = \mathbb{U}(7) = \{1, 2, 3, 4, 5, 6\}$, elemen 3 adalah elemen primitif, karena $3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5$, dan $3^6 = 1$. Perhitungan serupa menunjukkan bahwa 5 juga merupakan elemen primitif.
(2) Kita telah membahas $\mathbb{F} = \text{GF}(4) = \mathbb{Z}_2[\alpha] \cong \mathbb{Z}_2[x]/\langle x^2 + x + 1\rangle$ dalam Contoh 8.7.2 dan menuliskan tabel perkaliannya. Elemen α, memenuhi $\alpha^2 + \alpha + 1 = 0$, adalah elemen primitif, karena $\alpha^2 = \alpha + 1$ dan $\alpha^3 = 1$.

Contoh 10.4.5 Kita pertimbangkan $\mathbb{F} = \text{GF}(2^{10})$ dan mengerjakan ***lattice*** sublapangannya $\mathbb{Z}_2 \subseteq \mathbb{F}$ dan $[\mathbb{F} : \mathbb{Z}_2] = 10$. Dengan Teorema 10.2.5, untuk setiap sublapangan $\mathbb{Z}_2 \subseteq \mathbb{E} \subseteq \mathbb{F}$ kita memiliki $[\mathbb{E} : \mathbb{Z}_2] = 1, 2, 5$, atau 10. Dalam kasus pertama dan terakhir masing-masing $\mathbb{E} = \mathbb{Z}_2$ dan $\mathbb{E} = \mathbb{F}$. Dalam dua kasus lainnya, $\mathbb{E} \cong \text{GF}(2^2)$ atau $\mathbb{E} \cong \text{GF}(2^5)$. Karena $\mathbb{E}^*$ adalah subgrup dari $\mathbb{F}^*$ dan grup siklik hanya memiliki satu subgrup dari setiap order yang mungkin, hanya ada satu sublapangan GF(2^{10}) dari order tertentu. Oleh karena itu ***lattice*** sublapangan dari GF(2^{10}) adalah seperti yang ditunjukkan pada Gambar 10.3.

Teorema 10.4.3 Misalkan p adalah suatu bilangan prima dan n bilangan bulat positif.



Gambar 10.3: GF(2^{10})

(1) Jika $\mathbb{E}$ adalah suatu sublapangan dari GF(p^n) maka $\mathbb{E} \cong$ GF(p^r) untuk beberapa r yang membagi n.

(2) Jika r membagi n maka terdapat tunggal suatu sublapangan $\mathbb{E}$ dari GF(p^n) yang memiliki order p^r, diberikan oleh

$$\mathbb{E} = \{\beta \in \text{GF}(p^n) \mid \beta^{p^r} = \beta\}.$$

Bukti

(1) Jika $\mathbb{E}$ adalah suatu sublapangan dari GF(p^n) maka khar($\mathbb{E}$) $= p$ dan $\mathbb{Z}_p$ adalah suatu sublapangan dari $\mathbb{F}$. Jadi dengan Teorema 10.2.5

$$n = [\text{GF}(p^n) : \mathbb{Z}_p] = [\text{GF}(p^n) : \mathbb{E}] \cdot [\mathbb{E} : \mathbb{Z}_p].$$

Oleh karena itu $r = [\mathbb{E} : \mathbb{Z}_p]$ membagi n dan $|\mathbb{E}| = p^r$, jadi $\mathbb{E} \cong$ GF(p^r).

(2) Jika r membagi n maka $p^r - 1$ membagi $p^n - 1$. (Lihat Latihan 10.4.9 **23.**). Grup perkalian $\mathbb{F}^*$ dengan elemen-elemen bukan nol dari $\mathbb{F}$ adalah suatu grup siklik dengan order $p^n - 1$, memiliki tunggal subgrup dengan order d untuk setiap pembagi d dari $p^n - 1$ terdiri dari semua elemen-elemen yang ordernya membagi d. Secara khusus, GF(p^n)* memiliki tunggal subgrup dari grup berorder $p^r - 1$, yaitu

$$\mathbb{E}^* = \{\beta \in \text{GF}(p^n)^* \mid \beta^{p^r-1} = 1_{\mathbb{F}}\}.$$

Maka $\mathbb{E} = \mathbb{E}^* \cup \{0_{\mathbb{F}}\}$ berisi sebanyak p^r akar-akar berbeda dari $g(x) = x^{p^r} - x$ dan, seperti pada bukti Teorema 10.4.2, $\mathbb{E}$ membentuk suatu sublapangan dari $\mathbb{F}$.

