DASAR-DASAR ALJABAR MODERN: TEORI GRUP & TEORI RING

Dr. Adi Setiawan, M.Sc

Penerbit Tisara Grafika
SALATIGA
2014

Katalog Dalam Terbitan

512.24
ADI Adi Setiawan
d Dasar-dasar aljabar modern: teori grup & teori ring / Adi Setiawan. -- Salatiga : Tisara Grafika, 2014.
v, 182 hlm. ; 25 cm.

ISBN 978-602-9493-15-3

1. Group algebras. 2. Rings (Algebra) I. Title.

Cetakan pertama	:	Juni 2014
ISBN	:	978-602-9493-15-3
Hak Cipta	:	Pada Penulis
Desain Sampul	:	Tisara Grafika
Tata letak	:	Harrie Siswanto
Percetakan	:	Tisara Grafika
Penerbit	:	Tisara Grafika

Diterbitkan oleh:

Tisara GRAFIKA

JL. DIPONEGORO 98 D - SALATIGA 50714 - JAWA TENGAH
Telp.: 0298-321798 | Fax : 0298-321798
Mobile: 081 228 598 985 | 0819 0488 340| 0298-6138702
email: harisis_05@yahoo.com, harriesiswanto@gmail.com
Bank: BNI Cabang Salatiga No. Rek. 369 57809

KATA PENGANTAR

Aljabar abstrak atau struktur aljabar merupakan suatu mata kuliah yang memerlukan kemampuan berfikir logis yang berbeda dengan kemampuan berfikir yang diperlukan untuk mempelajari mata kuliah-mata kuliah lain seperti kalkulus misalnya. Liku-liku berfikir logis yang ditemui dalam mata kuliah ini memerlukan latihan yang cukup agar terbentuk cara berfikir yang diperlukan dalam pemecahan masalah yang ada dalam mata kuliah ini. Untuk membantu tercapainya tujuan itu, penulis dengan sengaja membuat tata letak penulisan bukti-bukti seperti yang digunakan dalam buku ini sehingga nantinya akan memudahkan pemahaman. Buku ini diharapkan bisa memberikan dasar-dasar aljabar modern yang nanti akan banyak digunakan dalam aljabar komputasi.

Materi kuliah Aljabar Abstrak dalam buku ini dibingkai dalam judul "Dasar-dasar Aljabar Modern: Teori Grup & Teori Ring" yang berisi tentang tentang teori grup dan teori ring. Sebagian besar bahan yang dipergunakan untuk menulis diktat kuliah ini mengambil dari pustaka [2] dan beberapa bagian lain mengambil dari pustaka [4], sedangkan pustaka yang lain dipergunakan untuk melengkapi latihan-latihan.

Penulis berharap bahwa buku ini nantinya dapat berguna untuk meningkatkan mutu dalam proses pembelajaran mata kuliah Aljabar Abstrak atau Struktur Aljabar di perguruan tinggi.

Salatiga, Juni 2014

Penulis

DAFTAR ISI

BAB I
PENDAHULUAN

Dasar-dasar Aljabar Modern yang akan dibahas dalam buku ini adalah tentang teori grup dan teori ring. Dasar-dasar teori tentang teori himpunan, operasi biner, bukti dengan induksi, algoritma pembagian, relasi ekuivalensi dan penyekatan berikut ini sangat penting dalam pembahasan tentang teori grup dan teori ring.

1. Himpunan

Himpunan adalah suatu kumpulan objek (kongkrit maupun abstrak) yang didefinisikan dengan jelas. Objek-objek dalam himpunan tersebut dinamakan *elemen* himpunan.

Contoh I.1

Ditulis $A = \{0, 1, 2, 3\}$ untuk menunjukkan bahwa himpunan A mengandung elemen 0, 1, 2, 3 dan tidak ada elemen lain. Simbol

$$\{0, 1, 2, 3\}$$

dibaca sebagai "himpunan dengan elemen 0, 1, 2, dan 3".

Contoh I.2

Himpunan B terdiri dari semua bilangan bulat non negatif dan ditulis

$$B = \{ 0, 1, 2, 3, \ldots \}.$$

Tanda tiga titik dinamakan pemendekan (*ellipsis*) yang berarti bahwa pola dikenalkan sebelumnya akan terus berlanjut. Simbol

$$\{ 0, 1, 2, 3, \ldots \}$$

dibaca sebagai himpunan elemen 0, 1, 2, 3 dan seterusnya.

Contoh I.3

Himpunan B dalam Contoh I.2 dapat digambarkan dengan menggunakan simbol pembangun himpunan sebagai berikut

$B = \{ x \mid x$ adalah bilangan bulat tidak negatif $\}$.

Garis tegak merupakan pemendekan untuk sedemikian hingga dan kita menulis sebagai "himpunan semua x sehingga x adalah bilangan bulat tidak negatif."

Untuk menyatakan simbol elemen atau elemen himpunan dapat digunakan $x \in A$ dan dibaca x elemen A sedangkan untuk menyatakan simbol x bukan elemen A digunakan $x \notin A$. Pada Contoh I.1 diperoleh $2 \in A$ dan $7 \notin A$.

Definisi I.1

Misalkan himpunan A dan himpunan B. Himpunan A dinamakan himpunan bagian (*subset*) dari B jika untuk setiap elemen dari A merupakan elemen dari B. Salah satu simbol $A \subseteq B$ atau $B \supseteq A$ menunjukkan bahwa A merupakan himpunan bagian dari B.

Definisi I.2

Dua himpunan dikatakan **sama** jika dan hanya jika keduanya mempunyai elemen yang tepat sama.

Himpunan A dan B sama dan kita menulis sebagai $A = B$ jika setiap elemen A juga menjadi elemen B dan jika setiap elemen B juga menjadi elemen A. Biasanya, bukti bahwa dua himpunan sama dinyatakan dalam 2 bagian. Pertama, menunjukkan bahwa $A \subseteq B$ dan yang kedua bahwa $B \subseteq A$ sehingga dapat disimpulkan bahwa $A = B$.

Definisi I.3

Jika A dan B himpunan maka A himpunan bagian sejati dari B jika dan hanya jika $A \subseteq B$ dan $A \neq B$.

Sering kali ditulis $A \subset B$ untuk menyatakan bahwa A himpunan bagian sejati dari B.

Contoh I.4

Pernyataan berikut ini untuk menggambarkan simbol himpunan bagian sejati dan kesamaan himpunan :

$$\{ 1, 2, 4 \} \subset \{ 1, 2, 3, 4, 5 \}, \quad \{ a, c \} = \{ c, a \}.$$

Pada himpunan, terdapat dua operasi dasar yaitu gabungan (*union*) dan irisan (*intersection*) yang digunakan untuk meng-kombinasikan.

Definisi I.4

Jika A dan B himpunan, gabungan A dan B adalah himpunan $A \cup B$ (yang dibaca A gabung B) yaitu

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

Irisan dari A dan B adalah himpunan $A \cap B$ (yang dibaca A irisan B) yaitu

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

Gubungan dua himpunan A dan B adalah himpunan yang elemennya berada di himpunan A atau di himpunan B atau di kedua himpunan tersebut. Irisan himpunan A dan B adalah himpunan yang elemennya berada di kedua himpunan tersebut.

Contoh I.5

Misalkan $A = \{ 2, 4, 6\}$ dan $B = \{ 4, 5, 6, 7\}$,

$$A \cup B = \{ 2, 4, 5, 6, 7\}$$

dan $A \cap B = \{ 4, 6 \}$.

Contoh I.6

Mudah dibuktikan bahwa $A \cup B = B \cup A$ yaitu

$$\begin{aligned} A \cup B &= \{ x \mid x \in A \text{ atau } x \in B \} \\ &= \{ x \mid x \in B \text{ atau } x \in A \} \\ &= B \cup A. \end{aligned}$$

Karena $A \cup B = B \cup A$ maka kita katakan bahwa operasi gabungan mempunyai sifat komutatif. Jelas dan mudah dibuktikan juga bahwa $A \cap B = B \cap A$ dan kita juga mengatakan bahwa operasi irisan mempunyai sifat komutatif.

Mudah untuk menemukan himpunan yang tidak mempunyai elemen bersama. Sebagai contoh, himpunan $A = \{ 1, -1 \}$ dan

$$B = \{ 0, 2, 3\}$$

yang tidak mempunyai elemen bersama. Hal itu berarti bahwa tidak ada elemen bersama dalam irisan mereka yaitu dalam $A \cap B$ dan dikatakan bahwa irisannya merupakan himpunan kosong (*empty set*).

Himpunan kosong adalah himpunan yang tidak mempunyai elemen dan himpunan kosong disimbolkan dengan $\varnothing$ atau { }. Dua himpunan A dan B dinamakan saling asing (*disjoint*) jika dan hanya jika $A \cap B = \varnothing$.

Himpunan { 1, -1} dan { 0, 2, 3} saling asing karena

$$\{ 1, -1\} \cap \{ 0, 2, 3\} = \varnothing.$$

Hanya terdapat 1 himpunan kosong $\varnothing$ dan $\varnothing$ merupakan himpunan bagian dari setiap himpunan. Untuk himpunan A dengan n elemen (n adalah bilangan bulat tidak negatif) dan dapat ditulis semua himpunan bagian dari A. Sebagai contoh, jika

$$A = \{ a, b, c \}$$

maka himpunan bagian dari A adalah

$$\varnothing, \{ a \}, \{ b \}, \{ c \}, \{a, b \}, \{ a, c\}, \{b, c \}, A.$$

Definisi I.5

Untuk sebarang himpunan A, kuasa (*power*) dari himpunan A dinotasikan dengan P(A) yaitu himpunan semua himpunan bagian dari A dan ditulis dengan

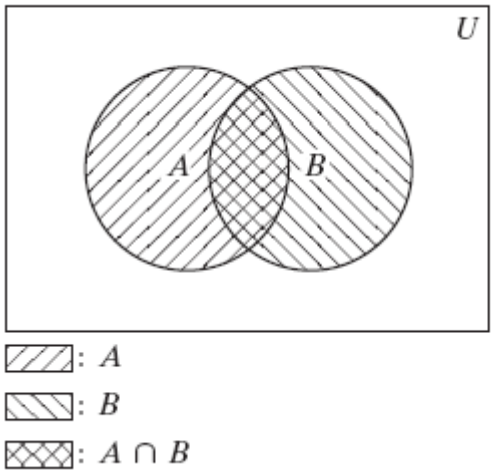
$$\mathrm{P}(A) = \{ X \mid X \subseteq A \}.$$

Contoh I.7

Untuk $A = \{ a, b, c \}$, kuasa himpunan A adalah

$$\mathrm{P}(A) = \{ \varnothing, \{ a \}, \{ b \}, \{ c \}, \{a, b \}, \{ a, c\}, \{b, c \}, A \}.$$

Sangatlah bermanfaat untuk mengambarkan himpunan yang menjadi perhatian dalam suatu gambar atau diagram. Apabila kita mengerjakan hal ini maka kita mengasumsikan bahwa himpunan yang menjadi perhatian merupakan himpunan bagian dari suatu himpunan semesta (*universal set*) yang disimbolkan dengan U yang dinyatakan dengan persegi panjang sehingga lingkaran termuat dalam persegi panjang. Irisan A dan B yaitu dinyatakan dengan daerah yang saling beririsan yaitu ketika dua buah lingkaran berhimpitan. Diagram yang digunakan untuk menyatakan hal ini dinamakan **diagram Venn**.



Gambar I.1

Definisi I.6

Sebarang himpunan bagian dari himpunan semesta U, komplemen B dalam A yaitu

$$A - B = \{ x \in U \mid x \notin A \}.$$

Simbol khusus $A^c = U - A = \{ s \in U \mid x \notin A \}$.

Simbol A^c dibaca komplemen A sebagai pemendekan dari komplemen A dalam U.

Contoh I.8

Misalkan U = { x | x adalah bilangan bulat }, A = { x | x bilangan bulat genap } dan B = { x | x bilangan bulat positif } maka

$B - A$ = { x | x adalah bilangan bulat positif ganjil } = { 1, 3, 5, 7, …. },

$A - B$ = { x | x adalah bilangan bulat tidak positif genap } = { 0, -2, -4, -6, ….},

A^c = { x | x adalah bilangan bulat ganjil },

B^c = { x | x adalah bilangan bulat tidak positif } = { 0, -1, -2, -3, …. }.

Banyak contoh dan latihan dalam buku ini melibatkan sistim bilangan yang banyak dikenal dan kita mengadopsi *standard* berikut ini untuk beberapa sistim ini:

Z menyatakan himpunan bilangan bulat,

$\boldsymbol{Z}^+$ menyatakan himpunan bilangan bulat positif,

Q menyatakan himpunan semua bilangan rasional,

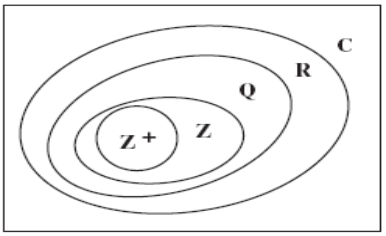
R menyatakan himpunan semua bilangan real,

C menyatakan himpunan semua bilangan kompleks.

Perlu diingat kembali bahwa bilangan kompleks didefinisikan sebagai bilangan berbentuk $a + b\,i$ dengan a dan b adalah bilangan real dan $i=\sqrt{-1}$. Demikian juga suatu bilangan rasional adalah jika dan hanya jika dapat dinyatakan sebagai perbandingan bilangan bulat dengan penyebut tidak nol yaitu

$$Q = \left\{ \frac{a}{b} \middle| \, a,b \in Z, \;\; b \neq 0 \right\}.$$

Hubungan antara sistim bilangan dalam paragraf terdahulu satu sama lain dapat dinyatakan dalam diagram Venn berikut ini.



$\mathbf{Z}^+ \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$

Gambar I.2

Contoh I.9

Himpunan $(A \cap B) \cap C$ dan $A \cap (B \cap C)$ adalah sama karena

$$\begin{aligned}(A \cap B) \cap C &= \{x \mid x \in A \text{ dan } x \in B\} \cap C \\ &= \{x \mid x \in A \text{ dan } x \in B \text{ dan } x \in C\} \\ &= A \cap \{x \mid x \in B \text{ dan } x \in C\} \\ &= A \cap (B \cap C).\end{aligned}$$

Analog dengan sifat asosiatif dari bilangan, operasi irisan juga mempunyai sifat asosiatif. Seringkali, jika kita bekerja dengan bilangan, kita menghilangkan penggunaan tanda kurung dan menulis

$$x + y + z = x + (y + z) = (x + y) + z.$$

Untuk himpunan A, B dan C, ditulis

$$A \cap B \cap C = (A \cap B) \cap C = A \cap (B \cap C).$$

Dengan cara yang sama sifat asosiatif juga berlaku untuk gabungan

$$A \cup B \cup C = (A \cup B) \cup C = A \cup (B \cup C).$$

Sifat distributif juga berlaku dalam operasi himpunan yaitu :

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Dapat juga dibuktikan berlaku hukum De Morgan yaitu

$$(A \cap B)^c = A^c \cup B^c \text{ dan } (A \cup B)^c = A^c \cap B^c.$$

2. Operasi biner

Dalam aljabar tidak hanya dibahas tentang himpunan tetapi juga himpunan bersama dengan operasi penjumlahan dan perkalian yang didefinisikan pada himpunan.

Definisi I.6

Misalkan A himpunan tidak kosong.
Operasi biner * pada A adalah pemetaan dari setiap pasangan berurutan x, y dalam A dengan tepat satu elemen $x * y$ dalam A.

Himpunan bilangan bulat Z mempunyai dua operasi biner yang dikenakan padanya yaitu penjumlahan (+) dan perkalian (.). Dalam hal ini untuk setiap pasangan x dan y dalam Z, $x+y$ dan $x.y$ *dikawankan secara tunggal* dengan suatu elemen dalam Z.
Operasi biner mempunyai dua bagian dari definisi yaitu:

1. terdefinisikan dengan baik (*well-defined*) yaitu untuk setiap pasangan berurutan x, y dalam A dikawankan dengan tepat satu nilai $x*y$.
2. A *tertutup* di bawah operasi * yaitu untuk setiap x, y dalam A maka $x*y$ masih dalam A.

Contoh I.10:

Diketahui N himpunan semua bilangan bulat positif.
Didefinisikan * dengan aturan $x*y = x-y$.
Karena 3, 5 dalam N dan 3*5 = 3-5 = -2 tidak berada dalam N maka N tidak tertutup di bawah operasi * sehingga * bukan operasi biner pada N.

Contoh I.11:

Didefinisikan operasi # dengan aturan $x \# y = x + 2y$ dengan x, y dalam

$$\boldsymbol{N} = \{ 1, 2, 3, \ldots \}.$$

Akan ditunjukkan bahwa # merupakan operasi biner.
Jelas bahwa # terdefinisikan dengan baik karena rumus $x + 2y$ memberikan hasil tunggal untuk setiap x, y dalam N.
Untuk sebarang x, y dalam N maka jelas bahwa $x + 2y$ masih merupakan bilangan bulat positif. Lebih jauh $2y + x > 0$ jika $x > 0$ dan $y > 0$.
Berarti hasil dari $x + 2y$ masih merupakan bilangan positif dan akibatnya N tertutup di bawah operasi #.

3. Hukum-hukum Aljabar

Suatu *sistim aljabar* terdiri dari himpunan objek dengan satu atau lebih operasi yang didefinisikan padanya. Bersama dengan hukum-hukum yang dibutuhkan dalam operasi.

Definisi I.7

Misalkan * operasi biner pada himpunan A.
(1) operasi * assosiatif jika $(a*b)*c = a*(b*c)$ untuk semua a, b, c dalam A.
(2) operasi * komutatif jika $a*b = b*a$ untuk semua a, b dalam A.

Dalam pembahasan selanjutnya hukum-hukum dasar aljabar untuk penjumlahan dan perkalian yang didefinisikan pada bilangan bulat Z dan bilangan real R sebagai aksioma (*axioms*) yaitu diterima tanpa bukti.

Contoh I.12:

Operasi * didefinisikan pada himpunan bilangan real $\boldsymbol{R}$ dengan

$$a*b = (1/2)ab.$$

Akan ditunjukkan bahwa * assosiatif dan komutatif.
Karena $(a*b)*c = (1/2\ ab)*c$

$= (1/2)((1/2\ ab)c)$
$= (1/4)\ (ab)c$

dan pada sisi lain

$a*(b*c) = a*((1/2)\ bc)$
$= (1/2)\ a((1/2)\ bc)$
$= (1/4)(ab)\ c$

untuk semua a, b dan c dalam $\boldsymbol{R}$ maka * assosiatif.

Karena $a*b = (1/2)ab$
$= (1/2)ba$
$= b*a$

untuk semua a, b dalam $\boldsymbol{R}$ maka * komutatif.

Contoh I.13:

Operasi $\oplus$ didefinisikan pada bilangan bulat $\boldsymbol{Z}$ dengan aturan

$$a \oplus b = a + 2b.$$

Akan ditunjukkan bahwa $\oplus$ tidak komutatif dan tidak assosiatif.

Karena pada satu sisi

$$(a \oplus b) \oplus c = (a+2b) \oplus c = (a+2b)+2c$$

dan pada sisi lain

$a \oplus (b \oplus c) = a \oplus (b+2c)$
$= a+2(b+2c)$
$= a+(2b+4c)$
$= (a+2b)+4c$

dari kedua hasil tersebut tidak sama untuk $c \neq 0$ maka $\oplus$ tidak assosiatif.

Karena $a \oplus b = a+2b$ dan $b \oplus a = b+2a$ dan kedua hasil ini tidak sama untuk $a \neq b$ maka $\oplus$ tidak komutatif.

Terlihat bahwa aturan untuk * tidak menjamin bahwa himpunan X tertutup di bawah operasi *. Berikut ini diberikan suatu cara untuk membuktikan bahwa suatu himpunan tertutup terhadap suatu operasi.

Untuk membuktikan sifat tertutup dari suatu system X dimulai dengan dua sebarang elemen yang dioperasikan dengan operasi * dan kemudian ditunjukkan bahwa hasilnya masih memenuhi syarat keelemenan dalam X.

Untuk selanjutnya dalam tulisan ini $\boldsymbol{R}^2$ dimaksudkan himpunan semua pasangan berurutan dari bilangan real

$$\boldsymbol{R}^2 = \{ (a,b) \mid a, b \text{ dalam } \boldsymbol{R} \}.$$

Contoh I.14:

Misalkan $\oplus$ mempunyai aturan $(a,b) \oplus (c,\text{d}) = (a+c, b+d)$.
Akan ditunjukkan bahwa $\boldsymbol{R}^2$ tertutup di bawah operasi $\oplus$.
Untuk sebarang (a,b) dan (c,d) dalam R^2 berlaku

$$(a,b) \oplus (c,d) = (a+c,b+d)$$

dengan $a+c$ dan $b+d$ dalam R sehingga $(a+c,b+d)$ dalam $\boldsymbol{R}^2$.
Oleh karena itu hasilnya merupakan pasangan berurutan dan tertutup di bawah operasi $\oplus$.

Selanjutnya operasi $< A, * >$ menyatakan himpunan A dan * merupakan operasi yang didefinisikan pada A.

Definisi I.8:

(1) $< A,* >$ memenuhi hukum identitas asalkan A mengandung suatu elemen e sehingga $e*a = a*e = a$ untuk semua a dalam A. Elemen A yang mempunyai sifat demikian dinamakan *identitas* untuk $< A,* >$.

(2) $< A, * >$ memenuhi hukum invers asalkan A mengandung suatu identitas e untuk operasi * dan untuk sebarang a dalam A terdapat suatu elemen a' dalam A yang memenuhi

$$a*a' = a'*a = e.$$

Elemen a' yang memenuhi sifat di atas dinamakan invers dari a.

Sebagai contoh, $\boldsymbol{Z}$ mengandung identitas 0 untuk operasi penjumlahan dan untuk setiap a dalam $\boldsymbol{Z}$, elemen $-a$ memenuhi

$$a+(-a) = (-a)+a = 0$$

sehingga a mempunyai invers terhadap operasi penjumlahan dan $< Z, + >$ memenuhi hukum invers. Di samping itu $\boldsymbol{Z}$ mengandung identitas 1 terhadap operasi perkalian tetapi $\boldsymbol{Z}$ tidak mengandung invers terhadap perkalian kecuali 1 dan -1.

Untuk membuktikan hukum identitas dilakukan dengan menduga elemen tertentu e dalam himpunan yang berlaku sebagai identitas dan kemudian menguji apakah e*a = a dan a*e = a untuk sebarang a dalam himpunan. Untuk membuktikan hukum invers dilakukan dengan sebarang elemen x dalam himpunan yang mempunyai identitas e dan menduga invers dari x yaitu x′ dalam himpunan dan kemudian menguji apakah x*x′ = e dan x′*x = e.

Contoh I.15:

Bila operasi didefinisikan seperti pada Contoh I.6 maka akan dibuktikan bahwa hukum invers dan hukum identitas berlaku.
Diduga bahwa (0,0) merupakan elemen identitas.
Karena untuk sebarang (a,b) dalam $\boldsymbol{R}^2$ berlaku

$$(0,0)+(a,b) = (0+a,\ 0+b) = (a,b)$$

dan (a,b) + (0,0) = $(a+0,\ b+0) = (a,b)$ maka (0,0) identitas dalam R^2**.**

Bila diberikan sebarang (a,b) dalam $\boldsymbol{R}^2$ maka akan ditunjukkan $(-a,-b)$ dalam $\boldsymbol{R}^2$ merupakan inversnya. Karena $-a$ dan $-b$ dalam R maka $(-a,-b)$ dalam $\boldsymbol{R}^2$. Lebih jauh lagi,

$$(a,b) \oplus (-a,-b) = (a-a,b-b) = (0,0)$$

dan

$$(-a,-b) \oplus (a,b) = (-a+a,-b+b) = (0,0)$$

sehingga $(-a,-b)$ merupakan invers dari (a,b) dalam $\boldsymbol{R}^2$.

Contoh I.16:

Bila * didefinisikan pada $\boldsymbol{R}$ dengan aturan $a*b = ab + a$ maka akan ditunjukkan bahwa $< \boldsymbol{R}, *>$ tidak memenuhi hukum identitas.

Karena supaya $a*e$ sama dengan a untuk semua a haruslah dimiliki $ae + a = a$ sehingga e perlulah sama dengan 0.
Tetapi meskipun $a*0 = a$ maka $0*a = 0*(a+0) = 0$ yang secara umum tidak sama dengan a.
Oleh karena itu tidak ada e dalam $\boldsymbol{R}$ yang memenuhi $a*e = a$ dan

$$e*a = a.$$

Terbukti bahwa tidak ada identitas dalam $\boldsymbol{R}$ terhadap *.

3. Bukti dengan induksi

Dalam pembuktian biasanya diinginkan untuk membuktikan suatu pernyataan tentang bilangan bulat positif n. Berikut ini diberikan dua prinsip tentang induksi berhingga.

Prinsip pertama induksi berhingga

Misalkan $S(n)$ pernyataan tentang bilangan bulat positif n.
Apabila sudah dilakukan pembuktian :
(1) $S(n_0)$ benar untuk bilangan bulat pertama n_0,
(2) Dibuat anggapan induksi (*induction assumption*) bahwa pernyataan benar untuk suatu bilangan bulat positif $k \geq n_0$ dan mengakibatkan $S(k+1)$ benar, maka $S(n)$ benar untuk semua bilangan bulat $n \geq n_0$.

Contoh I.17

Akan dibuktikan bahwa $2^n > n + 4$ untuk semua bilangan bulat $n \geq 3$ dengan menggunakan induksi.
Bukti pernyataan benar untuk $n_0 = 3$.
Untuk $n_0 = 3$ maka pernyataan $2^3 > 3 + 4$ benar.
Asumsi induksi.
Dianggap pernyataan benar berarti $2^k > k + 4$ untuk suatu bilangan bulat $k \geq 3$.

Langkah induksi.
Dengan anggapan induksi berlaku $2^k > k + 4$ dan bila kedua ruas digandakan dengan 2 diperoleh 2 $(2^k) > k+4$ atau $2^{k+1} > 2k + 8$ dan jelas bahwa $2k + 8 > 5$ karena k positif sehingga diperoleh

$$2^{k+1} > k + 5 = (k + 1) + 4.$$

Berarti bahwa dianggap pernyataan benar untuk $S(k)$ maka sudah dibuktikan bahwa pernyataan benar untuk $S(k+1)$.
Jadi dengan prinsip induksi maka $S(n)$ benar untuk semua bilangan bulat $n \geq 3$.

Prinsip induksi berikut ekuivalen dengan prinsip pertama induksi berhingga tetapi biasanya lebih cocok untuk bukti tertentu.

Prinsip kedua induksi berhingga

Misalkan S(n) suatu pernyataan tentang bilangan bulat n.
Apabila sudah dilakukan pembuktian:

(1) S(n_0) benar untuk suatu bilangan bulat pertama n_0.
(2) Dibuat anggapan $S(k)$ benar untuk semua bilangan bulat k yang memenuhi $n_0 \leq k < m$ dan mengakibatkan $S(m)$ benar.

maka S(n) benar untuk semua bilangan bulat $n > n_0$.

Prinsip kedua induksi tersebut di atas dapat digunakan untuk membuktikan teorema faktorisasi berikut ini.

Teorema I.1

Setiap bilangan bulat positif $n \geq 2$ dapat difaktorkan sebagai hasil kali berhingga banyak bilangan prima yaitu $n = p_1 p_2 \ldots\ldots p_w$..

Bukti

Untuk $n_0 = 2$ maka 2 = 2 yaitu faktorisasi dengan satu faktor prima.
Anggapan induksi adalah bahwa semua bilangan bulat positif $k < m$ dengan $k \geq 2$ dapat difaktorkan sebagai hasil kali bilangan prima sebanyak berhingga.
Jika m bilangan prima maka jelas faktorisasinya adalah $m = m$.

Jika m bukan bilangan prima maka m mempunyai faktor sejati $m = st$ dengan s dan t lebih kecil dari m tetapi lebih besar atau sama dengan 2.
Dengan anggapan induksi maka s dan t mempunyai faktor prima yaitu:

$$s = p_1 p_2 \ldots p_u$$

dan

$$t = q_1 q_2 \ldots q_v.$$

Oleh karena itu, $m = s = p_1 p_2 \ldots p_u q_1 q_2 \ldots q_v$ dan berarti m juga mempunyai faktor prima. Jadi dengan menggunakan prinsip kedua induksi maka teorema tersebut telah dibuktikan.

Algoritma berikut ini dikenal dengan nama algoritma pembagian dan sangat penting dalam aljabar.

Algoritma pembagian

Untuk sebarang dua bilangan bulat a dan b dengan $b > 0$ terdapatlah dengan tunggal q dan r sehingga $a = bq + r$ dengan $0 \le r < b$. Lebih jauh b merupakan *faktor* dari a jika dan hanya jika $r = 0$.

Bukti:

Bila diamati barisan bilangan b, $2b$, $3b$, ... maka pada suatu saat barisan itu akan melampaui a.
Misalkan $q + 1$ adalah bilangan positif terkecil sehingga $(q + 1)b > a$ sehingga

$$qb \le a < (q + 1)b$$

dan berarti $qb \le a < qb + b$ atau $0 \le a - qb < b$.
Misalkan ditulis $r = a - qb$.
Akibatnya $a = qb + r$ dengan $0 \le r < b$.
Akan ditunjukkan bahwa q dan r yang terpilih adalah tunggal.
Misalkan $a = bq_1 + r_1$ dan dianggap bahwa $r_1 \le r$.
Karena $bq_1 + r_1 = bq + r$ maka $b(q_1 - q) = r - r_1$.
Tetapi $r - r_1$ lebih kecil dari b dan $r - r_1$ tidak negatif karena $r_1 \le r$.
Oleh karena itu $q_1 - q \ge 0$.

Tetapi jika $q_1 - q \geq 1$ maka $r - r_1$ akan melampaui atau sama dengan b dan berarti timbul suatu kontradiksi sehingga didapat $q_1 - q = 0$ dan juga $r - r_1 = 0$.
Berarti $r_1 = r$ dan $q_1 = q$.
Kejadian $a = bq$ untuk suatu bilangan bulat q jika dan hanya jika $r = 0$ sehingga b dan q merupakan faktor dari a.

Relasi ekuivalensi dan penyekatan

Objek matematika dapat direlasikan dengan yang lain dalam berbagai cara seperti:

m membagi n,
x dibawa ke y dengan fungsi f

dan sebagainya. Secara intuitif relasi R dari suatu himpunan X ke himpunan Y adalah *aturan yang memasangkan elemen X dengan elemen Y.* Secara formal, relasi R dari X ke Y didefinisikan berikut ini. Pertama-tama didefinisikan hasil kali Cartesian $X \times Y$ sebagai himpunan pasangan berurutan $\{ (x,y) \mid x$ dalam X dan y dalam $Y \}$. Kemudian didefinisikan suatu relasi R sebagai himpunan bagian tertentu dari $X \times Y$. Jika pasangan berurutan (s,t) elemen himpunan bagian tertentu untuk R maka ditulis s R t.

Contoh I.18

(a) Relasi $<$ didefinisikan pada himpunan bilangan real dengan sifat $x < y$ jika dan hanya jika $x - y$ positif.
(b) Relasi membagi habis ($\mid$) didefinisikan pada himpunan bilangan bulat positif dengan sifat $m \mid n$ jika dan hanya jika $n = mq$ untuk suatu bilangan bulat q.

Definisi I.9

Suatu relasi R pada himpunan X dikatakan mempunyai sifat:
(1) *Refleksif* jika x R x untuk semua x dalam X.
(2) *Simetrik* jika x R y menyebabkan y R x.
(3) *Transitif* jika x R y dan y R z menyebabkan x R z.
(4) *Antisimetris* jika x R y dan y R x menyebabkan $x = y$.

Definisi I.10

Misalkan ~ relasi yang didefinisikan pada suatu himpunan X. Jika relasi ~ refleksif, simetrik dan transitif maka relasi ~ merupakan *relasi ekuivalensi*.

Contoh I.19

Diketahui $f : A \to B$ suatu fungsi.
Jika didefinisikan pada A dengan $x \sim y$ jika $f(x) = f(y)$ maka dapat dibuktikan bahwa relasi ~ merupakan relasi ekuivalensi.

Suatu penyekatan (*partition*) dari himpunan X merupakan suatu keluarga himpunan bagian tidak kosong dari X yang saling asing dan gabungannya sama dengan X. Penyekatan merupakan hal yang penting dalam matematika dan terdapat hubungan antara relasi ekuivalensi dan penyekatan. Jika x dalam X dan ~ relasi pada X maka dapat didefinisikan suatu kelas dari x yang dinotasikan dengan $C(x)$ adalah himpunan semua y dalam x sehingga $x \sim y$. Jika ~ merupakan relasi ekuivalensi maka $C(x)$ dinamakan *ekuivalensi* dari x.

Teorema 1.2 :

Jika ~ suatu relasi ekuivalensi pada himpunan X maka keluarga kelas ekuivalensi $C(x)$ membentuk penyekatan himpunan X.

Bukti :

Karena ~ refleksif maka $x \sim x$ untuk semua x dalam X.
Oleh karena itu, kelas $C(x)$ mengandung x.
Misalkan $C(x)$ dan $C(y)$ mempunyai paling sedikit satu elemen serikat z.
Akibatnya $x \sim z$ dan $y \sim z$ (berarti juga $z \sim y$) dan akibatnya $x \sim y$.
Hal itu berarti bahwa untuk setiap t sehingga $y \sim t$ menyebabkan $x \sim t$ dan diperoleh $C(y) \subseteq C(x)$.
Dengan cara yang sama dapat dibuktikan pula bahwa $C(y) \subseteq C(x)$.
Akibatnya $C(y) = C(x)$ sehingga kelas-kelas ekuivalensi yang bertumpang tindih akan sama dan kelas-kelas yang berbeda akan saling asing.

Latihan

1. Misalkan A himpunan bagian B.
   Buktikan bahwa $A \cap B = A$ dan $A \cup B = B$.
2. Tuliskan himpunan pangkat (*power set*) dari setiap himpunan A berikut ini.
   a. $A = \{ a \}$.
   b. $A = \{ a, b, c \}$.
   c. $A = \{ 0, 1 \}$.
3. Diketahui $A = \{ 6m \mid m \text{ dalam } Z \}$, $B = \{ 4m \mid m \text{ dalam } Z \}$ dan $C = \{ 12m \mid m \text{ dalam } Z \}$. Buktikan bahwa $A \cap B = C$.
4. Buktikan bahwa jika $A \subseteq B$ dan $B \subseteq C$ maka $A \subseteq C$.
5. Buktikan bahwa $A \subseteq B$ jika dan hanya jika $B^c \subseteq A^c$.
6. Buktikan bahwa jika $A \subseteq B$ jika dan hanya jika $A \cup C \subseteq B \cup C$.
7. Buktikan bahwa $B - A = B \cap A^c$.
8. Buktikan bahwa $A \cup B - A = A \cup B$.
9. Buktikan bahwa $(A - B) \cup (A \cap B) = A$.
10. Buktikan bahwa $A \cup B - C = (A - C) \cup (B - C)$.
11. Diberikan operasi * dengan aturan $a*b = -ab$ dengan a dan b bilangan bulat.
    a. Jelaskan mengapa * operasi biner pada Z.
    b. Buktikan * assosiatif.
    c. Buktikan bahwa * komutatif.
    d. Buktikan bahwa Z mengandung suatu identitas terhadap operasi *.
    e. Jika a dalam Z maka tentukan z' dalam Z terhadap operasi *.
12. Misalkan bahwa * adalah operasi biner pada himpunan tidak kosong A. Buktikan bahwa
    $$a * [b * (c * d)] = [a * (b * c)] * d$$

untuk semua a, b, c dan d dalam A.

13. Misalkan * adalah operasi biner pada himpunan tidak kosong A. Jika * mempunyai sifat komutatif dan asosiatif maka buktikan bahwa

$$[\,(a * b) * c\,] * d = (d * c) * (a * b)$$

untuk semua a, b, c dan d dalam A.

14. Buktikan bahwa $1 + 5 + 9 + \ldots + (4n + 1) = (2n + 1)(n + 1)$ untuk semua $n \geq 0$.

15. Relasi didefinisikan pada himpunan orang-orang dan dikatakan bahwa $a \sim b$ jika dan hanya jika a dan b mempunyai hari ulang tahun yang sama (tidak perlu tahun kelahirannya sama)
    a. Tunjukkan bahwa ~ merupakan relasi ekuivalensi.
    b. Berapa banyak kelas-kelas ekuivalensi yang ada ? Jelaskan !

***

BAB II
GRUP

Suatu cabang matematika yang mempelajari struktur aljabar dinamakan aljabar modern atau abstrak (*abstract algebra*). Sistim aljabar (*algebraic system*) terdiri dari suatu himpunan objek, satu atau lebih operasi pada himpunan bersama dengan hukum tertentu yang dipenuhi oleh operasi. Salah satu alasan yang paling penting untuk mempelajari sistim tersebut adalah untuk menyatukan sifat-sifat pada topik-topik yang berbeda dalam matematika.

Definisi II.1

Suatu grup (*group*) $< G , * >$ terdiri dari himpunan elemen G bersama dengan operasi biner * yang didefinisikan pada G dan memenuhi hukum berikut :

(1) Hukum tertutup : $a * b \in G$ untuk semua $a, b \in G$,

(2) Hukum assosiatif : $(a * b) * c = a * (b * c)$ untuk semua $a, b, c \in G$,

(3) Hukum identitas : terdapatlah suatu elemen $e \in G$ sehingga

$$e * x = x * e = x$$

untuk semua $x \in G$,

(4) Hukum invers : untuk setiap $a \in G$, terdapatlah $a' \in G$ sehingga $a * a' = a' * a = e$.

Biasanya lambang $< G , * >$ hanya dituliskan G, demikian juga ab artinya $a * b$ dan a^{-1} adalah lambang untuk invers a.

Contoh II.1

1. Himpunan bilangan bulat $\boldsymbol{Z}$ merupakan grup terhadap operasi +.
2. Himpunan bilangan asli $\boldsymbol{N}$ bukan grup terhadap operasi +.
3. Himpunan bilangan kompleks $\boldsymbol{C}$ merupakan grup terhadap operasi +.
4. Himpunan bilangan real $\boldsymbol{R} - \{0\}$ merupakan grup terhadap operasi perkalian.

5. Himpunan bilangan bulat modulo n merupakan grup terhadap operasi penjumlahan modulo n.
6. Himpunan bilangan rasional merupakan grup terhadap operasi +.
   Sistim ini dilambangkan dengan $< \boldsymbol{Q} , + >$ dengan
   $$Q = \{ a/b \mid a, b \in \boldsymbol{Z} \text{ dan } b \neq 0\}.$$
   Operasi penjumlahan didefinisikan dengan aturan
   $$a/b + c/d = (ad + bc)/(bd)$$
   akan dibuktikan bahwa $\boldsymbol{Q}$ grup berdasarkan sifat-sifat bilangan bulat.

   Hukum tertutup

   Misalkan $a/b, c/d \in Q$. Berdasarkan definisi operasi penjumlahan pada bilangan rasional didapat $(ad + bc)/(bd)$.
   Karena operasi perkalian dan penjumlahan dalam bilangan bulat bersifat tertutup maka pembilang dan penyebutnya merupakan bilangan bulat. Karena b dan d tidak nol maka bd juga tidak nol.
   Berarti penjumlahan bilangan rasional bersifat tertutup.

   Hukum assosiatif.

   Misalkan $a/b, c/d$ dan $e/f \in \boldsymbol{Q}$.
   Akan ditunjukkan bahwa sifat assosiatif berlaku.
   $$\begin{aligned}(a/b + c/d) + e/f &= (ad + bc)/(bd) + e/f \\ &= [(ad + bc)f + (bd)e] \,/\, (bd)f \\ &= [(ad)f + (bc)f + (bd)e] \,/\, (bd)f \\ &= [a(df) + b(cf) + b(de)] \,/\, b(df) \\ &= a/b + (cf+de) \,/\, (df) \\ &= a/b + (c/d + e/f).\end{aligned}$$

Berarti sifat assosiatif berlaku.

Hukum identitas

Elemen $0/1$ merupakan identitas karena
$$\begin{aligned}0/1 + a/b &= (0.b + 1.a) \,/\, (1.b) \\ &= (0 + a) \,/\, b \\ &= a/b.\end{aligned}$$

Pada sisi lain, $a/b + 0/1 = (a.1 + b.0) / (b.1)$

$= (a + 0) / b$

$= a/b$.

Hukum invers

Untuk sebarang elemen $a/b \in \boldsymbol{Q}$ akan ditunjukkan bahwa $(-a)/b$ merupakan inversnya.

Jelas bahwa $(-a)/b \in \boldsymbol{Q}$. Elemen $(-a)/b$ merupakan invers a/b karena

$a/b + (-a)/b = ab + b(-a)/(bb)$

$= (ab + (-a)b / (bb)$

$= 0.b / (bb)$

$= 0 / b$

$= 0 / 1$.

Terbukti $\boldsymbol{Q}$ grup.

Sifat-sifat sederhana dalam grup

Dalam pembahasan terdahulu telah dicacat bahwa sebagai akibat definisi grup, sebarang persamaan $a * x = b$ mempunyai penyelesaian dalam suatu grup yaitu $x = a' * b$. Sifat-sifat sederhana yang lain dinyatakan dalam teorema berikut ini.

Teorema II.1

Dalam sebarang grup berlaku sifat sifat berikut :

1. Hukum *kanselasi kiri* : Jika $a\,x = a\,y$ maka $x = y$.
2. Hukum *kanselasi kanan* : Jika $x\,a = y\,a$ maka $x = y$.
3. Elemen identitas itu *tunggal* yaitu jika e dan e' elemen G yang memenuhi hukum identitas maka $e = e'$.
4. Invers dari sebarang elemen G akan tunggal yaitu jika a dan b merupakan invers dari x maka $a = b$.
5. $(ab)^{-1} = b^{-1}\,a^{-1}$.

Bukti:

1. Diberikan $ax = ay$.

   Karena G grup dan $a \in G$ maka terdapat a^{-1} sehingga

   $a\,a^{-1} = a^{-1}\,a = e$

dengan e identitas. Akibatnya

$$a^{-1}(ax) = a^{-1}(ay)$$

dan dengan menggunakan hukum assosiatif diperoleh

$$(a^{-1}a)x = (a^{-1}a)y$$

dan dengan hukum invers diperoleh

$$ex = ey$$

akhirnya dengan hukum identitas $x = y$.

2. Analog dengan 1 (untuk latihan).
3. Karena e suatu elemen identitas maka $e\,e' = e'$.
   Pada sisi lain, karena e' elemen identitas maka $e\,e' = e$, sehingga
   $$e\,e' = e' = e.$$
4. Karena a dan b merupakan invers x maka berlaku $xa = e$ dan $xb = e$.
   Karena elemen identitas itu tunggal maka $xa = e = xb$.
   Akibatnya dengan menggunakan hukum kanselasi kiri maka $a = b$.
5. Karena
   $$ab \,.\, b^{-1}a^{-1} = a\,(b\,b^{-1})\,a^{-1} = a\,e\,a^{-1} = a\,a^{-1} = e$$
   dan
   $$b^{-1}a^{-1} \,.\, ab = b^{-1}(a^{-1}a)b = b^{-1}\,e\,b = b^{-1}\,b = e$$
   maka $(ab)^{-1} = b\,a$.

Latihan

1. Jika $\boldsymbol{R}^+$ menyatakan bilangan real positif maka buktikan bahwa $\boldsymbol{R}^+$ bukan grup.
2. Tunjukkan bahwa himpunan bilangan bulat $\boldsymbol{Z}$ bukan grup terhadap pengurangan.
3. Buktikan bahwa $< \boldsymbol{Q}, + >$ merupakan grup komutatif (abelian).
4. Misalkan $M_{2\times 2}$ adalah himpunan semua matrik ordo 2. Buktikan bahwa $M_{2\times 2}$ merupakan grup terhadap operasi penjumlahan dua matrik.
5. Buktikan sifat-sifat berikut :
   (1) Tunjukkan bahwa invers dari a^{-1} adalah : $(a^{-1})^{-1}$.
   (2) $(a^{-1} x\, a)^{-1} = a^{-1} x^{-1} a$.
   (3) $(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} a_{n-1}^{-1} \ldots a_2^{-1} a_1^{-1}$.
6. Operasi * didefinisikan pada R dengan aturan $a * b = a + b + 2$. Buktikan bahwa $< \boldsymbol{R}, * >$ merupakan grup.
7. Buktikan bahwa $(a^{-1} x\, a)^2 = a^{-1} x^2 a$ dan dengan induksi
   $$(a^{-1} x\, a)^n = a^{-1} x^n a$$
   untuk semua bilangan bulat positif n.
8. Misalkan $\boldsymbol{R}^{**}$ menyatakan himpunan semua bilangan real kecuali -1. Operasi * didefinisikan pada $\boldsymbol{R}^{**}$ dengan aturan
   $$a * b = a + b + ab.$$
   Buktikan bahwa $\boldsymbol{R}^{**}$ adalah grup di bawah operasi tersebut.
9. Misalkan $\boldsymbol{R}^{*2}=\{(a,b)\in\boldsymbol{R}^2 | a\neq 0 \text{ dan } b\neq 0\}$. Didefinisikan multiplikasi pada $\boldsymbol{R}^{*2}$ dengan $(a,b)\ (c,d) = (ac, bd)$. Tunjukkan bahwa R^{*2} grup di bawah operasi ini.
10. Misalkan $< A, . >$ sistim yang memenuhi 3 hukum pertama dalam grup dan A^* adalah himpunan dari semua elemen dari A yang mempunyai invers dalam A. Buktikan bahwa $< A^*, . >$ grup.
11. Buktikan bahwa jika $x = x^{-1}$ untuk semua x dalam grup G maka G abelian.
12. Buktikan bahwa jika $(ab)^{-1} = a^{-1} b^{-1}$ untuk semua a dan b dalam grup G maka G abelian.