Latihan

Latihan 10.4.1 Dalam Latihan **1** hingga **4** buat lapangan $\mathbb{F}$ berorder sebagaimana ditunjukkan oleh N jika memungkinkan.
1. $N = 9$, **2.** $N = 10$, **3.** $N = 15$, **4.** $N = 16$.

Latihan 10.4.2 Dalam Latihan **5** hingga **8** tentukan elemen primitif untuk lapangan yang ditunjukkan oleh $\mathbb{F}$.
5. $\mathbb{F} = \mathbb{Z}_5$, **6.** $\mathbb{F} = \mathbb{Z}_{17}$, **7.** $\mathbb{F} =$ GF(8), **8.** $\mathbb{F} =$ GF(9).

Latihan 10.4.3 Dalam Latihan **9** hingga **12** tentukan banyaknya elemen-elemen primitif yang oleh ditunjukkan lapangan $\mathbb{F}$
9. $\mathbb{F} = GF(9)$, **10.** $\mathbb{F} = GF(19)$, **11.** $\mathbb{F} = GF(27)$, **12.** $\mathbb{F} = GF(32)$.

Latihan 10.4.4 Dalam Latihan **13** hingga **18** buat ***lattice*** sublapangan dari lapangan yang ditunjukkan oleh $\mathbb{F}$.
13. $\mathbb{F} = GF(8)$, **14.** $\mathbb{F} = GF(16)$, **15.** $\mathbb{F} = GF(2^6)$,
16. $\mathbb{F} = GF(2^{12})$, **17.** $\mathbb{F} = GF(3^{18})$, **18.** $\mathbb{F} = GF(5^{30})$.

Latihan 10.4.5 **19.** (**Aturan rantai**) Misalkan $f(x)$ dan $g(x)$ merupakan polinomial dalam $\mathbb{F}[x]$. Menggunakan Definisi 10.4.1, tunjukkan bahwa

$$[f(g(x))]' = f'(g(x))g'(x).$$

Latihan 10.4.6 **20.** Misalkan $\mathbb{F}$ adalah suatu lapangan dengan khar$(F) = p$. Tunjukkan bahwa untuk $a, b \in \mathbb{F}$ dan sembarang bilangan bulat positif i, kita memiliki

$$(a + b)^i = a^i + b^i.$$

Latihan 10.4.7 **21.** Misalkan $\mathbb{F}$ adalah suatu lapangan berhingga dengan khar$(\mathbb{F}) = p$. Tunjukkan bahwa homomorpisma Frobenius $\phi : \mathbb{F} \to \mathbb{F}$ yang didefinisikan oleh $\phi(\alpha) = \alpha^p$ untuk semua $\alpha \in \mathbb{F}$ adalah suatu isomorpisma.

Latihan 10.4.8 **22.** Misalkan $\mathbb{F}$ adalah suatu lapangan berhingga dengan khar$(\mathbb{F}) = p$ dan $\phi : \mathbb{F} \to \mathbb{F}$ automorpisma Frobenius seperti pada Latihan sebelumnya. Tunjukkan bahwa

(a) $\phi^i(\alpha) = \alpha^{p^i}$ untuk semua $\alpha \in \mathbb{F}$ dan sebarang bilangan bulat positip i.

(b) $\mathbb{K} = \{\alpha \in \mathbb{F} \mid \phi^n(\alpha) = \alpha\}$ untuk suatu n tetap adalah suatu sublapangan dari $\mathbb{F}$.

Latihan 10.4.9 **23.** (a) Diketahui bilangan bulat positif r dan s tunjukkan bahwa

$$x^{rs} - 1 = (x^r - l)(x^{rs-r} + x^{rs-2r} + x^{rs-3r} + \cdots + x^r + 1).$$

(b) Gunakan hasil dari (a) untuk menunjukkan bahwa jika r membagi n, maka x^{p^r-1} membagi x^{p^n-1}.

Latihan 10.4.10 **24.** Hitung:
(a) [GF(16) : GF(4)], (b) [GF(64) : GF(8)], (c) [GF(p^n) : GF(p^r)].

Latihan 10.4.11 **25.** Misalkan α adalah suatu akar dari $x^3 + x + 1$ di beberapa lapangan perluasan dari $\mathbb{Z}_2$ dan misalkan β adalah suatu akar dari $x^3 + x^2 + 1$ di beberapa lapangan perluasan dari $\mathbb{Z}_2$. Tunjukkan bahwa $\mathbb{Z}_2(\alpha) \cong \mathbb{Z}_2(\beta)$.

Latihan 10.4.12 **26.** Daftar semua polinomial monik tak-tereduksi berderajat 1, 2, dan 4 atas $\mathbb{Z}_2$. Tunjukkan bahwa hasil perkaliannya adalah $x^{16} - x$.

Latihan 10.4.13 **27.** Tunjukkan bahwa $x^{p^n} - x$ adalah hasil perkalian semua polinomial monik tak-tereduksi atas $\mathbb{Z}_p$ yang derajatnya membagi n.

Latihan 10.4.14 28. Misalkan $f(x) \in \mathbb{F}[x]$ adalah suatu polinomial tak-konstan. Tunjukkan bahwa $f(x)$ dan $f'(x)$ relatif prima di $\mathbb{F}[x]$ jika dan hanya jika setiap akar-akar dari $f(x)$ di lapangan perluasan dari $\mathbb{F}$ memiliki rangkap $s = 1$.

Latihan 10.4.15 29. Tunjukkan bahwa jika khar($\mathbb{F}$) = 0, dan $f(x)$ tak-tereduksi atas $\mathbb{F}$ maka semua akar-akar dari $f(x)$ di sebarang perluasan dari $\mathbb{F}$ memiliki rangkap $s = 1$.

Latihan 10.4.16 30. Tunjukkan bahwa jika $\mathbb{F}$ adalah suatu lapangan tertutup secara aljabar, maka $\mathbb{F}$ tak-berhingga.

Daftar Pustaka

[1] Aigli Papantonopoulou. "Algebra Pure & Applied", Prentice Hall, USA, 2002.

[2] J.B. Fraleigh. "A First Course In Abstract Algebra, Seventh Edition", 2003.

[3] D.A.R. Wallace. "Groups, Rings and Fields", Springer-Verlag London Limited, 1998.

[4] Joseph A. Gallian. "Contemporary Abstract Algebra, Tenth Edition", Taylor & Francis Group, LLC, USA, 2021.

[5] Joseph J. Rotman. "Advanced Modern Algebra", Prentice Hall, 2003.

[6] Jeffrey Bergen. "A Concrete Approach to Abstract Algebra", ELSEVIER, 2010.

[7] Thomas W. Judson. "Abstract Algebra Theory and Applications", http://abstract.pugetsound.edu, 2014.

[8] Robert A. Beezer. "Sage for Abstract Algebra, A Supplement to Abstract Algebra, Theory and Applications", Department of Mathematics and Computer Science, University of Puget Sound, 2014.

[9] Joseph J. Rotman. "A First Course In Abstract Algebra, Third Edition", Prentice Hall, USA, 2010.

[10] Stephan Folders. "Fundamental Structures of Algebra and Discrete Mathematics", John Wiley & Sons, Inc., 1994.

[11] Randall B. Maddox. "A Transition to ABSTRACT MATHEMATICS Learning Mathematical Thinking and Writing, Second Edition", Academic Press, 2009.

[12] Otto F.G. Schilling and W. Stephen Piper. "Basic Abstract Algebra", Ally and Bacon. Inc., 1975.

[13] J. Eldon Whitesitt. "Principles of Modern Algebra, Second Edition", Addison-Wesley Publishing Company, 1973.

[14] John R. Durbin. "Modern Algebra An Introduction, Sixth Edition", John Wiley & Sons, Inc., 2009.

[15] Wildah Mahmudah. "Kajian Indeks Sikel Polinomial Grup dan Aplikasi Teorema Polya pada Molekul Tetrahedron", Tugas Akhir, Jurusan Matematika FMIPA-ITS, 2006.