13. Buktikan bahwa jika $(xy)^2 = a^2\, b^2$ untuk semua a dan b dalam grup G maka G abelian.
14. Suatu elemen x dalam grup G multiplikatif G disebut idempoten (*idempotent*) jika $x^2 = x$. Buktikan bahwa elemen identitas e merupakan satu-satunya elemen yang idempoten dalam grup G.
15. Misalkan $G = \{ 1, i, j, k, -1, -i, -j, -k \}$ dengan elemen identitas 1 dan perkalian elemen-elemennya adalah sebagai berikut :

    $(-1)^2 = 1$, $(i)^2 = (j)^2 = (k)^2 = -1$, $ij = -ji = k$,

    $jk = -kj = i$, $ki = -ik = j$, $-x = (-1)x = x(-1)$

    untuk semua $x \in G$. Buktikan G grup terhadap operasi perkalian. Apakah G komutatif ?

***

BAB III
GRUP BAGIAN

Sistim aljabar yang besar biasanya mengandung sistim bagian yang lebih kecil. Sistim yang lebih kecil mungkin lebih penting dan mungkin membangun sistim yang lebih besar. Sebagai contoh grup $< \boldsymbol{R}, + >$ mengandung grup yang lebih kecil seperti $< \boldsymbol{Q}, + >$ dan $< \boldsymbol{Z}, + >$. Dengan cara yang sama, terhadap operasi perkalian,

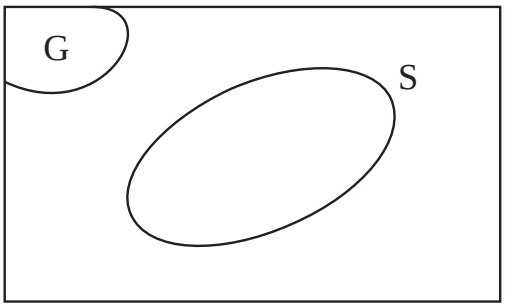
$$\boldsymbol{C}^* = \boldsymbol{C} - \{ 0 \}$$

mengandung $\boldsymbol{R}^* = \boldsymbol{R} - \{ 0 \}$.

Contoh-contoh di atas menyarankan bahwa di samping tipe tertentu dari sistim juga dipelajari sistim bagian (*subsystem*) sehingga dalam penelaahan grup juga dibahas tentang sistim bagiannya yang dinamakan grup bagian.

Definisi III.1

Suatu grup bagian *S* dari grup *G* adalah himpunan dari bagian *G* yang merupakan grup di bawah ***operasi yang sama*** dalam *G* yang dibatasi pada *S*.



Contoh III.1

1. Himpunan bilangan bulat $\boldsymbol{Z}$ merupakan grup bagian dari $\boldsymbol{R}$.
2. $S = \{ 0, 2, 4 \}$ merupakan grup bagian dari Z_6.
3. Z_6 bukan grup bagian dari Z_{12}.

4. Untuk sebarang grup G, himpunan $\{ e \}$ dan G merupakan grup bagian dari G.
   Grup bagian ini dinamakan **grup bagian tak sejati** (*improper subgroup*) dari G, sedangkan grup bagian yang lain dinamakan grup bagian sejati.

Teorema berikut merupakan teorema yang efisien untuk membuktikan bahwa suatu himpunan bagian dari grup G merupakan grup bagiannya.

Teorema III.1

Diketahui S himpunan bagian dari grup G dengan elemen identitas e. Himpunan S merupakan grup bagian dari G jika dan hanya jika memenuhi sifat :

1. $e \in S$,
2. S tertutup di bawah operasi dari G ,
3. untuk sebarang $x \in S$, inversnya x^{-1} terletak dalam S.

Bukti :

$\Rightarrow$

1. Dengan mengingat definisi S grup bagian maka S merupakan grup sehingga elemen identitasnya $e' \in S$.
   Akan ditunjukkan bahwa e' sebenarnya adalah e yaitu elemen identitas dalam G. Karena e' elemen identitas dalam S maka $e' e' = e'$.
   Dengan menggunakan sifat identitas dari e maka $e' = e' e$ sehingga
   $$e' e' = e' e$$
   dan dengan hukum kanselasi didapat $e' = e$.
2. Karena S grup maka S tertutup di bawah operasi dalam G.
3. Misalkan x sebarang elemen S.
   Karena S grup maka x mempunyai invers x' dalam S.
   Dengan mengingat ketunggalan dari suatu invers maka $x' = x^{-1}$ yaitu invers dari x dalam G.

$\Leftarrow$

Syarat 1 sampai 3 merupakan tiga syarat supaya suatu himpunan merupakan grup.
Syarat lain yang harus dipenuhi adalah hukum assosiatif.
Karena $(ab)\ c = a\ (bc)$ untuk semua elemen dalam G maka tentu saja juga berlaku untuk semua elemen dalam $S \subseteq G$.

Contoh III.2

1. $\boldsymbol{Q}^* = \{\ p/q \mid p$ dan q tidak nol dalam $\boldsymbol{Z}\ \}$ merupakan grup bagian dari $\boldsymbol{R}^*$.
2. Himpunan bilangan genap $\boldsymbol{E}$ merupakan grup bagian dari $\boldsymbol{Z}$.
3. $S = \{\ 3^k \mid k \in \boldsymbol{Z}\ \}$ merupakan grup bagian dari $\boldsymbol{R}^*$.

   Bukti:

   1) Elemen identitas berada dalam S.
      Karena $1 = 3^0$ maka berarti elemen identitas berada dalam S.
   2) Misalkan 3^j , 3^k dalam S.
      Karena perkalian 3^j dan 3^k adalah $3^j\ 3^k = 3^{j+k}$ dengan $j+k$ bilangan bulat maka $3^j\ 3^k \in$ S.
   3) Misalkan $3^k \in S$. Invers dari 3^k adalah $(3^k)^{-1} = 3^{-k}$ dengan $-k \in \mathbf{Z}$. Berarti $3^{-k} \in S$.

Contoh III.3 :

Tentukan grup bagian dari Z_4 yang dibangun oleh 2.

Jawab :

Grup $Z_4 = \{\ 0, 1, 2, 3\ \}$ merupakan grup terhadap operasi penjumlahan modulo 4.
Elemen 2 dalam Z_4 sehingga grup bagian yang dibangun oleh 2 adalah

$$(2) = \{\ k\ .\ 2 \mid k \in \mathrm{Z}\} = \{\ 0, 2\ \}.$$

Contoh III.4

Tentukan grup bagian dari ***R*** yang dibangun oleh 1.

Jawab :

Grup ***R*** merupakan grup terhadap operasi penjumlahan.
Elemen 1 dalam ***R*** sehingga grup bagian yang dibangun oleh 2 adalah

$(1) = \{ k \,.\, 1 \mid k \in Z \} = \{ \ldots\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\ldots \} = Z.$

Hal itu berarti grup bagian yang dibangun oleh 1 dalam ***R*** adalah himpunan bilangan bulat ***Z***.

Contoh III.4

Tentukan grup bagian yang dibangun oleh $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dalam $M_{2\times 2}^{*}$.

Jawab :

Grup $M_{2\times 2}^{*}$ merupakan grup terhadap operasi perkalian matriks dengan determinan tidak nol.
Berarti grup bagian yang dibangun oleh A adalah

$(A) = \{ A^k \mid k \in \mathrm{Z} \}$

$= \{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \ldots\ldots, \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}, \ldots\ldots \mid k \in Z \ \}.$

Latihan

1. Diketahui Z_4 merupakan grup terhadap operasi penjumlahan modulo 4. Tentukan semua grup bagian dari Z_4.
2. Diketahui Z_6 merupakan grup terhadap operasi penjumlahan modulo 6. Tentukan semua grup bagian dari Z_6.
3. Tentukan grup bagian dari Z_{18} yang dibangun oleh 4.
4. Tentukan grup bagian dari R^* yang dibangun oleh 1.
5. Buktikan bahwa $S = \{ 0 + b\,i \mid b \in \boldsymbol{R} \}$ merupakan grup bagian dari $\boldsymbol{C}$ tetapi bukan grup bagian dari $\boldsymbol{C}^*$.
6. Apakah $\boldsymbol{R}^+$ grup bagian dari $\boldsymbol{R}$? Buktikan jawaban anda !
7. Tentukan apakah himpunan berikut ini merupakan grup bagian dari grup $G = \{ 1, -1, i, -i \}$ di bawah operasi perkalian dan $i = \sqrt{-1}$. Jika himpunan ini bukan grup maka berikan alasannya.
   a. $\{ 1, -1 \}$
   b. $\{ i, -i \}$
   c. $\{ 1, i \}$
   d. $\{ 1, -i \}$
8. Diketahui $T = \{ x \in \boldsymbol{R}^+ \mid x \geq 1 \}$.
   a. Tunjukkan bahwa T mengandung identitas dari $\boldsymbol{R}^+$.
   b. Buktikan bahwa T bukan grup bagian dari $\boldsymbol{R}^+$.
9. Jika a sebarang elemen grup multiplikatif G maka buktikan bahwa
   $$(a^n) = (a^{-1})^n.$$
10. Diketahui $< G , + >$ grup abelian dan H, K grup bagian dari G.
    Jika didefinisikan $H + K = \{ h + k \mid h \in H \text{ dan } k \in K \}$, buktikan $H + K$ grup bagian dari G.
11. Misalkan $S = \{ (a,b) \in \boldsymbol{R}^2 \mid 2a - 3b = 0 \}$. Buktikan bahwa S grup bagian dari $< \boldsymbol{R}^2 , + >$.
12. Misalkan G sebarang grup dan $S = \{ x \in G \mid x^2 = e \}$.
    Tunjukkan bahwa S mengandung identitas dan mengandung invers dari semua elemennya tetapi tidak perlu menjadi grup bagian dari G.

13. Jika H dan K grup bagian dari grup G. Buktikan bahwa:

$$H \cap K = \{ x \mid x \in H \text{ dan } x \in K \}$$

merupakan grup bagian dari G.

14. Jika H dan K grup bagian dari grup G. Buktikan dengan contoh bahwa

$$H \cup K = \{ x \mid x \in H \text{ atau } x \in K \}$$

tidak perlu merupakan grup bagian dari G.

15. Misalkan G sebarang grup. Buktikan bahwa

$$C = \{ x \in G \mid gx = xg \text{ untuk semua } g \text{ dalam } G \}$$

merupakan grup bagian dari G.

16. Misakan S suatu himpunan bagian tidak kosong dari grup G. Jika untuk semua a dan b dalam S berlaku ab^{-1} dalam S maka buktikan bahwa S grup bagian dari G.

17. Buktikan bahwa

$$\{ A \in M_{2\times 2}^{*} \mid \det(A)=1 \}$$

grup bagian dari $M_{2\times 2}^{*}$.

18. Misalkan $< G , . >$ grup Abelian dan $S = \{ x \in G \mid x^3 = e \}$. Buktikan bahwa S grup bagian dari G.

19. Tentukan himpunan bagian dari Z yang tertutup terhadap penjumlahan tetapi bukan merupakan grup bagian dari Z terhadap operasi penjumlahan.

20. Misalkan G adalah grup dari semua bilangan real tidak nol di bawah operasi perkalian tetapi bukan grup bagian dari G.

***

BAB IV
GRUP SIKLIK

Dalam bab ini akan dibahas tentang grup siklik dan grup bagian siklik. Namun, sebelum itu terlebih dahulu didefinisikan pangkat bilangan bulat dalam suatu grup perkalian.

Definisi IV.1

Misalkan a sebarang elemen dari grup $< G, . >$. Didefinisikan :

$a^1 = a$

$a^2 = a \, . \, a$

$a^3 = a \, . \, a \, . \, a$

dan secara induksi, untuk sebarang bilangan bulat positif k berlaku sifat :

$$a^{k+1} = a \, . \, a^k \, .$$

Hal ini berarti bahwa a^n dimaksudkan sebagai perkalian a dengan a sampai n kali. Dalam hal ini suatu identitas dan invers dapat juga dinyatakan dengan menggunakan perpangkatan.

Definisi IV.2

Perjanjian bahwa $a^0 = e$ dan untuk sebarang integer positif n berlaku

$$a^{-n} = (a^{-1})^n = (a^{-1})(a^{-1}) \ldots (a^{-1})$$

sebanyak n faktor.

Dengan mudah dapat dibuktikan bahwa

$$a^n \, a^m = a^{m+n}$$

$$(a^m)^n = a^{mn} \, .$$

Jika $ab = ab$ maka $(ab)^n = a^n \, b^n$.

Catatan : Biasanya $(ab)^n \neq a^n b^n$. Jika $a \, b = b \, a$ maka $(ab)^n = a^n b^n$.

Notasi a^n digunakan dalam grup dengan operasi perkalian, sedangkan dalam grup dengan operasi penjumlahan digunakan definisi berikut ini.

Definisi IV. 3

Misalkan a sebarang elemen dari grup $< G, + >$.
Perkalian $n \,.\, a$ didefinisikan sebagai berikut :

1. $a = a$
2. $a = a + a$
3. $a = a + 2 \,.\, a$

dan secara induksi untuk sebarang integer positif k,

$$(k + 1) \,.\, a = a + k \,.\, a \,.$$

Lebih jauh,

$0 \,.\, a = 0$ (elemen identitas)

$- n \,.\, a = n \,.\, (-a) = (-a) + (-a) + \ldots + (-a)$

sebanyak n suku.

Perlu dicatat bahwa seperti dalam a^n , n dalam $n \,.\, a$ bukanlah elemen grup. Di samping itu berlaku sifat berikut :

$n \,.\, a + m \,.\, a = (n + m). a$

$n \,.(m \,.\, a) = (nm) \,.\, a$

$n \,.\, (a + b) = n \,.\, a + n \,.\, b$ jika $a + b = b + a$.

Teorema IV.1

Misalkan $< G , . >$ grup dan misalkan a sebarang elemen tertentu dari G. Jika

$$(a) = \{ a^k \mid k \in Z \}$$

maka himpunan (a) merupakan grup bagian dari G.

Bukti :

(digunakan sebagai latihan).

Definisi IV.4

Grup bagian (a) seperti yang didefinisikan dalam teorema di atas dinamakan *grup bagian siklik* yang dibangun oleh a.

Catatan: Grup bagian (a) merupakan grup bagian terkecil yang mengandung a.

Teorema IV.2

Misalkan a sebarang elemen grup $< G , . >$
Sifat – sifat berikut ini berlaku :

1. Jika untuk semua bilangan bulat positif m didapat $a^m \neq e$ maka berbagai pangkat dari a akan berbeda dan
$$(a) = \{ \ldots, a^{-2}, a^{-1}, a^0, a^1, a^2, \ldots \}$$
mempunyai elemen sebanyak tak hingga.
2. Jika terdapat bilangan bulat positif terkecil m sehingga $a^m = e$ maka
$$(a) = \{a^1, a^2, \ldots , a^m \}$$
mempunyai tepat m elemen.

Bukti

1. Misalkan k dan n bilangan bulat dengan $k > n$.
Karena $k > n$ maka $k - n$ positif dan dengan anggapan didapat $a^{k-n} \neq e$ sehingga
$$a^k = a^n .$$
Hal ini berarti bahwa pangkat berbagai bilangan bulat positif akan berbeda.
Akibatnya (a) mempunyai elemen tak hingga banyak.
2. Misalkan bilangan bulat positif terkecil m sehingga $a^m = e$ dan a^k sebarang pangkat bilangan bulat positif dari a.
Dengan menggunakan algoritma pembagian maka untuk k dan m dalam $\boldsymbol{Z}$ terdapatlah q dan r dalam $\boldsymbol{Z}$ sehingga
$$k = m\, q + r$$
dengan $0 \leq r < m$.

Akibatnya

$$a^k = a^{mq+r} = a^{mq}\, a^r = (a^m)^q\, a^r = a^q\, a^r = e\, a^r = a^r.$$

Hal ini berarti bahwa sebarang pangkat a^k dapat mereduksi menjadi a^r dengan

$$0 \le r < m.$$

Bila $r = 0$ maka $a^r = a^0 = e = a^m$.

Jika $0 < r < s \le m$ maka $0 < s - r < m$ sehingga $a^{r-s} \ne e$ dan akibatnya

$$a^r \ne a^s .$$

Jadi $a^1, a^2, \ldots, a^m$ semuanya berbeda dan (a) mempunyai m elemen.

Berdasarkan pembahasan pada bab-bab sebelumnya dapat diberikan sifat-sifat berikut ini :

1. Orde dari grup G adalah banyak elemen dalam G.
2. Grup G dikatakan abelian jika $ab = ba$ untuk semua $a, b \in G$.
3. Grup G dikatakan siklik asalkan $G = (a)$ untuk suatu elemen a dalam G yaitu

   $$G = \{ a^n \mid n \in \boldsymbol{Z} \}.$$

   Berarti G dibangun oleh a.
4. Orde dari elemen a dalam suatu grup G didefinisikan sebagai banyak elemen dalam grup bagian siklik (a).

Berikut ini diberikan contoh-contoh yang berkaitan dengan sifat-sifat di atas.

Contoh IV.1

1. Z_6 mempunyai orde 6 karena mengandung 6 elemen yaitu 0, 1, 2, 3, 4 dan 5. Secara umum Z_n mempunyai orde n.
2. $\boldsymbol{Z}$ mempunyai orde tak hingga karena $\boldsymbol{Z}$ mempunyai tak berhingga banyak elemen.
3. Orde dari himpunan $(i) = \{ i, -1, -i, 1 \}$ adalah 4.
4. Grup $M_{n \times n}$* untuk $n > 1$ bukanlah grup Abelian karena terdapat A, B dalam $M_{n \times n}$*

dengan $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ dan B = $\begin{pmatrix} 2 & 1 \\ 3 & 1 \end{pmatrix}$.

Tetapi dalam hal ini $AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix} = \begin{pmatrix} 5 & 1 \\ 3 & 0 \end{pmatrix}$ dan

$$BA = \begin{pmatrix} 2 & 1 \\ 3 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 3 & 3 \end{pmatrix}.$$

Berarti secara umum $AB \neq BA$.

5. Himpunan bilangan kompleks tidak nol $\boldsymbol{C}^*$ merupakan grup komutatif.
6. Grup Z_n untuk $n \geq 1$ merupakan grup siklik karena $Z_n = (1)$ untuk $n \geq 2$ sedangkan $Z_1 = (0)$. Demikian juga $\boldsymbol{Z}$ merupakan grup siklik karena $\boldsymbol{Z} = (1)$.
7. Himpunan bilangan real $\boldsymbol{R}$ bukan grup siklik tidak ada elemen $\boldsymbol{R}$ yang dapat membangun R.
8. Elemen 2 dalam Z_6 mempunyai orde 3 karena (2) = {0, 2, 4 } mempunyai 3 elemen.
   Berikut ini daftar dari orde elemen-elemen Z_6.

Elemen Z_6	0	1	2	3	4	5
Orde	1	6	3	2	3	6

9. Dalam sebarang grup G, identitas e mempunyai orde 1 karena (e) = {e} dan tidak ada elemen lain yang mempunyai orde 1 karena jika a dalam G dan $a \neq e$ maka (a) paling sedikit mengandung dua elemen yaitu a dan e.
10. Dalam himpunan bilangan real R, elemen -1 dalam R mempunyai orde tak hingga karena

    (-1) = { ..., 2, 1,0, -1, -2, -3, ... }

    mempunyai tak hingga banyak elemen. Ternyata, dapat dibuktikan bahwa semua elemen $\boldsymbol{R}$ yang tidak nol mempunyai orde tak hingga.
11. Dalam $\boldsymbol{R}^*$, -1 mempunyai orde 2 karena (-1) = { -1, 1 }.
12. Dalam $\boldsymbol{C}^*$, i mempunyai orde 4 karena (i) = { i, -1, -i, 1 }.

13. Dalam M_{2x2}^* , matriks $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ mempunyai orde 4 karena matriks ini membangun suatu grup bagian dari M_{2x2}^* yang mempunyai 4 elemen yaitu:

$$\left\{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}.$$

Untuk menjadi grup siklik suatu grup harus mempunyai pembangun (*generator*). Jika suatu grup mempunyai 20 elemen maka pembangunnya harus mempunyai orde 20.

Teorema IV.2

Grup berhingga G yang berorde n siklik jika dan hanya jika G mengandung suatu elemen dengan orde n.

Untuk grup tak hingga, tidak berlaku sifat yang analog dengan teorema di atas. Suatu grup tak hingga yang mengandung suatu elemen dengan orde tak hingga tidak perlu merupakan grup siklik. Sebagai contoh yaitu $\boldsymbol{R}$ dan $\boldsymbol{Q}$.

Teorema IV.3

Jika G grup siklik maka G abelian.

Bukti:

Misalkan G grup siklik.
Karena G siklik maka $G = (a)$ untuk suatu $a \in G$.
Misalkan $G = \{a^k \mid k \in Z\}$
Akan ditunjukkan bahwa $xy = yx$ untuk setiap $x, y \in G$.
Ambil sebarang x, y dalam G.
Karena x, y dalam G maka

$$x = a^m \text{ dan } y = a^n$$

untuk suatu m dan n dalam Z, sehingga

$$a^m a^n = a^{m+n}$$

dan

$$yx = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = xy.$$

Terbukti G grup abelian.