[16] Luluk Handayani. "Kajian Teorema Burnside dan Teorema Polya serta Aplikasinya pada Enumerasi Pola Molekul Karbon (*C*)", Tugas Akhir, Jurusan Matematika FMIPA-ITS, 2004.

[17] Dr U.M. Swamy and Dr A.V.S.N. Murty. "Algebra-Abstract and Modern", Dorling Kindersley (India) Pvt. Ltd., 2012.

[18] Nadiya Gubareni. "Introduction to Modern Algebra and its Applications", CRC Press Taylor & Francis Group, 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742, 2021.

Indeks

Bio Data Penulis

Penulis bernama ***Subiono***, lahir di Surabaya, 11 April 1957, merupakan anak kedua dari tiga bersaudara. Penulis menempuh pendidikan formal di SD ***Swasta Jangkar***, Surabaya, SMP ***Kepanjen Satu***, Surabaya dan **SMAN VIII**, Surabaya. Setelah lulus dari SMA penulis melanjutkan studi di **Jurusan Matematika** ITS diterima sebagai mahasiswa angkatan 1977 lulus tahun 1983 dengan Tugas Akhir bidang **"Aljabar Linier"**. Kemudian penulis melanjutkan S2 **Jurusan Matematika** di ITB pada tahun 1987 dengan Tesis pada bidang **"Aljabar"** dan lulus pada tahun 1989. Selanjutnya penulis menempuh pendidikan S3 di **TU Delft**, Belanda pada tahun 1995 dengan Disertasi pada bidang **"Aljabar Min-Max Plus"** dan lulus pada tahun 2000. **PENGALAMAN KERJA**: Dosen Senior Jurusan Matematika, Fakultas Sains dan Analisis Data, Institut Teknologi Sepuluh Nopember, sejak 1984-sekarang. Kepala Laboratorium Model dan Sistem, Jurusan Matematika, Institut Teknologi Sepuluh Nopember (ITS) tahun 2004-2007. Ketua Program Magister Matematika, Institut Teknologi Sepuluh Nopember (ITS) tahun 2012-2016. Kepala Laboratorium Analisis, Aljabar dan Pembelajaran Matematika pada periode 2021-2025. Beberapa **Publikasi** (**Jurnal dan Konferensi Terbaru**) adalah:

- Bijan Davvaz, Dian Winda Setyawati, Soleha, Imam Mukhlash, **Subiono**, "Near Approximations in Modules", ***Foundations of Computing and Decision Sciences, The Journal of Poznan University of Technology***. Volume 46 (2021), Issue 4 (December 2021). https://sciendo.com/issue/FCDS/46/4

- **Subiono**, Joko Cahyono, Dieky Adzkiya and Bijan Davvaz, "A cryptographic algorithm using wavelet transforms over max-plus algebra", (2020), ***Journal of King Saud University Computer and Information Sciences***, https://doi.org/10.1016/j.jksuci.2020.02.004

- B. Davvaz , **Subiono**, and M. Al Tahan, "Calculus of meet plus hyperalgebra (tropical semihyperrings)", (2020), ***Communications in Algebra***, https://doi.org/10.1080/00927872.2019.1710178

- Dian Ayu Merdekawati and **Subiono**, "Closed Shop Scheduling Optimisation using Max-Plus Automata", ***Journal of Physics: Conference Series*** 1341 (2019) 042015 ***IOP Publishing*** https://iopscience.iop.org/article/10.1088/1742-6596/1341/4/042015

- **Subiono**, Kistosil Fahim and Dieky Adzkiya, "GENERALIZED PUBLIC TRANSPORTATION SCHEDULING USING MAX-PLUS ALGEBRA", ***KYBERNETIKA*** (2018), vol. 54, number 2 : 243-267. https://www.kybernetika.cz/content/2018/2/243

- Kistosil Fahim, **Subiono** and Jacob van der Woude, "On a generalization of power algorithms over max-plus algebra", ***DEDS, Discrete Event Dyn Syst*** (2017) 27:181-203, https://link.springer.com/article/10.1007%2Fs10626-016-0235-4,Springer Science+Business Media New York 2017.

Sebagai Pembicara yang diundang (*Invited Speaker*):

- "Petri nets dan Penggunaannya pada Aljabar Max-Plus", sebagai pembicara pada **Seminar Nasional Matematika 2017** di UNS Surakarta, 14 Oktober 2017.

- "On Computing Max Plus Algebra and Its Application" as keynote speaker at **1st INTERNATIONAL CONFERENCE ON APPLIED & INDUSTRIAL MATHEMATICS AND STATISTICS** (**ICoAIMS 2017**) with the theme "Bridging Mathematics and Industry", Universiti Malaysia Pahang, August 8-10,2017.

- "KOMPUTASI SIMBOLIK dan NUMERIK menggunakan SAGEMATH", sebagai pemateri pada Pelatihan Software Matematika Untuk Pengajaran & Penelitian, di Jurusan Matematika FMIPA-Unsyiah Banda Aceh, 13 Agustus 2020.

- "Aljabar Maxplus dan Aplikasinya pada masalah riil", memberikan **Kuliah Umum** di prodi S2 Matematika, Undip, Semarang, 6 Nopember 2020.

- "Masalah Komputasi pada Aljabar Maxplus", sebagai narasumber pada kegiatan **Webinar: Eksistensi Matematika pada Dunia Nyata**, Program Studi S1 Matematika FMIPA Universitas Bengkulu, 21 Nopember 2020.

- "On Computing Max Plus Algebra and Its Application" as as keynote speaker at **International Virtual Conference on Mathematical and Computational Models-ICMCM'21**, Bannari Amman Institute of Technology & Kongunadu Arts and Science College, India, October 29-30, 2021.

Website Penulis adalah :
https://www.its.ac.id/matematika/en/lecturer-and-staff/list-of-lecturers/subiono/,
sedangkan alamat email adalah : subiono2008@matematika.its.ac.id

Aljabar : Suatu Pondasi Matematika

Buku teks tingkat sarjana ini untuk kuliah dua semester dalam bidang aljabar, merupakan bagian matematika yang luas yaitu aljabar abstrak (kadang-kadang disebut aljabar modern) memperkenalkan prinsip struktur aljabar modern. Pembahasan dimulai mendefinisikan konsep himpunan, relasi, fungsi, grup, subgrup, grup yang bertindak pada suatu himpunan, teorema Sylow dan aplikasinya, ring, teori lapangan, dan teori Galois yang terkait dengan lapangan berhingga. Beberapa pembahasan dari contoh-contoh disertakan komputasinya menggunakan **SageMath** versi 9.3.

Buku ini disusun dengan maksud untuk membantu mempermudah mahasiswa dalam mempelajari materi kuliah Aljabar. Isi bahasan dimulai dengan pendahuluan membahas dasar-dasar teori yang digunakan pada hampir seluruhan bahasan berikutnya. Selanjutnya bahasan dibagi menjadi dua : yaitu bagian pertama mengenai teori grup yang merupakan bahan materi kuliah Aljabar I dan Kapita Selekta I bidang Aljabar. Bagian kedua adalah Ring dan Lapangan yang merupakan materi kuliah Aljabar II dan Kapita Selekta II bidang Aljabar. Oleh karenanya tidak berlebihan bahwa, selain dari apa yang telah disebutkan, penyusunan buku ini juga dimaksudkan untuk menambah suatu bahan bacaan khususnya bagi para peminat Aljabar.

Dalam buku ini diberikan beberapa konsep pengertian dan sifat dari materi yang disajikan didahului contoh-contoh untuk mempermudah pemahaman pengertian dan sifat yang dibahas. Selain itu juga diberikan beberapa contoh aplikasi yang mungkin, kemudian diakhiri dengan materi latihan dari setiap pembahasan topik.

Topik bahasan disajikan dengan penekanan pada “matematika” tetapi tidaklah menjadikan para pemakai lain akan mengalami kesulitan dalam mempelajari buku ini, karena peletakan penekanan aspek matematika dibuat dengan porsi yang seimbang. Sehingga para peminat matematika tetap dapat menikmati dan menggunakan ilmunya terutama dalam Aljabar, begitu juga untuk para pemakai yang lainnya diharapkan mendapat tambahan wawasan untuk melihat matematika sebagai alat yang dibutuhkan terutama dalam kajian Aljabar untuk menyelesaikan masalah-masalah praktis yang dihadapinya.

itspress

ISBN 978-623-318-091-7

9 786233 180917