Teorema IV.4

Jika G grup siklik maka setiap grup bagian G merupakan grup siklik.

Bukti:

Misalkan $G = \{ a^k \mid k \in Z \}$dan S sebarang grup bagian dari G.

Kasus 1

Jika $S = \{ e \}$ maka jelas bahwa S siklik karena dibangun oleh e sendiri.

Kasus 2

Jika S mengandung elemen lain selain e maka ada suatu j tidak nol sehingga a^j dalam S.

Diasumsikan bahwa j positif karena untuk j negatif dapat diamati pada a^{-j}.

Karena S Grup bagian maka mengandung invers dari a^j yaitu a^{-j}.

Akan dibuktikan bahwa S siklik sehingga diperlukan suatu pembangun S.

Misalkan L bilangan bulat positif terkecil sehingga a^L dalam S.

Akan ditunjukkan bahwa $S = (a^L)$.

Karena a^L elemen dari grup S maka jelas bahwa $(a^L) \subseteq S$.

Misalkan $a^t \in S$.

Akan ditunjukkan bahwa a^t merupakan pangkat dari a^L .

Karena t dan L dalam Z maka dengan mengingat algoritma pembagian terdapatlah q dan r sehingga $t = Lq + r$ dengan $0 \leq r < L$.

Karena $a^t = a^{Lq+r}$ maka $a^t = a^{Lq} a^r$.

Karena $a^{-Lq} = (a^L)^q$ merupakan suatu pangkat dari a^L maka a^{-Lq} juga berada dalam S.

Lebih lanjut, $a^{-Lq} a^t = a^{-Lq} a^{Lq+r}$ sehingga $a^{-Lq} a^t = a^r$.

Karena ruas kiri dalam persamaan (*) merupakan perkalian dari dua elemen S maka a^r dalam S.

Karena L merupakan bilangan bulat positif terkecil sehingga a^L dalam S dan mengingat $0 \leq r < L$ maka $r = 0$.

Akibatnya $t = Lq$, sehingga $a^t = a^{Lq} = (a^L)^q$.

Hal ini berarti sebarang elemen a^t dalam merupakan pangkat dari a^L.

Teorema IV.5

Misalkan a sebarang elemen grup G.

1. Jika tidak ada pangkat positif dari a yang sama dengan e maka orde dari a adalah ∞ .
2. Jika terdapat bilangan bulat positif terkecil m sehingga $a^m = e$ maka orde dari a adalah m.

Bukti :

Analog dengan Teorema IV.2.

Teorema IV.6

Misalkan x sebarang elemen dari suatu grup multiplikatif G. Terdapat bilangan bulat positif k sehingga $x^k = e$ jika dan hanya jika orde dari x merupakan pembagi k.

Bukti :

$\Rightarrow$

Misalkan $x^k = e$ dan N orde dari x.

Untuk menunjukkan bahwa N membagi k digunakan algoritma pembagian

$$k = Nq + r$$

dengan $0 \leq r < N$.

Akan ditunjukkan bahwa $r = 0$.

Karena $e = x^k = x^{Nq+r} = x^{Nq}\, x^r$ dan N orde dari x (N bilangan bulat positif terkecil sehingga $x^N = e$) maka $x^r = e$.

Dengan mengingat N orde dari x dan $0 \leq r < N$ maka $r = 0$.

Terbukti bahwa orde dari x merupakan pembagian k.

$\Leftarrow$

(Digunakan sebagai latihan).

Teorema IV.7

Misalkan a sebarang elemen Z_n. Jika d merupakan pembagi persekutuan terbesar dari a dan n maka orde dari a sama dengan n/d.

Bukti :

Dianggap $a \neq 0$.
Orde dari a merupakan bilangan positif terkecil k sehingga $k\,a = 0$.
Untuk $k \,.\, a$ sama dengan 0 dalam Z_n maka $k.\ a$ haruslah merupakan kelipatan n.
Terlihat bahwa $k \,.\, a$ merupakan kelipatan a juga.
Tetapi k bilangan positif terkecil sehingga $k \,.\, a$ sama dengan 0 dan berarti $k \,.\, a$ harus merupakan kelipatan persekutuan terkecil dari a dan n.
Kelipatan persekutuan terkecil dari x dan y sama dengan xy/d dengan d pembagi persekutuan terbesar dari x dan y. Akibatnya

$$k \,.\, a = na/d$$
$$= (n/d)\, a$$
$$k = n/d.$$

Akhirnya untuk $a = 0$ didapat $k = 1$ dan $d = n$.

Contoh IV.2 :

Untuk menentukan orde dari 4 dalam Z_6 maka ditentukan terlebih dahulu factor persekutuan terbesar dari 4 dan 6 yaitu

$$FPB(4,6) = (\,2^2, 2.\,3\,) = 2$$

sehingga $n/d = 6/2 = 3$.
Di samping itu, untuk menentukan orde dari 36 dalam Z_{135}, pertama-tama ditentukan terlebih dulu pembagi persekutuan terbesar dari 36 dan 135.
Karena pembagi persekutuan terbesar dari 36 dan 135 adalah

$$(36, 135) = (2^2.\,3^2\,,\, 3^3\,.5\,) = 3^2 = 9.$$

Dengan menggunakan teorema di atas orde dari 36 sama dengan $n/d = 135/9 = 15$.

Contoh IV.3 :

Himpunan $Z_3 = \{ 0, 1, 2 \}$ grup terhadap penjumlahan modulo 3.
Grup bagian dari Z_3 yang dibangun oleh 0 adalah

$$(0) = \{ k.\, 0 \mid k \in \mathbf{Z} \} = \{ 0 \}$$

sehingga 0 mempunyai orde 1.
Grup bagian dari Z_3 yang dibangun oleh 1 adalah

$$(1) = \{ k.\, 1 \mid k \in \mathrm{Z} \} = \{ 0, 1, 2 \}$$

sehingga 1 mempunyai orde 3 dan berarti 1 merupakan pembangun Z_3.
Grup bagian dari Z_3 yang dibangun oleh 2 adalah

$$(2) = \{ k.\, 2 \mid k \in \mathrm{Z} \} = \{ 0, 2, 1 \}$$

sehingga 2 mempunyai orde 3 dan berarti 2 merupakan pembangun Z_3.
Hal itu berarti bahwa dalam Z_3 tidak ada grup bagian sejati.

Contoh IV.4

Tentukan grup bagian dari M_{2x2}^* yang dibangun oleh matriks

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Jawab:

Akan dihitung pangkat-pangkat dari A.

$$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

$$A^3 = A^2 A = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

$$A^4 = A^3 A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$ (identitas dalam M_{2x2}^*).

Oleh karena itu dalam M_{2x2}^* grup bagian yang dibangun oleh A adalah

$$\{ A, A^2, A^3, A^4 \}.$$

Perlu dicatat bahwa karena $\{ A, A^2, A^3, A^4 \}$ dibangun oleh A maka juga merupakan grup bagian siklik artinya ada elemen pembangun yaitu A.

Contoh IV.5

Misalkan A suatu elemen tertentu dari grup G. Jika didefinisikan

$$T = \{ x \in G \mid ax = xa \}$$

maka buktikan T grup bagian dari G.

Jawab :

1. T mengandung identitas e karena $ea = a = ae$.
2. Akan dibuktikan bahwa T tertutup.
   Jika dimisalkan x, y dalam T maka
   $$(xy)a = x(ya) = x(ay) = (ax)y = a(xy).$$
   Berarti xy dalam T atau T tertutup.
4. Jika dimisalkan x dalam T maka
   $$ax = xa$$
   $$x^{-1}(ax) = x^{-1}(xa)$$
   $$x^{-1}ax = a$$
   $$x^{-1}ax\,x^{-1} = a\,x^{-1}$$
   $$x^{-1}a = a\,x^{-1}.$$
   Berarti x^{-1} dalam T. Terbukti bahwa T grup bagian G.

Contoh IV.6

Jika $S = \{ x \in \boldsymbol{R} \mid x < 1 \}$ maka tunjukkan bahwa S bukan grup bagian dari $\boldsymbol{R}$.

Penyelesaian:

Karena 1/2 dan 3/4 dalam S tetapi jumlah dari keduanya tidak berada dalam S maka S bukan grup bagian dari R.

Contoh IV.7

$T = \{ 0, 2, 6 \}$ himpunan bagian dari Z_8 tetapi bukan grup bagian dari $\boldsymbol{R}$. Buktikan!

Jawab :

Karena 2 elemen dari T sedangkan 2 + 2 tidak berada dalam T maka T bukan grup bagian dari T.

Latihan

1. Buktikan bahwa $(a) = \{ a^k \mid k \in \boldsymbol{Z} \}$ merupakan grup bagian dari grup G.
2. Tentukan semua grup bagian dari Z_6 yang merupakan grup terhadap operasi penjumlahan modulo 6.
3. Buktikan bahwa setiap grup bagian dari suatu grup *A*belian merupakan grup abelian.
4. Buktikan bahwa $\boldsymbol{Q}$ tidak siklik.
5. Tentukan semua pembangun (*generator*) dari grup siklik Z_n di bawah operasi penjumlahan untuk $n = 8$, $n = 10$ dan $n = 12$.
6. Buktikan bahwa himpunan

$$H = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \middle| \ a \in Z \right\}$$

   adalah subgrup siklik dari grup semua matrik yang mempunyai invers dalam $M_{2\times 2}(\boldsymbol{R})$.
7. Buktikan bahwa jika x mempunyai orde berhingga N maka sebarang bilangan bulat q dan r berlaku $x^{Nq+r} = x^r$.
8. Misalkan a dan b dalam grup G. Buktikan bahwa jika $a \in (b)$ maka $(a) \subseteq (b)$.
9. Buktikan bahwa jika orde x membagi k maka $x^k = e$.
10. Misalkan G sebarang grup abelian dengan x, y dalam G.
    a. Jika x dan y masing-masing mempunyai orde 3 dan 4 maka tentukan orde dari xy.
    b. Jika x dan y masing-masing mempunyai orde 3 dan 6 maka tentukan orde xy.
    c. Berikan cara untuk menentukan orde dari sebarang elemen dalam G.
11. Diketahui G grup abelian. Misalkan

    $S = \{ x$ dalam $G \mid$ orde dari x merupakan pangkat dari $p \}$

    dengan p bilangan prima tertentu.
    Buktikan bahwa S grup bagian dari G.
12. Jika G merupakan suatu grup sehingga $x^2 = e$ untuk semua x dalam G. Buktikan bahwa G abelian.
13. Diketahui G grup abelian. Jika $T = \{ x$ dalam $G \mid$ orde x berhingga $\}$.

Buktikan bahwa T grup bagian dari G.

14. Misalkan a sebarang elemen dari grup perkalian G.
    a. Buktikan bahwa a^{-1} dan a mempunyai orde yang sama.
    b. Nyatakan hubungan antara orde dari a dan orde dari a^k.

15. Diketahui matriks $A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

    dan matriks $B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$.

    Tentukan orde dari A, B dan AB.

***

BAB V
GRUP Z_n^*

Perkalian dapat didefinisikan pada himpunan $Z_n = \{ 0, 1, 2, \ldots , n-1 \}$ dari bilangan bulat modulo n. Jika a, b dalam Z_n maka perkalian dari $a\ b$ (mod n) adalah :

1. Kalikan bilangan bulat a dan b.
2. Ambil sisa pembagian dari ab dengan n yaitu r. Berarti $a\ b = r$.

Mudah dibuktikan bahwa untuk $n > 1$, Z_n mengandung identitas perkalian 1. Tetapi dalam Z_n, invers terhadap perkalian tidak selalu ada sehingga Z_n bukanlah grup terhadap operasi perkalian. Untuk $n \geq 2$ didefinisikan

$Z_n^* = \{ x$ dalam $Z_n \mid x$ mempunyai invers terhadap perkalian dalam $Z_n \}$.

Teorema V.1

Untuk $n \geq 2$ maka $< Z_n^* , . >$ merupakan grup abelian.

Beberapa contoh berikut ini memperlihatkan bahwa grup Z^* mungkin siklik atau tak siklik.

Contoh V.1

$Z_2^* = \{ x$ dalam $Z_2 \mid x$ mempunyai invers perkalian dalam $Z_2 \} = \{ 1 \}$.
Berarti Z_2^* mempunyai orde 1 dan elemen 1 dalam Z_2^* mempunyai orde 1. Grup bagian dalam Z_2^* hanyalah Z_2^*.

Contoh V.2

$Z_3^* = \{ x$ dalam $Z_3 \mid x$ mempunyai invers perkalian dalam $Z_3 \} = \{ 1, 2 \}$.
Berarti Z_3^* mempunyai orde 2 dan elemen 1 dalam Z_2^* mempunyai orde 1 karena $(1) = \{ 1 \}$. Elemen 2 dalam Z_3^* mempunyai orde 2 karena $(2) = \{ 2^k \mid k \in Z \} = \{ 1, 2\}$. Grup bagian dalam Z_3^* hanyalah

{1} dan Z_3*. Demikian juga karena ada elemen dalam yang mempunyai orde 2 maka merupakan grup siklik.

Contoh V.3

Untuk menemukan elemen Z_{10}* dapat digunakan metode *trial and error* sehingga

1 . 1 = 1,
3 . 7 = 7 . 3 =1,
9 . 9 = 1,

dan oleh karena itu 1, 3, 7 dan 9 merupakan elemen Z_{10}*.
Dapat dibuktikan juga bahwa 0, 2, 4, 6, dan 8 tidak mempunyai invers terhadap perkalian dalam Z_{10}* .
Oleh karena itu Z_{10}* = { 1, 3, 7, 9 }.
Dalam pembahasan teori grup, apabila ditemui suatu grup selalu muncul pertanyaan berapakah orde dari grup tersebut ?
Jelas bahwa Z_{10}* mempunyai orde 4 dan dengan Teorema V.1 maka maka Z_{10}* abelian.
Pertanyaan selanjutnya adalah apakah Z_{10}* siklik ?
Dengan mengingat Teorema IV.2, dibutuhkan suatu elemen Z_{10}* yang mempunyai orde 4 supaya Z_{10}* siklik.
Misalkan diambil elemen 3 dalam Z_{10}* dan dicek orde dari elemen itu:

$$3^2 = 9 , 3^3 = 7 , 3^4 = 1.$$

Dari perhitungan di atas terlihat bahwa 3 mempunyai orde 4.
Dapat dibuktikan juga bahwa 1 mempunyai orde 1, 7 mempunyai orde 4 dan 9 mempunyai orde 2.
Karena terdapat suatu elemen Z_{10}* yang mempunyai orde 4 maka Z_{10}* siklik.

Contoh V.4:

Dapat dibuktikan bahwa Z_8* = { 1, 3, 5, 7 } dan merupakan suatu grup abelian dengan orde 4 dan elemennya memenuhi $1^1 = 3^2 = 5^2 = 7^2 = 1$.
Oleh karena itu elemen-elemennya mempunyai orde 1 atau 2 dan akibatnya Z_8* tidak siklik.

Teorema V.2

Elemen Z_n^* adalah elemen a dalam Z_n sehingga pembagi persekutuan terbesar (*greatest common divisor*) dari a dan n adalah 1 atau $d = (a, n) = 1$.

Catatan:

Dalam hal ini a dan n dinamakan *prima relatif*. Dengan kata lain, teorema tersebut mengatakan bahwa elemen Z_n^* merupakan elemen Z_n sehingga a prima relatif dengan n.

Bukti :

Jika d=1 maka orde dari a dalam Z_n sama dengan $n/d = n/1 = n$ sehinggga semua n elemen Z_n termasuk dalam $1 . a, 2 . a, \ldots\ldots, n . a = 0$.
Oleh karena itu, salah satunya akan sama dengan 1, misalkan $k . a = 1$ dengan $1 \leq k < n$.
Akibatnya k dalam Z_n^* merupakan invers perkalian dari a.
Pada sisi lain, misalkan a sebarang elemen dari Z_n^* dengan invers perkalian b maka untuk bilangan bulat $b . a = 1$.
Akibatnya grup bagian $(a) = \{ 1 . a, 2 . a, \ldots\ldots, b . a, \ldots\ldots, 0 \}$ dari Z_n mengandung $b . a = 1$ sehingga (a) mengandung $(1) = Z_n$.
Oleh karena itu a membangun Z_n dan mempunyai orde n dalam Z_n sehingga $n/d = n$ dan $d = 1$.

Contoh V.5

Jika p bilangan prima maka sebarang elemen tidak nol dalam Z_p akan prima relatif dengan p sehingga $Z_p^* = \{ 1, 2, 3, \ldots\ldots, p\text{-}1 \}$ dan berarti orde dari Z_p^* adalah p-1.

Contoh V.6

Z_{15}^* mengandung semua elemen a dalam Z_{15} sehingga a prima relatif dengan 15.
Dalam hal ini $Z_{15}^* = \{ 1, 2, 4, 7, 8, 11, 13, 14 \}$ dan $9 \notin Z_{15}^*$ karena $(9,15) = 3$.

Latihan

1. Berikan sifat-sifat dari Z_4*.
2. Berikan sifat-sifat dari Z_5*.
3. Berikan sifat-sifat dari Z_6*.
4. Berikan sifat-sifat dari Z_7*.
5. Berikan sifat-sifat dari Z_9*.
6. Berikan sifat-sifat dari Z_{11}*.
7. Berikan sifat-sifat dari Z_p* dengan p bilangan prima.
8. Berikan sifat-sifat dari Z_{14}*.
9. Tentukan banyak elemen dari Z_{15}*.
10. Tentukan banyak elemen dari Z_{2013}*.
11. Berikan sifat dari Z_{p^2}* yaitu Z_4*, Z_9* dan Z_{25}*.
12. Berikan sifat-sifat dari Z_{pq}* dengan p dan q bilangan prima yang berbeda.
13. Buktikan mengapa setiap Z_n* dengan $n \geq 3$ mempunyai orde genap.
14. Diketahui G grup dan a dalam G yang memenuhi $a^8 \neq e$ dan $a^{16} = e$.
    Tentukan orde a dan beri alasannya.
15. Berikan contoh khusus dari grup G dan a dalam G yang memenuhi $a^6 \neq e$ dan $a^{12} = e$ tetapi orde dari a tidak sama dengan 12.

***

BAB VI
TEOREMA LAGRANGE

Bila suatu grup G diperkenalkan maka dengan sendirinya diteliti apakah grup itu abelian dan apakah grup tersebut siklik. Di samping itu juga ditentukan orde dari grup G dan orde dari elemen-elemennya. Meskipun dapat dibuktikan bahwa semua grup bagian dari grup siklik merupakan grup siklik dan semua grup bagian dari grup abelian merupakan grup abelian, tetapi masih menyisakan pertanyaan-pertanyaan yang belum terjawab :

1. Bagaimana orde dari suatu grup bagian S dibandingkan dengan orde dari grup yang mengandung S ?
2. Bagaimana orde dari suatu elemen grup G dibandingkan orde dari G ?

Teorema terbukti ini sangat penting dalam teori grup dan sekaligus menjawab kedua pertanyaan tersebut.

Teorema VI.1 (*Teorema Lagrange*)

Jika G sebarang grup berhingga dan S grup bagian G maka orde S membagi orde G.

Keterangan :

1. Himpunan aS dan bS dinamakan koset kiri dari S.
   Dinamakan koset kiri karena elemen a dan b berada di kiri. Dengan definisi
   $$aS = \{ as \mid s \text{ dalam } S \}.$$
2. Karena $S = eS$ maka berarti S merupakan koset kiri juga.
   Jika $aS \neq S$ maka aS tidak mengandung identitas e.
3. Di samping itu juga terdapat koset kanan $Sa = \{ sa \mid s \text{ dalam } S \}$.
4. Dalam notasi penjumlahan, koset kiri ditulis sebagai
   $$a + S = \{ a + s \mid s \text{ dalam } S \}.$$

Beberapa contoh berikut ini menjelaskan bahwa koset-koset S, aS, bS, ... menyekat grup G menjadi himpunan-himpunan bagian yang saling asing.

Contoh VI.1

Diketahui $G = Z_{25}^*$ dan $S = (16)$.
Akan diperhatikan penyekatan grup G ke dalam koset–koset kiri dari S.

$S = \{ 16, 6, 21, 11, 1 \}$, $3S = \{ 23,18, 13, 8, 3 \}$,
$2S = \{ 7, 12, 17, 22, 2 \}$, $4S = \{ 14, 24, 9, 19, 4 \}$.

Berarti koset – koset kiri dari S membagi 20 elemen dalam Z_{25}^* ke dalam 4 himpunan bagian yang saling asing dan masing-masing mengandung 5 elemen.

Contoh VI.2 :

Misalkan $G = \boldsymbol{Z}$ dan $S = (4)$.
Akan ditunjukkan bahwa dalam grup dengan orde tak hingga koset-koset $S = (4)$.
Menyekat grup $\boldsymbol{Z}$ ke dalam himpunan dengan ukuran yang sama.
Karena $S = \{....., -8, -4, 0, 4, 8,...\}$ maka koset-koset kiri adalah

$1 + S = \{ ....., -7, -3, 1, 5, 9, 13,...\}$,
$2 + S = \{ ....., -6, -2, 2, 6, 10, 14, ...\}$,
$3 + S = \{ ...., -5, -1, 3, 7, 11, ...\}$.

Terlihat bahwa terdapat 4 koset kiri dari $S = (4)$ yang berbeda dalam $\boldsymbol{Z}$ yaitu $0 + S$, $1 + S$, $2 + S$ dan $3 + S$.
Meskipun dalam grup tak hingga konsep orde S membagi orde G tetapi koset-koset kiri dari S tetap membagi Z ke dalam himpunan-himpunan bagian yang tidak saling asing dan masing-masing dengan banyak elemen yang sama.

Teorema VI.2

Jika G sebarang grup berhingga berorde n dan a sebarang elemen G maka orde a membagi orde G.

Bukti:

Elemen a membangun grup bagian siklik (a).
Dengan menggunakan definisi, orde dari a sama dengan orde dari (a) dan dengan mengingat teorema Lagrange, orde dari grup bagian (a) membagi orde G.

Bilangan prima mempunyai arti penting dalam teori grup dan teorema Lagrange memberikan *informasi penting tentang grup dengan orde prima*.

Teorema VI.3

Jika grup G mempunyai orde prima p maka G siklik dan isomorfis dengan Z_p.

Bukti :

Dengan mengingat Teorema VI.2, Jika a sebarang elemen G maka ordenya membagi p karena p prima maka a mempunyai orde 1 atau p.
Tetapi karena hanya elemen identitas yang mempunyai orde 1 maka untuk $a \neq e$ mempunyai orde p.
Oleh kaena itu, G dibangun oleh sebarang elemen $a \neq e$.
Berarti G siklik.
Karena G siklik dan mempunyai orde p maka $G \cong Z_p$.

Teorema di atas mengelompokkan bahwa semua grup orde p. Untuk sebarang bilangan prima p dimiliki tepat satu kelompok untuk grup orde p dan dinamai Z_p. Akibat lainnya adalah bahwa tidak ada grup orde p yang tidak komutatif.

Contoh VI.3

Berikan sifat-sifat dari Z_4.

Jawab

Himpunan Z_4 = { 0, 1, 2, 3 } merupakan grup terhadap penjumlahan modulo 4. Grup bagian yang dibangun oleh elemen-elemen dalam Z_4 adalah:

$(0) = \{ k \,.\, 0 \mid k \in \boldsymbol{Z} \} = \{ 0 \}$,
$(1) = \{ k \,.\, 1 \mid k \in \boldsymbol{Z} \} = \{ 0, 1, 2, 3 \}$,
$(2) = \{ k \,.\, 2 \mid k \in \boldsymbol{Z} \} = \{ 0, 2 \}$,
$(3) = \{ k \,.\, 3 \mid k \in \boldsymbol{Z} \} = \{ 0, 3, 2, 1 \}$.

Hal itu berarti bahwa elemen 0 mempunyai orde 1, elemen 1 dan 3 mempunyai orde 4 dan elemen 2 mempunyai orde 2 sehingga grup tersebut siklik karena ada elemen dalam Z_4 yang mempunyai orde 4 yaitu 1 dan 3. Grup bagian dari adalah {0}, { 0, 2} dan Z_4 yang berturut-turut mempunyai orde 1, 2 dan 4.

Contoh VI.4 :

Tentukan sifat-sifat dari Z_{12}^*.

Jawab

Himpunan Z_{12}^* = { 1, 5, 7, 11 } merupakan grup dengan orde 4. Dengan menggunakan teorema Lagrange maka elemen-elemen dalam Z_{12}^* mempunyai orde 1, 2 atau 4. Elemen 1 mempunyai orde 1, elemen 5 mempunyai orde 2, elemen 7 mempunyai orde 1 dan elemen 11 mempunyai orde 2. Karena tidak ada elemen dalam Z_{12}^* yang mempunyai orde 4 maka Z_{12}^* bukanlah grup siklik. Grup bagian dalam Z_{12}^* mempunyai orde 1 , 2 atau 4 yaitu sesuai dengan teorema Langrange. Dalam hal ini, grup bagian tersebut adalah { 1 }, { 1, 5}, { 1, 7 }, {1, 11} dan Z_{12}^*.

Latihan :

1. Tentukan orde dari setiap elemen dalam Z_5. Tentukan semua grup bagian dalam Z_5.
2. Tentukan orde dari setiap elemen dalam Z_6.
3. Tentukan orde dari setiap elemen dalam Z_7* dan tentukan semua grup bagiannya.
4. Tentukan orde dari setiap elemen dalam Z_9* dan apakah grup tersebut siklik?
5. Tentukan orde dari setiap elemen dalam Z_{11}* dan tentukan semua grup bagiannya.
6. Tentukan orde dari setiap elemen dalam Z_{13}*.
7. Tentukan banyaknya grup bagian dalam Z_{14}*.
8. Tentukan banyaknya grup bagian dalam Z_{20}*.
9. Tentukan orde dari setiap elemen dalam Z_{15}* dan apakah grup tersebut siklik?
10. Misalkan G grup yang mempunyai orde p^m dengan p prima dan $m > 0$.
    Buktikan bahwa G mengandung grup bagian dengan orde p. Jika $m \geq 2$ maka apakah G perlu mempunyai elemen yang mempunyai orde p^2 ?
11. Berikan contoh grup berhingga orde n yang tidak mengandung sebarang elemen dengan orde d untuk suatu d pembagi sejati dari n.
12. Buktikan bahwa $aS = bS$ jika dan hanya jika $b^{-1} a \in S$.
13. Buktikan bahwa grup G dengan 2 elemen merupakan grup abelian.
14. Buktikan bahwa grup G dengan 3 elemen merupakan grup abelian.
15. Buktikan bahwa grup G dengan 4 elemen merupakan grup abelian.

***

BAB VII
HOMOMORFISMA GRUP

Dalam mempelajari sistim, perlu juga mempelajari tentang suatu fungsi yang mengawetkan operasi aljabar. Sebagai contoh, dalam aljabar linier dipelajari tentang alih ragam linier (*linear transformation*). Fungsi ini $T : V \to W$ ***mengawetkan*** penjumlahan dan perkalian skalar. Dalam teori grup digunakan definisi berikut ini.

Definisi VII.1

Diketahui pemetaan/fungsi $f : A \to B$. Fungsi f dikatakan surjektif jika dan hanya jika untuk setiap $y \in B$ terdapat $x \in A$ sehingga $y = f(x)$.

Contoh VII.1 :

Diketahui fungsi $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = x$. Fungsi f merupakan fungsi yang surjektif. Sedangkan fungsi $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = x^2$ bukan fungsi surjektif karena $-2 \in \boldsymbol{R}$ tetapi tidak ada $x \in \boldsymbol{R}$ sehingga

$$f(x) = x^2 = -2.$$

Definisi VII.1

Diketahui pemetaan/fungsi $f : A \to B$. Fungsi f dikatakan injektif jika dan hanya jika untuk setiap $x, y \in A$ dengan $f(x) = f(y)$ berlaku $x = y$.

Contoh VII.2 :

Diketahui fungsi $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = x^3$. Fungsi f merupakan fungsi yang injektif karena untuk setiap $x, y \in \boldsymbol{R}$ dengan $f(x) = f(y)$ maka $x^3 = y^3$ sehingga berlaku $x = y$. Sedangkan fungsi $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan

$f(x) = x^2$ bukan fungsi injektif karena ada -2 , $2 \in \boldsymbol{R}$ dan $-2 \neq 2$ tetapi $f(-2) = (-2)^2 = 4 = 2^2 = f(2)$.

Definisi VII.1

Diketahui pemetaan/fungsi $f : A \to B$. Fungsi f dikatakan bijektif jika f injektif dan f surjektif.

Contoh VII.3 :

1. Fungsi $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = x$ merupakan fungsi bijektif.
2. Fungsi $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = x^2$ merupakan bukan fungsi bijektif karena f tidak injektif.
3. Fungsi $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = 2x + 3$ merupakan fungsi bijektif.
4. Fungsi $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = x^3$ merupakan fungsi bijektif.
5. Fungsi $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = e^x$ merupakan fungsi bijektif.

Definisi VII.1

Misalkan $< G, * >$ dan $< H, . >$ grup.
Pemetaan $f : G \to H$ dinamakan homomorfisma grup jika f mengawetkan operasi yaitu asalkan bahwa $f(x * y) = f(x) . f(y)$ untuk semua x, $y \in G$.

Contoh VII.4

Misalkan $< G, . >$ suatu grup abelian dan n bilangan bulat tertentu.
Akan ditunjukkan bahwa aturan $f(x) = x^n$ mendefinisikan suatu homomorfisma

$$f : G \to G.$$

Karena $f(xy) = (xy)^n = x^n y^n = f(x) f(y)$ maka f mengawetkan operasi.
Khususnya, $\phi : Z_{10}^* \to Z_{10}^*$ dengan $\phi(x) = x^2$. Hal itu berarti $\phi(1) = 1$, $\phi(3) = 9$, $\phi(7) = 9$, dan $\phi(9) = 1$.

Contoh VII.5

Determinan sebenarnya merupakan homomorfisma dari M_{2x2}* ke $\boldsymbol{R}$* karena determinan mempunyai sifat det(AB) = det(A) . det(B) yang berarti fungsi determinan mengawetkan operasi. Dalam hal ini determinan juga merupakan fungsi yang surjektif.

Suatu homomorfisma grup yang bijektif (surjektif dan injektif) dinamakan *isomorfisma* grup, sedangkan isomorfisma dari grup G ke dirinya sendiri dinamakan *automorfisma*. Dalam teori grup automorfisma dapat digunakan untuk menghubungkan grup bagian dari suatu grup G dengan grup bagian yang lain dalam upaya menganalisis struktur dari grup G. Salah satu bentuk automorfisma yang penting adalah sebagai berikut: untuk setiap b dalam G terdapat suatu automorfisma f_b yang membawa x ke konjugatnya yaitu $b^{-1}xb$. Peta dari sebarang grup bagian S di bawah automorfisma f_b adalah $b^{-1}Sb = \{ b^{-1} s b \mid s \text{ dalam } S \}$. Dalam hal ini merupakan grup bagian dari G yang isomorfis dengan S. Berbagai grup bagian $b^{-1}Sb$ dinamakan *konjugat* dari S.

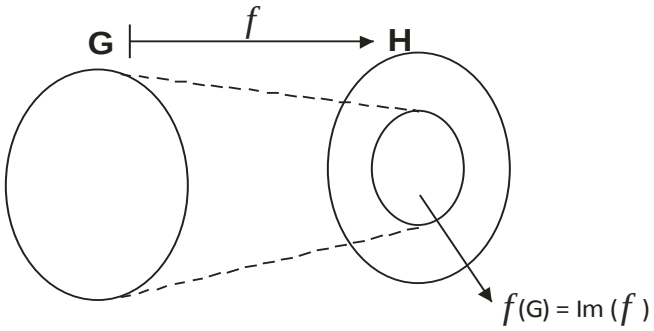
Manfaat utama dari homomorfisma $f : G \to H$ yaitu dengan melihat sifat-sifat dari petanya (*image*) dapat disimpulkan sifat-sifat dari grup G.

Definisi VII.3

Peta Im(f) atau $f(G)$ dari homomorfisma grup $f : G \to H$ didefinisikan sebagai

$$\text{Im}(f) = f(G) = \{ f(G) \mid g \in G \}.$$

Peta dari homomorfisma f sama dengan H jika f surjektif atau f pada (*onto*) H.



Teorema VII.1

Jika $f: G \to H$ homomorfisma grup maka $f(G) = \text{Im}(f)$ grup bagian dari H.

Bukti

Akan dibuktikan bahwa f(G) tertutup.
Ambil sebarang $f(a)$, $f(b)$ dalam $f(G)$. Karena f homomorfisma maka $f(ab) = f(a)\, f(b)$.
Tetapi a, b dalam G sehingga ab dalam G (sebab G grup).
Jadi $f(a)\, f(b) = f(ab)$ dalam G dengan ab dalam G atau $f(G)$ tertutup.
Akan dibuktikan bahwa e′ dalam f(G).
Elemen e' adalah identitas dalam H untuk membedakan dengan e dalam G.
Misalkan $f(b)$ sebarang elemen dalam $f(G)$.
Karena $f(b)$ dalam $f(G)$ maka $f(e)\, f(b) = f(eb) = f(b) = e'\, f(b)$.
Dengan menggunakan hukum kanselasi kanan didapat $f(e) = e'$.
Akan dibuktikan f(G) mengandung invers dari elemen f(G).
Misalkan $f(x)$ dalam $f(G)$.
Elemen $f(x^{-1})$ merupakan invers dari $f(x)$ karena

$$f(x)\ f(x^{-1}) = f(xx^{-1}) = f(e) = e'.$$

Dengan cara yang sama, didapat $f(x^{-1})\, f(x) = e'$ dan $f(x^{-1})$ invers (yang tunggal) dari $f(x)$ dengan $f(x^{-1})$ dalam $f(G)$.

Teorema di atas dapat dikembangkan untuk fungsi $f: G \to B$ dengan B tidak perlu suatu grup. Sebagai contoh $M_{2\times 2}$ bukan merupakan grup di bawah operasi perkalian matriks tetapi dapat

didefinisikan suatu fungsi $f : G \to M_{2\times 2}$ yang mengawetkan perkalian matriks.

Teorema VII.2

Misalkan < G, . > grup dan < B,* > sistim aljabar dengan operasi *.
Jika fungsi $f : G \to B$ mengawetkan operasi maka Im(f) merupakan grup terhadap operasi * yang termuat dalam sistim B.

Bukti:

Dengan sedikit perubahan pada pembuktian Teorema VII.1 maka dapat dibuktikan sifat ketertutupan, identitas dan hukum invers. Tinggal dibuktikan bahwa hukum assosiatif berlaku.
Misalkan $f(a), f(b), f(c)$ dalam $f(G)$.
Pada satu sisi,

$$(f(a)*f(b)) * f(c) = f(ab)*f(c) = f((ab)c).$$

Sedangkan pada sisi lain,

$$f(a) * (f(b)*f(c)) = f(a)*f(bc) = f(a(bc)).$$

Karena G grup maka $(ab)\, c = a\, (bc)$ sehingga kedua hasil di atas sama.

Sistim aljabar $<M_{2\times 2}$, .> bukanlah suatu grup (terhadap operasi perkalian matriks) karena hukum invers tidak dipenuhi. Dengan mendefinisikan pemetaan $f : C^* \to M_{2\times 2}$ dengan

$$f(a + b\, i) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

Dapat ditunjukkan bahwa f mengawetkan operasi perkalian matriks. Oleh karena itu peta f yaitu

$$S = \{ \quad \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \quad | \ a, b \text{ dalam } R \text{ dengan } a \text{ dan } b \text{ tidak keduanya nol } \}$$

merupakan grup di bawah perkalian dan S termuat dalam $M_{2\times 2}$.

Contoh VII.6

Dalam contoh ini diperlihatkan bagaimana menggunakan suatu fungsi dari grup $\boldsymbol{Z}$ ke Z_n untuk membuktikan bahwa Z_n grup. Didefinisikan $f : \boldsymbol{Z} \to Z_n$ dengan $f(x) = r$ dan r merupakan sisa pembagian x oleh n.
Akan ditunjukkan bahwa f mengawetkan operasi penjumlahan.
Misalkan x, y dalam Z dan ditulis $x = n\,q_1 + r_1$ dan $y = n\,q_2 + r_2$ sehingga

$$x + y = (\,n\,q_1 + r_1\,) + (\,n\,q_2 + r_2\,) = n\,(\,q_1 + q_2\,) + (\,r_1 + r_2\,)$$

dan demikian juga $r_1 + r_2$ dapat dinyatakan sebagai $nq + r$ sehingga

$$x + y = n\,(\,q_1 + q_2 + q\,) + r.$$

Dengan menerapkan f pada $x + y$ diperoleh

$$f(x + y) = r.$$

Karena $x + y$ mempunyai sisa r bila dibagi dengan n.
Pada sisi lain

$$f(x) + f(y) = r_1 + r_2 = r.$$

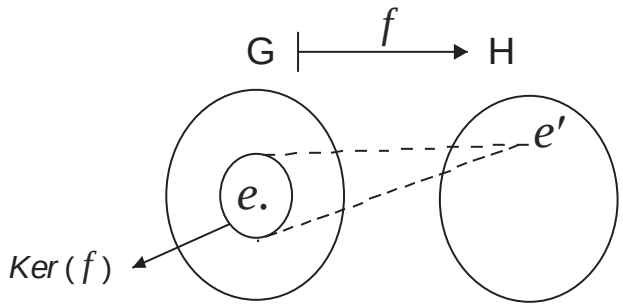
Karena $r_1 + r_2$ mempunyai sisa r bila dibagi dengan n.
Oleh karena itu $f(x + y) = f(x) + f(y)$.
Dalam hal ini jelas bahwa peta dari f adalah Z_n sehingga dengan mengingat teorema diperoleh Z_n grup.

Konsep yang berlaku pada peta dari homomorfisma f dapat juga digunakan pada inti (*kernel*) dari homomorfisma.

Definisi VII.4

Misalkan $f : G \to H$ homomorfisma grup. Inti dari f atau Ker(f) didefinisikan sebagai elemen G yang dipetakan oleh f ke elemen identitas dari H yaitu

$$\text{Ker}(f) = \{\, x \in G \mid f(x) = e \,\}.$$



Contoh VII.7

Bila didefinisikan pemetaan $f : Z_{20}^* \rightarrow Z_{20}^*$ dengan $f(x) = x^2$ maka dengan menggunakan metode *trial and error* akan diperoleh

$$\text{Ker}(f) = \{1, 9, 11, 19\}.$$

Teorema VII.3

Jika $f : G \rightarrow H$ homomorfisma grup maka Ker(f) grup bagian dari G.

Bukti :

Akan dibuktikan bahwa e dalam Ker(f).
Telah ditunjukkan bahwa $f(e) = e'$.
Akibatnya identitas e dalam G merupakan elemen Ker(f).
Akan ditunjukkan bahwa Ker(f) tertutup.
Misalkan x, y dalam Ker(f).
Karena x, y dalam Ker(f) maka $f(x) = e'$ dan $f(y) = e'$ sehingga

$$f(xy) = f(x)\, f(y) = e'\, e' = e'.$$

Oleh karena itu , xy dalam Ker(f).
Akan ditunjukkan bahwa Ker(f) mengandung invers dari elemennya.
Misalkan x dalam Ker(f).
Karena x dalam Ker(f) maka $f(x) = e'$ sehingga

$$\begin{aligned} f(x) &= e' \\ f(x)\, f(x^{-1}) &= e'\, f(x^{-1}) \\ f(x\, x^{-1}) &= f(x^{-1}) \\ f(e) &= f(x^{-1}) \\ e' &= f(x^{-1}) \end{aligned}$$

Berarti $f(x^{-1})$ dalam Ker(f).■

Dalam pembahasan suatu homomorfisma grup, sangatlah bermanfaat untuk menentukan inti dan peta dari f. Teorema berikut ini berkaitan dengan sifat peta homomorfisma.

Teorema VII.4

Misalkan $f : G \to H$ homomorfisma grup dengan peta $f(g)$. Sifat-sifat berikut ini berlaku:

1. Jika G berhingga maka orde dari $f(G)$ membagi orde G.
2. Jika G siklik maka $f(G)$ siklik.
3. Jika $a \in G$ mempunyai orde berhingga maka orde dari membagi orde a.
4. Jika G abelian maka $f(G)$ abelian.

Bukti :

(1) Untuk latihan.

(2) Misalkan $G = (a) = \{ a^k \mid k \in Z \}$.
Akibatnya $f(G) = \{ f(a^k) \mid k \in Z \}$.
Tetapi karena $f(a^k) = (f(a))^k$ (dengan induksi) maka
$f(G) = \{ (f(a))^k \mid k \in Z \}$.
Berarti $f(G)$ dibangun oleh $f(a)$ atau $f(G)$ siklik.

(3) Orde dari $f(a)$ sama dengan orde dari grup bagian siklik ($f(a)$)
Tetapi pada bagian (2) dalam bukti ini terlihat bahwa f membawa (a) pada ($f(a)$).
Pada bagian (1) dalam bukti ini juga menjelaskan bahwa orde dari ($f(a)$) membagi orde (a).
Dengan kata lain, orde dari ($f(a)$) membagi orde a.

(4) Ambil sebarang $f(a), f(b)$ dalam $f(G)$ dengan G abelian.
Akibatnya $f(a)\, f(b) = f(ab) = f(ba) = f(a)\, f(b)$.
Berarti $f(G)$ abelian.■

Pada bukti bagian 1 teorema di atas menunjukkan bahwa suatu homomorfisma f tepat k ke 1 dengan k menyatakan banyak elemen dalam inti f yaitu untuk setiap elemen peta f tepat mempunyai k elemen yang dibawa kepadanya.

Contoh VII.8 :

Fungsi $f: Z_{10} \to Z_{10}$ dengan $f(x) = 8x$ merupakan homomorfisma 2 ke 1.
Karena $f(0) = 0$ dan $f(5) = 0$ maka $K = \text{Ker}(f) = \{ 0, 5 \}$. Koset dari K dibawa ke elemen dari peta f yaitu 10 elemen Z_{10} dibawa dalam 2 ke 1 cara ke 5 elemen peta f.

$\{ 0 , 5 \} \to 0,$
$\{ 1 , 6 \} \to 8,$
$\{ 2 , 7 \} \to 6,$
$\{ 3 , 8 \} \to 4,$
$\{ 4 , 9 \} \to 2.$

Teorema VII.5

Misalkan $f: G \to H$ homomorfisma grup dengan inti Ker(f) dan peta $f(G)$.
Sifat-sifat berikut ini berlaku :

1. Fungsi f injektif jika dan hanya jika Ker(f) = { 0 }.
2. Jika f injektif maka G isomorfis dengan $f(G)$.

Bukti :

(1) $\Rightarrow$
Misalkan $x \neq e$. Karena f injektif maka $f(x) \neq f(e) = e'$.
Berarti $x \notin \text{Ker}(f)$.
Oleh karena itu Ker(f) = { e }.
$\Leftarrow$
Misalkan $f(a)$ sebarang elemen $f(G)$.
Koset kiri $a\,K = a\,\{ e \} = \{ a \}$ mengandung satu dan hanya satu elemen G yang dibawa oleh f ke $f(a)$.
Berarti f injektif.

(2) Misalkan $h : G \to f(G)$ dengan $h(a) = f(a)$ untuk a dalam G.

Karena f injektif maka h injektif dan jelas bahwa h surjektif sehingga h isomorfisma. Akibatnya G isomorfis dengan $f(G)$.

Contoh VII.9 :

Didefinisikan pemetaan $f : \boldsymbol{Z} \to \boldsymbol{Z}$ dengan aturan $f(x) = 3x$.
Karena $f(x + y) = 3(x + y) = 3x + 3y = f(x) + f(y)$ maka f homomorfisma.
Penyelesaian persamaan $3x = 0$ adalah $x = 0$ sehingga $\text{Ker}(f) = \{ 0 \}$ atau f injektif.
Dengan menggunakan Teorema VII.5 maka $\boldsymbol{Z}$ isomorfis dengan

$$\text{Im}(f) = \{ 3x \mid x \text{ dalam } \boldsymbol{Z} \} = (3)$$

yang merupakan grup bagian sejati dari Z.

Contoh VII.10

Misalkan diketahui $\boldsymbol{R}$ himpunan bilangan real dan $\boldsymbol{R}^*=\boldsymbol{R}-\{0\}$. Didefinisikan $f : \boldsymbol{R}^* \to \boldsymbol{R}^*$ dengan $f(x) = x^2$. Buktikan f homomorfisma tetapi f tidak injektif.

Jawab :

Berdasarkan Contoh VII.4, dengan mengingat $\boldsymbol{R}^*$ grup terhadap operasi perkalian maka f homomorfisma tetapi

$$\text{Ker}(f) = \{ x \in \text{R}^* \mid f(x) = x^2 = 1 \} = \{ 1, -1 \} \neq \{ 1 \}$$

sehingga f tidak injektif.

Latihan

1. Tentukan fungsi ini homomorfisma atau bukan.
   a. $f : \boldsymbol{Z} \to \boldsymbol{R}^*$ dengan $f(k) = 2^k$.
   b. $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = x^2$.
   c. $f : Z_6 \to Z_2$ dengan $f(k.\,1) = k.\,1$.
2. Jika pada soal nomor 1 di atas homomorfisma maka tentukan peta dan intinya.
3. Jika G dan H sebarang grup dan $f : G \to H$ dengan $f(x) = e$ untuk semua x dalam G maka buktikan bahwa f homomorfisma.
4. Misalkan $f : \boldsymbol{R}^* \to \boldsymbol{R}^*$ dengan $f(x) = x^{-3}$.
   a. Tunjukkan bahwa f homomorfisma.
   b. Tunjukkan f injektif dengan menguji Ker(f).
5. Diketahui bahwa $f : G \to H$ dan $h : H \to K$ homomorfisma.
   a. Buktikan bahwa $f\,h$ homomorfisma.
   b. Gunakan uji inti (*kernel*) untuk membuktikan bahwa jika f dan h injektif maka $f\,h$ juga injektif.
6. Diketahui $f : G \to H$ homomorfisma grup dengan image $f(G)$. Buktikan bahwa jika G abelian maka $f(G)$ abelian.
7. Diketahui $f : \boldsymbol{C}^* \to M_{2\times 2}$ dengan $f(a + b\,i) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.
   Tunjukkan bahwa f mengawetkan operasi.
8. Diketahui $f : \boldsymbol{R} \to \boldsymbol{R}^+$ dengan $f(x) = 2^{-x}$. Tunjukkan bahwa f homomorfisma yang injektif dengan uji inti.
9. Diketahui $Z_4 = \{ 0, 1, 2, 3 \}$ dan $f : Z_4 \to Z_4$ dengan $f(x) = 2x$. Apakah f homomorfisma bijektif ?
10. Diketahui $Z_4 = \{ 0, 1, 2, 3 \}$ dan $f : Z_4 \to Z_4$ dengan $f(x) = 2x + 3$. Apakah f homomorfisma bijektif ?
11. Diketahui $Z_3^* = \{ 1, 2 \}$ dan $f : Z_3^* \to Z_3^*$ dengan $f(x) = x^2$. Apakah f homomorfisma bijektif ?

12. Diketahui Z_3^* = { 1, 2 } dan f : $Z_3^* \to Z_3^*$ dengan $f(x) = x^3$. Apakah f homomorfisma bijektif ?
13. Diketahui $\boldsymbol{C}^*$ adalah himpunan bilangan kompleks tidak nol dan f : $\boldsymbol{C}^* \to \boldsymbol{C}^*$ dengan $f(x) = x^5$. Apakah f homomorfisma bijektif ?
14. Apakah Z_8^* isomorfis dengan Z_{10}^* ?
15. Apakah Z_8^* isomorfis dengan Z_{12}^* ?

***

BAB VIII
GRUP NORMAL

Inti dari sebarang homomorfisma grup mempunyai sifat tambahan yaitu mengandung semua konjugat (*conjugates*) dari elemennya.

Definisi VIII.1

Grup bagian S dari grup G dikatakan grup bagian normal (*normal subgroup*) asalkan untuk setiap elemen s dalam S dan setiap $a \in G$ berlaku bahwa $a^{-1} s\, a \in S$.

Istilah S grup bagian normal dari grup G sering kali disingkat sebagai S normal dari G. Berikut ini sifat-sifat tentang normal dari suatu grup.

Teorema VIII.1

1. Untuk sebarang grup G berlaku bahwa { 0 } dan G merupakan normal dalam G.
2. Jika G abelian maka setiap grup bagian dari G normal dalam G.
3. Grup bagian S normal dalam G jika dan hanya jika $aS = Sa$ untuk semua $a \in G$.
4. Grup bagian S normal dalam G jika hanya jika $a^{-1}Sa = S$ untuk semua $a \in G$.
5. Jika S normal dalam G dan T sebarang grup bagian dari G maka
   $$ST = \{ st \mid s \in S \text{ dan } t \in T \}$$
   grup bagian dari G.

Bukti :

(1) & (2) untuk latihan.

(3) $\Rightarrow$

Misalkan a dalam G dan s dalam S.

Karena S normal dari S maka $a^{-1}sa = s'$ dalam S dan didapat $sa = as'$.

Hal ini menunjukkan bahwa sebarang elemen sa dari koset kanan Sa berbentuk as' dan berarti terkandung dalam aS atau $Sa \subseteq aS$.

Dengan cara yang sama $a\ s\ a^{-1} = (a^{-1})^{-1}$ s $a^{-1} = s''$ sehingga $as = s''\ a$ untuk sebarang as dalam aS dan akibatnya $aS \subseteq Sa$.

Terbukti $aS = Sa$.

$\Leftarrow$

Untuk latihan.

(4) Sifat ini merupakan akibat langsung dari sifat (3).

(5) (a) NT mempunyai identitas berbentuk ee.

(b) Misalkan $n_1\ t_1$ dan $n_2\ t_2$ dalam NT.

Maka

$(n_1\ t_1)\ (n_2\ t_2) = n_1\ (t_1\ n_2)\ t_2 = n_1\ (n_3\ t_1)\ t_2 = (n_1\ n_3)\ (t_1\ t_2)$

yang masih dalam NT dan berarti NT tertutup.

(c) Jika nt dalam NT maka inversnya $t^{-1}\ n^{-1}$ dapat dinyatakan sebagai $n_4\ t^{-1}$ yang merupakan elemen NT.

Teorema VIII.2 :

Jika $f: G \to H$ homomorfisma grup maka inti Ker(f) normal dalam G.

Bukti :

Misalkan $x \in$ Ker(f) dan $a \in G$.

Akan ditunjukkan bahwa $a^{-1}\ xa$ dalam Ker(f).

$f(a^{-1}xa) = f(a^{-1})\ f(x)\ f(a) = f(a^{-1})\ e'\ f(a) = f(a^{-1}a) = f(e) = e'$.

Berarti $a^{-1}\ xa$ dalam Ker(f).

Contoh VIII.1

Himpunan $Z_4 = \{ 0, 1, 2, 3 \}$ merupakan grup terhadap operasi penjumlahan modulo 4. Karena Z_4 grup Abelian maka setiap grup bagiannya merupakan (grup bagian) normal dalam Z_4. Hal itu berarti, grup bagian dari Z_4 yaitu $\{ 0 \}$, $\{ 0, 2\}$ dan Z_4 normal dalam Z_4.

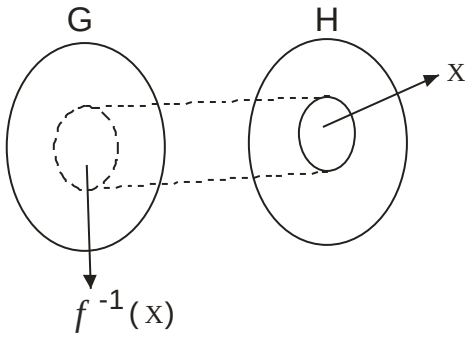
Contoh VIII.2

Himpunan Z_5^* = { 1, 2, 3, 4 } merupakan grup terhadap operasi perkalian modulo 5. Karena Z_5^* grup Abelian maka setiap grup bagiannya merupakan (grup bagian) normal dalam Z_5^*. Hal itu berarti, grup bagian dari Z_5^* yaitu { 1 }, { 1, 4} dan Z_5^* normal dalam Z_5^*.

Definisi VIII.2 :

Misalkan $f : G \to H$ sebarang fungsi dan X sebarang himpunan bagian dari H. Prapeta (*invers image*) X di bawah f yang dilambangkan dengan $f^{-1}(X)$ didefinisikan sebagai :

$$f^{-1}(X) = \{ g \in G \mid f(g) \in X \}.$$



Contoh VIII.3

Diketahui Z_5^* = { 1, 2, 3, 4 } merupakan grup terhadap operasi perkalian modulo 5. Didefinisikan $f : Z_5^* \to Z_5^*$ dengan $f(x) = x^2$ sehingga f homomorfisma grup. Ker(f) = { 1, 4 } merupakan normal dalam G.

Contoh VIII.4

Diketahui $M_{2\times 2}{}^*(R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in R \,\&\, ad - bc \neq 0 \right\}$ merupakan grup terhadap operasi perkalian matriks ordo 2 × 2.

Didefinisikan $f: M_{2\times 2}{}^*(R) \rightarrow R^*$ dengan $f(A) = \det(A)$ sehingga f homomorfisma grup. Ker(f)= $\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | a,b,c,d \in R \,\&\, ad-bc=1\right\}$ merupakan normal dalam $M_{2\times 2}{}^*(R)$.

Teorema VIII.3

Misalkan $f: G \rightarrow H$ homomorfisma. Sifat – sifat berikut ini berlaku :

1. Jika S grup bagian dari H maka $f^{-1}(S)$ grup bagian dari G.
2. Jika N grup bagian normal dari H maka $f^{-1}(N)$ normal dari G.
3. Jika S grup bagian dari peta $f(G)$ dan orde dari G berhingga maka orde dari sama dengan $|K|\ |S|$ dengan K inti dari f.

Bukti:

(1) Karena $f(e) = e'$ dengan e' dalam S maka elemen dentitas e berada dalam $f^{-1}(S)$.
Misalkan x, y dalam $f^{-1}(S)$.
Karena $f(xy) = f(x)\, f(y) = s'\, s''$ untuk suatu s', s'' dalam S dan S tertutup maka $f(xy)$ dalam S.
Akibatnya xy dalam $f^{-1}(S)$.
Misalkan x^{-1} adalah invers dari x dengan x dalam $f^{-1}(S)$.

(2) Akan dibuktikan bahwa $f^{-1}(N)$ tertutup di bawah operasi konjugat dari elemennya.
Ambil sebarang x dalam $f^{-1}(N)$ dan a dalam G.
Karena x dalam $f^{-1}(N)$ maka $f(x)$ dalam N sehingga
$$f(a^{-1} xa) = f(a^{-1})\, f(x)\, f(a) = (\, f(a)\,)^{-1}\, f(x)\, f(a).$$
Karena N normal dalam $f(G)$ maka $(\, f(a)\,)^{-1}\, f(x)\, f(a)$ dalam $f(G)$ dan akibatnya $a^{-1} xa$ dalam $f^{-1}(N)$.
Berarti $f^{-1}(N)$ tertutup terhadap operasi konjugat.

(3) Untuk setiap s dalam S dapat dinyatakan $s = f(x)$ untuk suatu x dalam G karena $s \subseteq f(G)$.

Contoh VIII.6

Diketahui $M_{2\times 2}{}^*(R)=\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} | a,b,c,d \in R \,\&\, ad-bc \neq 0\right\}$ merupakan grup terhadap operasi perkalian matriks ordo 2 × 2.

Didefinisikan f : $M_{2\times 2}{}^*(R) \rightarrow R^*$ dengan $f(A)$ = det(A) sehingga f homomorfisma grup. Karena N = { 1, -1 } grup bagian dari R^* dan grup komutatif terhadap operasi perkalian maka N normal dalam R^*. Akibatnya, berdasarkan Teorema VIII.3, maka $f^{-1}(N)$ normal dalam $M_{2\times 2}{}^*(R)$. Demikian juga, Q^* normal dalam R^* sehingga $f^{-1}(Q^*)$ normal dalam $M_{2\times 2}{}^*(R)$.

Latihan

1. Berikan contoh bahwa untuk S dan T grup bagian dari grup G maka ST tidak perlu grup bagian dari G.
2. Buktikan bahwa jika S dan T normal dalam G maka ST juga normal dalam G.
3. Diketahui bahwa $f : G \to H$ homomorfisma grup.
   Buktikan bahwa jika N normal dalam G maka
   $$f(N) = \{ f(n) \mid n \text{ dalam } N \}$$
   grup bagian normal dari $\text{Im}(f) = f(G)$.
4. Misalkan H grup bagian normal dari G. Jika H dan G/H abelian maka apakah G harus abelian.
5. Jika H normal dari grup G maka buktikan bahwa
   $$C(H) = \{ x \in G \mid xH = Hx \}$$
   merupakan grup bagian normal dari G.
6. Tunjukkan bahwa
   $$H = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$
   adalah grup bagian normal dari grup matriks-matriks orde 2 yang mempunyai invers terhadap operasi perkalian matriks $M_{2\times 2}(R)^*$.
7. Berikan contoh 2 grup orde 6 yang tidak saling isomorfis.
8. Diketahui Z_6 grup terhadap operasi penjumlahan modulo 6. Sebutkan grup bagian dari Z_6. Apakah grup bagian tersebut normal ?
9. Diketahui Z_8^* grup terhadap operasi perkalian modulo 8. Sebutkan grup bagian dari Z_8^*. Apakah grup bagian tersebut normal ?
10. Diketahui Z_{10}^* grup terhadap operasi perkalian modulo 10. Sebutkan grup bagian dari Z_{10}^*. Apakah grup bagian tersebut normal ?

***

BAB IX
GRUP FAKTOR

Koset aS dapat digunakan untuk membentuk sistim aljabar yang baru. Misalkan S grup bagian dari grup G. Dapat dibentuk himpunan semua koset kiri dari S yaitu

$$\{ aS \mid a \text{ dalam } G \}.$$

Elemen G yang berbeda dapat saja membentuk koset yang sama. Untuk itu diperlukan cara untuk menguji kesamaan dari dua koset.

Teorema IX.1

1. Koset aS dan bS sama jika dan hanya jika $b^{-1}a \in S$.
2. $aS = S$ jika hanya jika $a \in S$.

Bukti :

1. $\Rightarrow$

   Jika diketahui $aS = bS$ maka $a = ae = bs$ untuk suatu s dalam S.

   Dengan kedua ruas dengan b^{-1} maka dapat $b^{-1}a = s$ yang berada dalam S.

   $\Leftarrow$

   Diketahui $b^{-1}a$ dalam S.

   Tulis $b^{-1}a \in S$.

   Didapat $a = bs$ atau $b = as^{-1}$

   Hal ini berarti, sebarang perkalian as' haruslah sama dengan $(bs)s' = b(ss)'$ dan sebarang perkalian $bs'' = (as^{-1})s'' = a(s^{-1}s'')$.

   Oleh karena itu dengan sifat ketertutupan S, sebarang as' sama dengan b dikalikan dengan suatu elemen S dan sebarang bs'' sama dengan a dikalikan dengan sebarang elemen S.

   Akibatnya $aS \subseteq bS$ dan $bS \subseteq aS$.

   Berarti $aS = bS$.

2. Karena $eS = S$ maka dengan menggunakan sifat (1) di atas didapat bahwa $eS = S$ jika hanya jika a dalam S.

Definisi IX.1

Aturan * dikatakan terdefinisikan dengan baik (*well-defined*) jika $a = a'$ dan $b = b'$ maka berakibat $a*b = a'*b'$.

Contoh IX.1

Diketahui himpunan bilangan rasional $\boldsymbol{Q}$ dan didefinisikan aturan pada $\boldsymbol{Q}$ dengan

$$a/b \oplus c/d = (a+c) / (b+d)$$

$a/b, c/d$ dalam $\boldsymbol{Q}$.

Karena pada satu sisi $1/2 = 3/6$ dan pada sisi lain

$$1/2 \oplus 1/3 = (1+1) / (2+3) = 2/5$$
$$3/6 \oplus 1/3 = (3+1) / (6+3) = 4/9$$

maka $\oplus$ tidak terdefinisikan dengan baik.

Teorema IX.2

Perkalian koset $aS \,.\, bS = abS$ terdefinisikan dengan baik jika dan hanya jika S grup bagian normal dari grup G.

Bukti :

$\Rightarrow$

Diketahui $aS \,.\, bS = abS$ terdefinisikan dengan baik.

Untuk sebarang s dalam S berlaku $eS = sS$ dan akibatnya, untuk semua b dalam G berlaku

$$sS \,.\, bS = eS \,.\, bS$$

atau

$$sbS = ebS$$

sehingga $sbS = bS$.

Dengan menggunakan Teorema IX.1 diperoleh b^{-1} (sb) dalam S atau $b^{-1}s\,b$ dalam S.

Berarti S grup bagian normal.

$\Leftarrow$

Diketahui S normal dalam G.

Misalkan $a_1S = aS$.

Akan ditunjukkan bahwa untuk sebarang bS berlaku

$a_1S \,.\, bS = aS \,.\, aS$ atau $a_1bS = abS$.

Hal ini benar asalkan $(ab)^{-1}(a_1b)$ dalam S.

Karena $(ab)^{-1}(a_1b) = (b^{-1}a^{-1})(a_1b) = b^{-1}(a^{-1}a_1)b = b^{-1} \,.\, s \,.\, b$ maka $b^{-1}\, s\, b$ dalam S (karena S normal).

Dengan cara yang sama, hal di atas dapat dikerjakan juga bila bS diganti dengan b_1S.

Jadi, bila $a_1S = aS$ maka $a_1Sb_1S = aSbS$.

Definisi IX.2

Misalkan S grup bagian normal dari grup G.

Himpunan G/S yang dibaca "G mod S" didefinisikan dengan:

$$G/S = \{\, a\, S \mid a \in G \,\}$$

dengan operasinya mempunyai aturan $aS\, bS = ab\, S$.

Teorema IX.3

Sistim G/S yang merupakan grup.

Bukti:

1. Akan dibuktikan bahwa operasi perkalian dalam G/S bersifat tertutup.
   Ambil sebarang x, y dalam G/S.
   Karena $x\, y = (aS)\ (bS) = ab\, S$ dengan ab dalam G.
   Berarti $x\, y$ dalam G/S.
2. Akan dibuktikan bahwa dalam G/S berlaku sifat assosiatif.
   Ambil x, y, z dalam G/S.
   Karena x, y, z dalam G/S maka $x = aS$, $y = bS$ dan $z = cS$ untuk suatu $a, b, c \in S$.

$$\begin{aligned}(x\, y)z &= (aSbS)cS \\ &= (ab\, S)\ cS \\ &= (ab)c\, S \\ &= a(bc)\, S \\ &= aS\ (bc\, S)\end{aligned}$$

$= aS\ (bS\ cS)$

$= x(yz)$.

Berarti dalam G/S berlaku sifat assosiatif.

3. Akan dibuktikan bahwa dalam G/S terdapat elemen identitas.
   Elemen G/S yaitu $eS = S$ merupakan identitas dalam G/S karena untuk sebarang aS dalam G/S berlaku

   $aS\ cS = ae\ S = aS$

   $eS\ aS = ea\ S = aS$

   Berarti $eS = S$ merupakan identitas dalam G/S.

4. Akan dibuktikan bahwa untuk setiap elemen G/S mempunyai invers dalam G/S.
   Ambil sebarang aS dalam G/S.
   Karena a dalam grup G maka terdapat a^{-1} dalam G sehingga $a\ a^{-1} = a^{-1}\ a = e$ sehingga $(aS)\ (a^{-1}\ S) = (a\ a^{-1})S = eS = S$ dan

   $(a^{-1}S)(aS) = eS = S$.

   Berarti $a^{-1}\ S$ merupakan invers dari aS.
   Terbukti bahwa G/S merupakan grup.

Karena G/S merupakan grup maka grup G/S sering dinamakan *grup faktor (factor group)*. Jika G grup terhadap penjumlahan maka kosetnya ditulis dengan $a + S$, $b + S$,...dan operasi dalam G/S adalah

$$(a + S) + (b + S) = (a + S) + S.$$

Dalam grup G/S elemen identitasnya adalah $0 + S$ dan invers dari $a + S$ adalah $-a + S$.

Contoh IX.2:

Diketahui himpunan bilangan bulat $\boldsymbol{Z}$ grup dan

$$(6) = \{..., -12, -6, 0, 6, 12,...\}$$

grup bagian dari $\boldsymbol{Z}$.
Akan ditunjukkan bahwab Z_6 isomorfis dengan $\boldsymbol{Z}/(6)$.
Grup faktor $\boldsymbol{Z}/(6) = \{0 + (6), 1 + (6), 2 + (6), 3 + (6), 4 + (6), 5 + (6)\}$.
Didefinisikan fungsi $f : G \rightarrow \boldsymbol{Z}/(6)$ dengan $f(a + (6)) = a$ dengan $0 \leq a < 5$.
Dapat dibuktikan bahwa fungsi f merupakan isomorfisma.

Contoh IX.3 :

Diketahui $Z_8^* = \{ 1, 3, 5, 7 \}$. Didefinisikan pemetaan $f : Z_8^* \to Z_8^*$ dengan $f(x) = x^2$. Berarti $f(1) = f(3) = f(5) = f(7) = 1$. Mudah dibuktikan bahwa f automorfisma. Pemetaan f tidak injektif dan tidak surjektif. $\text{Im}(f) = \{ 1 \}$ dan $\text{Ker}(f) = Z_8^*$.
Grup faktor $Z_8^*/K = \{ aK \mid a \in Z_8^* \} = \{ K \} = \{ Z_8^* \} = \{ \{1, 3, 5, 7\} \}$ sehingga grup faktor tersebut hanya mempunyai 1 elemen atau mempunyai orde 1.

Contoh IX.4

Diketahui $Z_{10}^* = \{ 1, 3, 7, 9 \}$. Didefinisikan pemetaan $f : Z_{10}^* \to Z_{10}^*$ dengan $f(x) = x^2$. Berarti $f(1) = f(9) = 1$, $f(7) = 9 = f(3)$. Mudah dibuktikan bahwa f automorfisma. Pemetaan f tidak injektif dan tidak surjektif. $\text{Im}(f) = \{ 1, 9 \}$ dan $K = \text{Ker}(f) = \{ 1, 9\}$.
Grup faktor $Z_{10}^*/K = \{ aK \mid a \in Z_{10}^* \} = \{ 1K, 3K \} = \{ \{1, 9\}, \{ 3, 7\} \}$. Dalam grup faktor ini mempunyai orde 2 dan K berfungsi sebagai elemen identitas sedangkan elemen lainnya adalah $3K$ yang mempunyai orde 2 sehingga merupakan grup siklik.

Contoh IX.5

Diketahui $Z_{10}^* = \{ 1, 3, 7, 9 \}$. Didefinisikan pemetaan $f : Z_{10}^* \to Z_{10}^*$ dengan $f(x) = x^3$. Berarti $f(1) = 1, f(3) = 7, f(7) = 3, f(9) = 9$. Mudah dibuktikan bahwa f automorfisma. Demikian juga pemetaan f bijektif . $\text{Im}(f) = \{ 1, 3, 7, 9 \} = Z_{10}^*$ dan $K = \text{Ker}(f) = \{ 1\}$.
Grup faktor
$Z_{10}^*/K = \{ a\text{K} \mid a \in Z_{10}^* \} = \{ 1K, 3K, 7K, 9K\} = \{ \{1\}, \{3\}, \{7\}, \{9\} \}$. Dalam grup faktor ini mempunyai orde 4, K berfungsi sebagai elemen identitas. Elemen $9K$ mempunyai orde 2. Elemen $3K$ dan $7K$ mempunyai orde 4 sehingga merupakan Z_{10}^*/K grup siklik.

Teorema IX.4

Untuk sebarang integer positif n berlaku $(aS)^n = a^n S$.

Bukti :

Akan dibuktikan dengan prinsip induksi.
Untuk $n = 1$, berlaku $(aS)^1 = a^1 S$.
Berarti teorema benar untuk $n = 1$.
Dianggap bahwa teorema benar untuk $n = k$. Berarti $(aS)^k = a^k S$.
Untuk $n = k + 1$, berlaku

$$\begin{aligned}(aS)^{k+1} &= (aS)\,(aS)^k \\ &= (aS)\,(a^k S) \\ &= (a \,.\, a^k)S \\ &= a^{k+1} S.\end{aligned}$$

Terbukti bahwa teorema benar untuk semua bilangan bulat positif n.

Teorema IX.5

Misalkan G/S sebarang grup faktor.

1. Jika G berhingga maka orde G/S sama dengan $|G| \,/\, |S|$.
2. Jika G siklik maka G/S siklik.
3. Jika a mempunyai orde berhingga maka orde dari aS dalam G/S membagi orde dari a.
4. Jika G abelian maka G/S abelian.

Bukti :

1. Dengan menggunakan Teorema Lagrange (untuk latihan).
2. Misalkan G siklik dengan $G = (a) = \{ a^k \mid k \text{ dalam } \boldsymbol{Z} \}$.
   Hal itu berarti G/S dibangun oleh suatu aS elemen dalam G/S karena untuk sebarang xS dalam G/S berlaku $x = a^m$ untuk suatu bilangan bulat m.
   Oleh karena itu $xS = a^m S = (aS)^m$.
   Terbukti G/S dibangun oleh suatu elemen dalam G/S atau G/S siklik.
3. Misalkan a mempunyai orde berhingga k dalam G.

Sehingga $a^k = e$ dan akibatnya $(aS)^k = a^k S = eS$ yaitu identitas dalam G/S.
Oleh karena itu dengan Teorema IV.6, orde dari aS membagi k.

4. Ambil sebarang aS, bS dalam G/S.
   Telah dibuktikan bahwa G/S grup jika G grup.
   Karena G abelian maka $aS\ bS = ab\ S = bS\ aS$.
   Berarti G/S grup abelian.

Teorema berikut tidaklah sulit untuk dibuktikan dan sangat penting dalam pembuktian teorema fundamental homomorfisma grup.

Teorema IX.6

Misalkan G/S sebarang grup faktor. Fungsi $f : G \to G/S$ yang didefinisikan dengan aturan $f(x) = xS$ merupakan homomorfisma surjektif dari G ke G/S dengan intinya S.

Pemetaan S yang didefinisikan dalam teorema di atas sering dikenal dengan nama homomorfisma alam (*natural homomorphism*) atau homomorfisma kanonik (*canonical homomorphism*).

Teorema IX.7

Jika G/S siklik dan setiap elemen S komutatif dengan semua elemen G maka G abelian.

Bukti :

Karena G/S siklik maka $G/S = (aS) = \{ (aS)^k \mid \text{dalam } Z \}$ untuk suatu koset aS.
Karena $(aS)^k = a^k S$ maka setiap koset kiri S berbentuk a^kS.
Ambil sebarang x dan y dalam G.
Misalkan masing–masing berada dalam suatu koset, misal x dalam a^mS dan y dalam a^nS untuk suatu bilangan bulat m dan n.
Akibatnya $x = a^m s_1$ dan $y = a^n s_2$ untuk suatu s_1, s_2 dalam S.

$$xy = (a^m s_1)\ (a^n s_2) = a^m\ a^n\ s_1\ s_2$$

$= a^n\ a^m\ s_1 s_2$
$= (a^n\ s_2)\ (a^m\ s_1)$
$= yx$.

Terbukti bahwa G abelian.

Teorema IX.8 (*Teorema Fundamental dari Homomorfisma Grup*).

Jika $f : G \to H$ homomorfisma grup dengan inti K dan peta $f(G)$ maka G/S isomorfis dengan $f(G)$.

Bukti :

Definisikan fungsi $g : G/K \to f(G)$ dengan $g(aK) = f(a)$.
Telah dibuktikan bahwa g bijektif sehingga tinggal membuktikan bahwa g homomorfisma.
Pada satu sisi,

$$g(aK\ bK) = g(abK) = f\ (ab) = f(a)\ f(b)$$

dan pada sisi lain,

$$g(aK)\ g(bK) = f(a)\ .\ f(b)$$

sehingga $g(aK\ bK) = g(aK)\ g(bK)$ untuk semua koset aK dan bK.

Contoh IX.6 :

Misalkan $T = \{\ x$ dalam $\boldsymbol{C}^* \mid \text{Abs}(x) = 1\ \}$.
Mudah dibuktikan bahwa fungsi Abs : $\boldsymbol{C}^* \to \boldsymbol{R}^*$ merupakan homomorfisma.
Karena 1 identitas dalam $\boldsymbol{R}^*$ dan T = Ker(Abs) maka dengan menggunakan teorema fundamental homomorfisma diperoleh bahwa $\boldsymbol{C}^*/T$ isomorfis dengan peta dari fungsi Abs yaitu R^+.
Oleh karena itu $\boldsymbol{C}^*/T \cong R^+$ sehingga $\boldsymbol{C}^*/T$ juga mempunyai sifat-sifat yang dimiliki R^+.
Jadi $\boldsymbol{R}^+$ grup abelian tidak siklik, ordenya tak hingga dan mempunyai elemen dengan orde 1 atau ∞.

Isomorfisma

Suatu grup yang nampaknya berbeda secara esensi dapat sama. Secara intuisi ide bahwa dua grup secara esensi sama akan menuju pada pemikiran tentang konsep isomorfisma.

Definisi IX.3

Misalkan $< G, * >$ dan $< H, . >$ grup. Grup G isomorfis dengan H jika terdapat fungsi $f : G \to H$ sehingga

1. f injektif,
2. f surjektif,
3. f homomorfisma

maka f dikatakan *isomorfisma*.

Teorema IX.9

Misalkan grup G dan H isomorfis. Sifat-sifat berikut ini berlaku :

1. Grup G dan H mempunyai orde yang sama.
2. Grup G dan H keduanya abelian atau tidak abelian.
3. Grup G dan H keduanya siklik atau tidak siklik.

Bukti :

Untuk latihan.

Contoh IX.7:

Diketahui Grup Z_4 dan Z_8*.
Kedua grup mempunyai orde 4 dan abelian tetapi Z_4 = (1) siklik sedangkan Z_8* tidak siklik karena tidak ada elemennya yang mempunyai orde 4.
Oleh karena itu Z_4 tidak isomorfis dengan Z_8*.

Teorema IX.10

1. Sebarang grup siklik tak berhingga isomorfis dengan $\boldsymbol{Z}$.
2. Sebarang grup siklik berhingga orde n isomorfis dengan Z_n.

Bukti :

Dalam setiap kasus, didefinisikan suatu fungsi yang diduga merupakan suatu fungsi yang isomorfisma, kemudian ditunjukkan bahwa fungsi tersebut injektif, surjektif dan mengawetkan operasi.

1. Misalkan G sebarang grup siklik tak hingga.
   Karena G siklik maka $G = (a) = \{ a^k \mid k \text{ dalam } Z \}$. Bentuk himpunan ini menyarankan untuk mendefinisikan suatu fungsi yang sesuai.
   Misalkan $f : G \rightarrow H$ dengan $f(x) = a^x$.
   Andaikan $a^x = a^y$.
   Dengan mengalikan kedua ruas dengan a^{-x} didapat $e = a^{x+y}$.
   Karena $y > x$ maka berarti terdapat pangkat positif dari a yang sama dengan identitas e.
   Hal ini kontradiksi dengan kenyataan bahwa a mempunyai orde tak hingga.
   Untuk sifat f surjektif dan mengawetkan operasi digunakan sebagai latihan.
2. Misalkan dipunyai grup siklik berhingga dengan orde n yaitu
   $$G = (b) = \{ b^1, b^2, b^3, \ldots, b^n = e \}.$$
   Dengan mendefinisikan $f : \boldsymbol{Z} \rightarrow G$ dengan aturan $f(k. 1) = b^k$ dengan k bilangan bulat antara 0 dan n-1 maka dapat dibuktikan bahwa f isomorfisma.

Latihan

1. Misalkan S = { (1), (2) } dan anggap bahwa semua koset aS untuk a dalam Z_4.
   Berikan contoh khusus untuk menunjukkan bahwa perkalian koset $aS \,.\, bS = ab\,S$ tidak terdefinisikan dengan baik.
2. Tunjukkan bahwa tidak ada dua dari himpunana-himpunan ini yang isomorfis : $\boldsymbol{R}^*$, $\boldsymbol{R}^+$ dan $\boldsymbol{C}^*$.
3. Bukti bahwa fungsi-fungsi berikut suatu isomorfisma.
   a. $f : Z_{100} \to Z_{100}$ dengan $f(x) = 3x$.
   b. $h : Z_{10}^* \to Z_{10}^*$ dengan $h(\mathrm{x}) = x^3$.
4. Tunjukkan bahwa fungsi berikut mengawetkan operasi tetapi tidak surjektif maupun injektif.
   a. $f : Z_{100} \to Z_{100}$ dengan $f(x) = 2x$.
   b. $h : Z_{10}^* \to Z_{10}^*$ dengan $h(x) = x^2$.
5. Didefinisikan $f : \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = -3x$. Buktikan bahwa f suatu automorfisma R yaitu isomorfisma dari $\boldsymbol{R}$ ke $\boldsymbol{R}$.
6. Misalkan G sebarang grup dan b elemen G.
   Didefinisikan $f_b : G \to G$ dengan aturan $f_b(x) = b^{-1}\, x\, b$.
   Tunjukkan bahwa f_b suatu automorfisma dari G.
7. Buktikan bahwa suatu grup G isomorfis dengan dirinya sendiri.
8. Diketahui grup faktor Z_6/S dengan S = { 0, 3 }. Tentukan orde dari grup faktor dan orde dari elemen-elemen dalam Z_6/S. Apakah Z_6/S siklik ?
9. Diketahui grup faktor Z_6/S dengan S = { 0, 2, 4 }. Tentukan orde dari grup faktor dan orde dari elemen-elemen dalam Z_6/S. Apakah Z_6/S siklik ?
10. Pilihlah S grup bagian sejati dalam Z_8^*. Tentukan orde dari grup faktor dan orde dari elemen-elemen dalam Z_8^*/S. Apakah Z_8^*/S siklik ?
11. Pilihlah S grup bagian sejati dalam Z_{10}^*. Tentukan orde dari grup faktor dan orde dari elemen-elemen dalam Z_{10}^*/S. Apakah Z_{10}^*/S siklik ?

12. Pilihlah S grup bagian sejati dalam Z_7^*. Tentukan orde dari grup faktor dan orde dari elemen-elemen dalam Z_7^*/S. Apakah Z_7^*/S siklik ?
13. Diketahui grup faktor $f : Z_7^* \rightarrow Z_7^*$ dengan $f(x) = x^2$. Tentukan Im(f) dan K=Ker(f). Apakah Z_7^*/K isomorfis dengan Im(f) ?
14. Diketahui grup faktor $f : Z_{10}^* \rightarrow Z_{10}^*$ dengan $f(x) = x^2$. Tentukan Im(f) dan K=Ker(f). Apakah Z_{10}^*/K isomorfis dengan Im(f) ?
15. Misalkan $S = \{ A \in M_{2\times 2}^* \mid \det(A) = 1 \}$. Buktikan bahwa S grup bagian normal dari $M_{2\times 2}^*$.

***

BAB X
HASIL KALI LANGSUNG GRUP

Dalam teori grup, terdapat cara untuk membangun grup yang lebih besar dari hasil kali langsung (*direct product*) grup-grup yang lebih kecil dan di samping itu sering juga diharapkan dapat memfaktorkan grup yang besar sebagai perkalian grup-grup yang kecil dan sederhana.

Definisi X.1:

Misalkan G dan H grup. Hasil kali langsung $G \times H$ adalah sistim aljabar yang didefinisikan dengan himpunan

$$G \times H = \{ (g,h) \mid g \in G \text{ dan } h \in H \}$$

dan operasi * didefinisikan sebagai $(a,b) * (c,d) = (a*c , b*d)$.

Himpunan $G \times H$ dinamakan ***hasil kali Cartesian*** dari himpunan G dan H yang terdiri dari pasangan berurutan (g,h). Dalam hal ini, G dan H dinamakan *faktor* dari $G \times H$. Bidang Cartesian

$$\boldsymbol{R}^2 = \{ (x,y) \mid x, y \text{ dalam } R \}$$

merupakan salah satu contohnya dan dalam hal ini $\boldsymbol{R}^2 = \boldsymbol{R} \times \boldsymbol{R}$.

Teorema X.1

Jika G dan H grup maka $G \times H$ grup.

Bukti :

Tertutup
Ambil (g_1,h_1), (g_2,h_2) dalam $G \times H$.
Karena $(g_1,h_1) * (g_2,h_2) = (g_1g_2, h_1h_2)$ dengan g_1g_2 dalam G (karena G tertutup) dan h_1h_2 dalam H (karena H tertutup) maka perkaliannya masih dalam $G \times H$.
Hukum Assosiatif
Ambil (g_1,h_1), (g_2,h_2) dalam $G \times H$.

Karena $(g_1,h_1)^* (g_2,h_2) = (g_1 g_2 , h_1 h_2)$ dengan $g_1 g_2$ dalam G (karena G tertutup) dan $h_1 h_2$ dalam H (karena H tertutup) maka penggandaanya masih dalam $G \times H$.

Hukum Asosiasif

$$\begin{aligned}((t,u)^*(v,w)^*(x,y) &= (tv,uw)^*(x,y)\\ &= ((tv)x,(uw)y)\\ &= (\ t\ (vx)\ ,\ u\ (wy)\ )\\ &= (t,u)^*(vx,wy)\\ &= (\ t,u)^*((v,w)^*(x,y).\end{aligned}$$

Hukum Identitas

Dengan menduga (e,e) dengan e pertama dalam G dan e kedua dalam H sebagai identitas dari $G \times H$.

Karena $(x,y)\ ^*\ (e,e) = (xe,ye) = (x,y)$ dan $(e,e)\ ^*\ (x,y) = (ex,ey) = (x,y)$ maka berarti (e,e) identitas dalam $G \times H$ mempunyai invers.

Contoh X.1

Akan ditentukan sifat-sifat dari grup $Z_2 \times Z_4$.

Dengan menggunakan prinsip perkalian maka grup $Z_2 \times Z_4$ mempunyai orde 8.

Abelian?

Karena $(a,b) + (c,d) = (a+c,b+d)$ dan $(c,d) + (a,b) = (c+a,d+b)$ dan dengan mengingat Z_2 dan Z_4 abelian maka $Z_2 \times Z_4$ juga abelian.

Orde dari elemen

Untuk sebarang elemen $Z_2 \times Z_4$ mempunyai sifat $k.\ (a,b) = (k\ .\ a,\ k\ .\ b)$ dengan k dalam Z khususnya 4. $(a,b) = (4\ .\ a,\ 4\ .\ b) = (0,\ 0)$.

Oleh karena itu orde dari (a,b) merupakan pembagi 4.

Elemen (0, 0), (1, 2) dan (1, 1) berturut-turut mempunyai orde 1, 2, dan 4.

Siklik?

Karena grup mempunyai orde 8 dan tidak ada elemen $Z_2 \times Z_4$ yang mempunyai orde lebih dari 4 maka $Z_2 \times Z_4$ tidak siklik. ▪

Contoh X.2

Akan ditentukan sifat-sifat dari grup $Z_2 \times Z_2 \times Z_2 \times Z_2$.
Orde dari grup $Z_2 \times Z_2 \times Z_2 \times Z_2$ adalah 2 . 2 . 2 . 2 = 16. Grup ini merupakan grup abelian karena Z_2 abelian. Orde dari setiap elemen 1 atau 2 sebagai contoh (1, 0, 1, 1) mempunyai orde 2. Tidak ada elemen yang mempunyai orde 16. Hal itu berarti $Z_2 \times Z_2 \times Z_2 \times Z_2$ bukan grup siklik.

Contoh X.3

Akan ditentukan sifat-sifat dari grup $\boldsymbol{R}^* \times \boldsymbol{R}^*$.
Terdapat banyak cara untuk memilih (a,b) sehingga ordenya berhingga. Elemen a, b dalam $\boldsymbol{R}^*$ dapat mempunyai orde 1, 2 atau ∞. Jika mempunyai orde berhingga maka (a,b) mempunyai orde 1 atau 2 sedangkan jika salah satu dari a atau b mempunyai orde ∞ maka (a,b) mempunyai orde ∞. Hal itu berarti elemen-elemen dalam $\boldsymbol{R}^* \times \boldsymbol{R}^*$ mempunyai orde 1, 2 atau ∞.
Perlu dicatat bahwa $\boldsymbol{R}^*$ dan $\boldsymbol{R}^* \times \boldsymbol{R}^*$ keduanya mempunyai orde, keduanya abelian, keduanya tidak siklik, elemen-elemennya dapat mencapai orde 1, 2 atau ∞. Namun demikian, keduanya tidak isomorfis karena dalam $\boldsymbol{R}^*$ hanya -1 yang mempunyai orde 2 sedangkan dalam $\boldsymbol{R}^* \times \boldsymbol{R}^*$ ada 3 elemen yang mempunyai orde 2 yaitu (-1,1), (1, -1) dan (-1,-1).

Definisi X.1

Misalkan $G_1, G_2, \ldots, G_k$ grup. Hasil kali langsung $G_1 \times G_2 \times \ldots \times G_k$ adalah sistim aljabar yang didefinisikan dengan himpunan

$$\{ (g_1, g_2, \ldots, g_k) \mid g_j \in G_j \text{ untuk setiap } j \}$$

dan operasi * didefinisikan dengan

$$(g_1, g_2, \ldots, g_k) * (h_1, h_2, \ldots, h_k) = (g_1 * h_1, g_2 * h_2 \ldots, g_k * h_k).$$

Teorema X.2

Jika G_1, G_2, …., G_k grup maka $G_1 \times G_2 \times \ldots \times G_k$ grup.

Bukti :

Untuk latihan.

Berikut ini diberikan sifat-sifat tanpa bukti.

1. Jika setiap faktor G mempunyai orde berhingga maka orde dari $G_1 \times G_2 \times \ldots \times G_k$ sama dengan $|G_1| \, |G_2| \, \ldots \, |G_k|$.
2. $G_1 \times G_2 \times \ldots \times G_k$ abelian jika dan hanya jika G_j abelian.

Latihan

1. Jika G dan H sebarang grup maka buktikan bahwa $G \times H$ isomorfis dengan $H \times G$.
2. Jika G sebarang grup dan $\{ e \}$ grup dengan satu elemen maka $G \cong G \times \{ e \}$.
3. Jika $f : G \times H \to G$ dengan $f(x,y) = x$ maka buktikan f homomorfisma.
4. Misalkan G mengandung grup bagian sejati H dan K sehingga $G \cong H \times K$. Dengan memperhatikan syarat apa yang harus dipenuhi untuk H dan K, tunjukkan bahwa fungsi $P : G \to K$ yang didefinisikan dengan baik dan homomorfisma.
5. Jelaskan secara singkat sifat-sifat dari $Z_2 \times Z_2$.
6. Jelaskan secara singkat sifat-sifat dari $Z_3 \times Z_4$.
7. Jelaskan secara singkat sifat-sifat dari $Z_4^* \times Z_5^*$.
8. Buktikan bahwa $Z_8^* \cong Z_2 \times Z_2$.
9. Jelaskan secara singkat sifat-sifat dari $\boldsymbol{Q}^* \times \boldsymbol{Q}^*$.
10. Diketahui $(a_1, a_2, \ldots, a_k) \in G_1 \times G_2 \times \ldots \times G_k$. Buktikan dengan induksi bahwa untuk sebarang bilangan bulat positif m berlaku : $(a_1, a_2, \ldots, a_k)^m = (a_1^m, a_2^m, \ldots, a_k^m)$.
11. Jelaskan secara singkat sifat-sifat dari $\boldsymbol{R} \times Z_2$.
12. Apakah $Z_4^* \times Z_5^*$ isomorfis dengan Z_4 ?
13. Apakah $Z_4^* \times Z_3$ isomorfis dengan Z_6 ?
14. Jelaskan secara singkat sifat-sifat dari $\boldsymbol{Q} \times \boldsymbol{Q}$.
15. Jelaskan secara singkat sifat-sifat dari $\boldsymbol{R} \times \boldsymbol{R} \times \boldsymbol{R}$.

***

BAB XI
RING DAN RING BAGIAN

Dalam pembahasan tentang teori grup hanya digunakan satu operasi. Sistim bilangan yang telah dikenal seperti bilangan bulat, bilangan rasional dan bilangan kompleks mempunyai dua operasi yang didefinisikan padanya yaitu penjumlahan dan perkalian. Di bawah operasi perkalian himpunan bilangan-bilangan tersebut di atas merupakan grup abelian. Sistim aljabar dengan dua operasi seperti di atas termasuk dalam sistim aljabar yang dinamakan *ring*.

RING

Definisi XI.1

Ring adalah sistim aljabar yang terdiri dari himpunan elemen A dengan dua operasi yaitu penjumlahan (+) dan perkalian (.) dan memenuhi hukum-hukum.

(1) $< A , +>$ grup abelian

(2) terhadap operasi perkalian

(a) hukum *tertutup* : jika a, b dalam A maka ab dalam A.

(b) hukum *assosiatif* : $(ab)c = a(bc)$ untuk semua a, b dan c dalam A.

(c) hukum *distributif kanan* : $a(b + c) = ab + ac$ untuk semua a, b dan c dalam A.

(d) hukum *distributif kiri* : $(a + b)c = ac + bc$ untuk semua a, b dan c dalam A.

Dalam sebarang ring 0 merupakan identitas terhadap penjumlahan sedangkan $-a$ menyatakan invers a terhadap penjumlahan. Dalam sebarang ring A, pengurangan didefinisikan pada A dengan $a - b = a + (-b)$.

Contoh XI.1

Dapat dibuktikan bahwa himpunan A yang terdiri dari 2 elemen yaitu $\{ 0, a \}$ dengan operasi yang didefinisikan dengan

$$0 + 0 = a + a = 0,$$
$$0 + a = a + 0 = a,$$
$$0\ 0 = 0\ a = a\ 0 = 0,$$
$$a\ a = a,$$

merupakan ring. Sebagai contoh nyata $Z_2 = \{ 0, 1 \}$ dengan operasi penjumlahan dan perkalian modulo 2 merupakan himpunan yang mempunyai sifat tersebut.

Contoh XI.2

Dapat dibuktikan bahwa himpunan A yang terdiri dari 2 elemen yaitu $\{ 0, a \}$ dengan operasi yang didefinisikan dengan

$$0 + 0 = a + a = 0,$$
$$0 + a = a + 0 = a,$$
$$0\ 0 = 0\ a = a\ 0 = a\ a = 0$$

merupakan ring. Dalam hal ini, himpunan $A = \{ 0, 2 \}$ dengan operasi penjumlahan dan perkalian modulo 4 merupakan himpunan yang mempunyai sifat tersebut.

Contoh XI.3

Dapat dibuktikan dengan mudah bahwa himpunan bilangan bulat $\boldsymbol{Z}$, himpunan bilangan real $\boldsymbol{R}$, himpunan bilangan rasional $\boldsymbol{Q}$ dan himpunan bilangan kompleks $\boldsymbol{C}$ merupakan ring terhadap operasi penjumlahan dan perkalian aritmatika.

Contoh XI.4

Himpunan $Z_n = \{0, 1, 2, \ldots, n\text{-}1\}$ merupakan ring.

Bukti :

Untuk membuktikan bahwa Z_n merupakan ring dilakukan dengan cara menemukan suatu fungsi yang menyatakan relasi antara Z_n

dengan ring Z. Bila fungsi yang didapat tersebut mengawetkan operasi maka peta dari fungsi mempunyai sifat-sifat yang sama dengan daerah asal (*domain*) dari fungsi.

Misalkan $f : Z \to Z_n$ dengan $f(x) = r$ dan r merupakan sisa pembagian bila x dibagi n. Dalam contoh sudah dibuktikan bahwa f mengawetkan operasi +.

Bila diambil sebarang x, y dalam Z maka $x = nq_1 + r_1$ dan $y = nq_2 + r_2$ untuk suatu q_1, q_2, r_1 dan r_2 dalam Z sehingga

$$xy = (nq_1 + r_1)\,(nq_2 + r_2) = n(nq_1 + r_1 + nq_2 + r_2) + r_1 r_2$$

dan $r_1 r_2$ dapat dinyatakan sebagai $nq + r$.

Akibatnya $xy = n\,(n\,q_1 q_2 + q_1 r_2 + r_1 q_2 + q) + r$.

Oleh karena itu, $f(xy) = r$ dan $f(x)\,f(y) = r_1 r_2$.

Dengan mengingat definisi perkalian dalam Z_n maka $r_1 r_2 = r$ dan berarti

$$f(xy) = f(x)\,f(y).$$

Karena f mengawetkan operasi penjumlahan dan penggandaan maka berakibat Z_n ring.

Teorema XI.1

Diketahui A sebarang ring dan a, b, c sebarang elemen A.

Sifat-sifat berikut ini berlaku :

(1) $0 \,.\, a = a \,.\, 0 = 0$,

(2) $(-a)\,b = a\,(-b) = -\,(ab)$,

(3) $-\,(-b) = b$,

(4) $(-a)\,(-b) = ab$,

(5) $a(b - c) = ab - ac$,

(6) $(a - b)c = ac - ab$.

Bukti :

(1) Karena $0 \,.\, a + ba = (0 + b)\,a = ba$ dan pada sisi lain

$$0 \,.\, a + ba = 0 + ba.$$

Dengan menggunakan hukum kanselasi didapat $0 \,.\, a = 0$.

Dengan cara yang sama didapat juga bahwa $a \,.\, 0 = 0$.

(2) Karena $(-a)b + ab = (-a + a)\ b = 0\ .\ b$ maka hal ini berarti bahwa $(-a)b$ merupakan invers dari ab terhadap penjumlahan.
Karena invers dalam grup $< A, + >$ tunggal maka $(-a)b$ satu-satunya invers dari ab terhadap penjumlahan.
Dengan simbol : $(-a)b = -(ab)$.
Dengan cara yang sama diperoleh $a(-b) = -(ab)$.

(3) Persamaan $b + (-b) = -b + b = 0$ menunjukkan bahwa b merupakan elemen (tunggal) yang bila ditambah dengan $(-b)$ sama dengan 0.
Oleh karena itu, b merupakan invers dari $-b$ terhadap penjumlahan dan disimbolkan dengan $b = -(-b)$.

(4) $(-a)\ (-b) = a(-(-b)) = ab$

(5) $a\ (b\text{-}c) = a(b + (-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac$.

(6) Untuk latihan.

Dalam mempelajari sebarang tipe aljabar selalu digunakan cara yang umum untuk penelaahannya. Setelah diberikan definisi dasar contoh-contoh yang berkenaan dengan istilah baru juga diteliti tentang sistim bagian, sifat-sifat dasar, sistim lebih besar yang mengandung sistim bagian yang lebih kecil, homomorfisma yaitu fungsi antara dua sistim sehingga mengawetkan operasi dan sistim seperti G/S yang diturunkan dari sistim asal G dengan membentuk koset. Penelaahan selanjutnya biasanya ditunjukkan untuk sifat-sifat yang lebih khusus dari sistim aljabar tersebut.

RING BAGIAN

Dalam contoh terdahulu telah dikenal bahwa ring $\boldsymbol{Z}$ terkandung dalam ring $\boldsymbol{Q}$ dan ring $\boldsymbol{R}$ terkandung dalam $\boldsymbol{C}$. Dalam hal ini dapat dilihat bahwa operasi dari ring yang lebih kecil adalah operasi dari ring yang lebih besar dan dibatasi pada ring yang lebih kecil. Sebagai contoh dalam ring $\boldsymbol{C}$ operasi perkalian didefinisikan sebagai

$$(a + b\,i)\ (\ c + d\,i\ ) = (\ ac - bd\ ) + (\ ad + bc\ )\ i$$

sedangkan operasi itu dibatasi pada R berarti operasi yang sama dengan pembatasan pada R sehingga berbentuk $(a + 0\ i)\ (c + 0\ i)$ dan didapat

$$(a + 0\ i)\ (c + 0\ i) = (ac - 0\ .\ 0) + (a.\ 0 + 0\ .\ c)\ i$$
$$= ac + 0i$$

yang bernilai sama dengan ac.

Definisi XI.2

Misalkan S himpunan bagian dari A.
Himpunan S dinamakan *ring bagian* dari A jika memenuhi
(1) S ring,
(2) Operasi penjumlahan dan perkalian dari S adalah operasi penjumlahan dan perkalian dari A yang dibatasi pada S.

Definisi tersebut tidak efisien untuk mengecek apakah suatu himpunan bagian dari ring A merupakan ring bagian dari A sehingga diperlukan teorema berikut ini.

Teorema XI.2

Diketahui S himpunan bagian dari ring A.
Himpunan S merupakan ring bagian dari A jika dan hanya jika S tertutup terhadap perkalian dan tertutup terhadap pengurangan.

Bukti :

$\Rightarrow$
Untuk latihan.
$\Leftarrow$
Akan ditunjukkan bahwa S tertutup terhadap pengurangan maka S grup bagian dari A (terhadap penjumlahan).
Karena S tidak kosong maka S mengandung paling sedikit satu elemen, misalkan x dan dengan mengingat S tertutup di bawah pengurangan maka $x - x = x + (-x) = 0$ juga dalam S.
Berarti S mengandung identitas terhadap penjumlahan.

Untuk sebarang y dalam S, karena S tertutup terhadap pengurangan maka

$$0 - y = 0 + (-y) = -y$$

dalam S sehingga S mengandung semua invers dari elemen-elemennya terhadap penjumlahan.
Untuk sebarang x, y dalam S maka $-y$ dalam S dan akibatnya

$$x - (-y) = x + (-(-y)) = x + y$$

berada dalam S.
Oleh karena itu S tertutup terhadap penjumlahan.
Berarti S grup bagian dari $< A , + >$.
Karena grup bagian dari suatu grup abelian $< A, + >$ maka S juga grup abelian.
Karena S himpunan bagian dari ring A maka syarat hukum assosiatif, hukum distributif kiri dan hukum distributif kanan terpenuhi.
Berarti S merupakan ring terhadap operasi yang sama pada ring A yang dibatasi pada S.
Terbukti S ring bagian dari A.

Contoh XI.3

Himpunan bilangan genap $\boldsymbol{E}$ membentuk ring bagian dari himpunan bilangan bulat $\boldsymbol{Z}$.

Bukti :

$\boldsymbol{E} = \{ 2k | k \in Z \}$ jelas himpunan yang tidak kosong. Tinggal dibuktikan bahwa $\boldsymbol{E}$ tertutup terhadap operasi perkalian dan pengurangan.
Tertutup terhadap operasi perkalian.
Hasil kali $(2m)(2n) = 2(m.2n)$ dengan $m.2n$ bilangan bulat sehingga dengan menggunakan hukum assosiatif perkalian maka hasil kalinya masih dalam $\boldsymbol{E}$.
Tertutup terhadap pengurangan.
Karena $(2m)-(2n) = 2(m-n)$ dan $m-n$ bilangan bulat ($\boldsymbol{Z}$ tertutup terhadap operasi pengurangan) sehingga dalam $\boldsymbol{E}$.

Contoh XI.4

Bila didefinisikan $\boldsymbol{Q}(\sqrt{2}) = \{ a + b\sqrt{2} \mid a, b \text{ dalam } \boldsymbol{Q} \}$ maka akan dibuktikan bahwa $\boldsymbol{Q}(\sqrt{2})$ merupakan ring bagian dari $\boldsymbol{R}$.
Karena $\boldsymbol{Q}$ himpunan yang tidak kosong maka jelas bahwa $\boldsymbol{Q}(\sqrt{2})$ juga himpunan yang tidak kosong.
Terhadap operasi perkalian bersifat

$$(a + b\sqrt{2}) (c + d\sqrt{2}) = (ac + 2\,bd) + (ad + bc)\sqrt{2}$$

dan terhadap operasi pengurangan bersifat

$$(a + b)\sqrt{2} - (c + d)\sqrt{2} = (a - c) + (b - d)\sqrt{2} .$$

Karena $ac + 2bd$, $ad + bc$, $a - c$ dan $a - d$ tetap dalam $\boldsymbol{Q}$ maka hasil perkalian dan hasil pengurangannya tetap dalam $\boldsymbol{Q}(\sqrt{2})$.
Oleh karena itu $\boldsymbol{Q}(\sqrt{2})$ merupakan ring bagian dari $\boldsymbol{R}$.

Perlu dicatat bahwa $\boldsymbol{Q}(\sqrt{2})$ similar dengan himpunan bilangan kompleks

$$\boldsymbol{C} = \{ a + b\,i \mid a, b \text{ dalam R} \}$$

karena bentuk $a + b\,i$ analog dengan bentuk $a + b\sqrt{2}$ dan dalam hal ini ring $\boldsymbol{Q}(\sqrt{2})$ mengandung $\boldsymbol{Q}$, seperti juga $\boldsymbol{C}$ mengandung $\boldsymbol{R}$.

Contoh XI.5

Diketahui A ring dan b elemen tertentu dari A.
Jika didefinisikan $C_b = \{ x \text{ dalam } A \mid bx = xb \}$ maka akan dibuktikan C_b ring bagian dari A.
Himpunan C_b tidak kosong karena b komutatif dengan dirinya sendiri.
Misalkan x, y dalam C.
Karena $(xy)b = x (yb) = x (by) = (xb) y = (bx) y = b (xy)$ dan juga

$$(x - y)b = xb - yb = bx - by = b (x - y)$$

maka berarti xy dan $x - y$ komutatif dengan b sehingga merupakan elemen C.
Oleh karena itu C_b tertutup terhadap operasi penjumlahan dan operasi perkalian dan akibatnya C_b ring bagian dari A.

Contoh XI.6

Diketahui $M_{2\times 2}$ ring dan misalkan elemen tertentu $B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

Elemen $\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in C_b$ jika dan hanya jika

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} x & y \\ z & w \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

atau $\begin{pmatrix} z & w \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & x \\ 0 & z \end{pmatrix}$ yang benar jika dan hanya jika $z = 0$ dan $w = x$.

Hal ini berarti $C_B = \left\{ \begin{pmatrix} x & y \\ 0 & x \end{pmatrix} \mid x, y \in R \right\}$.

Contoh XI.7

Apabila *A* merupakan ring bagian dari ring *B*, sedangkan *B* mempunyai elemen satuan, apakah *A* juga harus mempunyai elemen satuan? Berikan contoh.

Jawab

Tidak perlu ring bagian *A* mempunyai elemen satuan. Sebagai contoh *A* adalah himpunan bilangan genap yang merupakan ring bagian dari himpunan bilangan bulat *B*. Himpunan *A* tidak mempunyai elemen satuan sedangkan elemen satuan dalam *B* adalah 1.

Macam-macam Ring

Seperti dalam teori grup, sifat-sifat dasar dari ring dapat digunakan untuk mengklasifikasikan ring dengan tujuan untuk membedakan antara ring-ring yang tidak isomorfis dengan menunjukkan perbedaan sifat- sifatnya. Tujuan lainnya adalah untuk mengurutkan ring-ring ke dalam kelas-kelas yang elemennya mempunyai sifat-sifat yang mengijinkan tipe tertentu dari suatu masalah dapat terselesaikan. Sebagai contoh, kelas ring apa yang selalu dapat mencari penyelesaian persamaan $ax + b = 0$ dengan a, b dalam A

dengan penyelesaiannya dalam A ? Untuk kelas ring apa yang setiap elemennya dapat difaktorkan secara tunggal ?

Beberapa sifat yang ditemui dalam bagian ini semuanya didasarkan pada sifat-sifat dari perkalian dalam ring himpunan bilangan bulat $\boldsymbol{Z}$ dan himpunan bilangan real $\boldsymbol{R}$. Dalam $\boldsymbol{Z}$ dan $\boldsymbol{R}$, perkalian dua elemen tidak nol dalam $\boldsymbol{Z}$ atau $\boldsymbol{R}$ masih tetap elemen tidak nol dalam $\boldsymbol{Z}$ atau $\boldsymbol{R}$. Tetapi sifat itu tidak ditemui dalam ring Z_6 karena $2 \,.\, 3 = 0$ dan dalam M_{2x2} berlaku sifat

$$\begin{pmatrix} 1 & -2 \\ 1 & -2 \end{pmatrix}\begin{pmatrix} 2 & 4 \\ 1 & 2 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Untuk menamakan kelas ring mempunyai sifat-sifat di atas terlebih dahulu didefinisikan sifat – sifat berikut ini.

Definisi XI.3

Elemen a dan b tidak nol dari ring A dinamakan pembagi nol (*divisors of zero*) jika $ab = 0$.

Seperti disebutkan di atas, himpunan bilangan real $\boldsymbol{R}$ tidak mempunyai pembagi nol dan demikian juga himpunan bilangan kompleks $\boldsymbol{C}$. Tetapi ring M_{nxn} untuk $n \geq 2$ dan Z_n dengan n tidak prima mempunyai pembagi nol. Di samping itu sifat lain dari $\boldsymbol{Z}$ dan $\boldsymbol{R}$ terhadap operasi perkalian adalah komutatif dan mempunyai elemen identitas 1. Tidak semua ring mempunyai sifat tersebut, sebagai contoh dalam M_{2x2} sifat komutatif tidak selalu berlaku dan pada ring himpunan bilangan genap tidak mempunyai elemen identitas terhadap operasi perkalian. Himpunan bilangan real $\boldsymbol{R}$ juga mempunyai sifat bahwa setiap elemen $\boldsymbol{R}$ yang tidak nol mempunyai invers. Berikut ini diberikan definisi untuk menggolongkan ring ke dalam kelas -kelas yang didasarkan pada sifat – sifat perkalian.

Definisi XI.4

(1) Ring A dinamakan *ring komutatif* jika $ab = ba$ untuk semua a, b dalam A.

(2) Ring A dinamakan ring dengan elemen satuan (*unity*) jika A mengandung identitas terhadap perkalian.
(3) Ring A dinamakan daerah integral (*integral domain*) jika A ring komutatif dengan elemen satuan dan tidak mempunyai pembagi nol.
(4) Ring A dinamakan field jika A ring komutatif dan setiap anggota yang tidak nol mempunyai invers.

Himpunan bilangan bulat $\boldsymbol{Z}$ merupakan daerah integral tetapi bukanlah suatu field. Konsep dari daerah integral merupakan perumuman dari $\boldsymbol{Z}$. Demikian juga dapat dilihat bahwa definisi tentang field didasari pada sifat-sifat yang ada pada $\boldsymbol{R}$. Jika ring F yang didapatkan merupakan field maka persamaan $ax + b = 0$ dengan a, b dalam F dan $a \neq 0$ selalu mempunyai penyelesaian dalam F. Dapat dibuktikan bahwa Z_n dengan n tidak prima merupakan ring komutatif dengan elemen satuan yang bukan daerah integral sedangkan Z_n untuk n prima merupakan daerah integral dan juga sekaligus field. Di samping itu dapat dibuktikan dengan mudah bahwa himpunan bilangan rasional $\boldsymbol{Q}$ merupakan field.

Contoh XI.8

Misalkan A suatu ring yang mempunyai lebih dari satu elemen. Jika A mempunyai elemen satuan e maka elemen satuan tersebut tersebut tidak sama dengan elemen netral 0.

Jawab

Karena ring A mempunyai lebih dari satu elemen maka pasti ada $a \in A$ dengan $a \neq 0$ maka $a\,0 = 0$ dan $a\,e = a$. Andaikan $e = 0$ maka $a = a\,e = a\,0 = 0$ sehingga kontradiksi dengan $a \neq 0$.

Contoh XI.9

Buktikan bahwa A ring komutatif jika dan hanya jika untuk setiap a, $b \in A$ berlaku

$$a^2 + 2\,ab + b^2 = (a + b)^2.$$

Jawab

Jika A ring komutatif maka untuk setiap $a, b \in A$ berlaku $ab = ba$ sehingga

$$(a + b)^2 = a^2 + ab + ba + b^2$$
$$= a^2 + 2\,ab + b^2.$$

Jika untuk setiap $a, b \in A$ berlaku

$$a^2 + 2\,ab + b^2 = (a + b)^2$$

maka $(a + b)^2 = a^2 + 2\,ab + b^2$ sehingga

$$a^2 + ab + ba + b^2 = a^2 + ab + ab + b^2.$$

Dengan menggunakan hukum kanselasi diperoleh $ab = ba$. Terbukti A ring komutatif.

Contoh XI.10

Jika ring A mempunyai tepat n elemen maka berlaku $n\,a = 0$ untuk setiap $a \in A$.

Jawab :

Elemen-elemen dari A merupakan grup terhadap operasi penjumlahan. Misalkan orde dari a adalah p. Hal ini berarti bahwa $pa = 0$. Dengan menggunakan teorema Lagrange dalam teori grup maka p membagi habis n atau terdapat bilangan bulat k sehingga $n = kp$. Akibatnya

$$n\,a = (kp)\,a = k\,(pa) = k\,0 = 0.$$

Contoh XI.11

Buktikan bahwa himpunan $A = \{ 0, 2, 4\}$ merupakan ring terhadap operasi penjumlahan perkalian modulo 6.

Jawab

Tabel-tabel untuk operasi penjumlahan modulo 6 dapat dibuat sebagai berikut :

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

sedangkan untuk operasi perkalian modulo 6 adalah:

.	0	2	4
0	0	0	0
2	0	4	2
4	0	2	4

Terlihat bahwa A ring komutatif yang mempunyai elemen satuan 4 dan setiap elemen yang tidak nol mempunyai invers terhadap perkalian.

Contoh XI.12

Apabila A ring bagian dari ring B yang mempunyai elemen satuan dan A mempunyai elemen satuan, apakah elemen satuan dalam A sama dengan elemen sama dengan elemen satuan B?

Jawab

Elemen satuan dari A dapat sama dengan elemen satuan dari B tetapi tidak selalu demikian. Dalam Contoh XI.11 ring A = { 0, 2, 4} merupakan ring bagian dari Z_6 terhadap operasi penjumlahan dan perkalian modulo 6. Dalam hal ini elemen satuan dalam A adalah 4 sedangkan elemen satuan dalam Z_6 adalah 1.

Latihan

1. Himpunan { 0, 6 } tertutup di bawah operasi perkalian tetapi bukan ring bagian dari Z_{10}.
2. Jelaskan mengapa Z_6 bukan ring bagian dari Z_{12}.
3. Buktikan bahwa $\boldsymbol{Z}[\sqrt{5}] = \{ a + b\sqrt{5} \mid a, b \text{ dalam } \boldsymbol{Z} \}$ merupakan sub ring dari $\boldsymbol{R}$.
4. Buktikan bahwa $\boldsymbol{Z}[\sqrt{-1}] = z[i] = \{ a + b\,i \mid a, b \text{ dalam } \boldsymbol{Z} \}$ merupakan ring bagian dari $\boldsymbol{C}$.
5. Jika a dalam Z_n maka buktikan bahwa himpunan (a) ring bagian dari Z_n dan bukan hanya bagian siklik dari Z_n.
6. Diketahui A ring dan b elemen tertentu dari A.
   Didefinisikan $N_b = \{ x \text{ dalam } A \mid xb = 0 \}$.
   Buktikan bahwa N_b merupakan ring bagian dari A.
   (N_b dinamakan annihilator kiri dari A).
7. (1) Jika $A = Z_s$ maka tentukan anihilator N_2.
   (2) Jika $A = M_{2x2}$ maka tentukan N_b dengan $b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.
8. Diketahui A ring dan T ring bagian dari A.
   (a) Buktikan bahwa $S \cap T$ ring bagian dari A.
   (b) Berikan contoh penyangkal untuk membuktikan bahwa $S \cup T$ tidak selalu ring bagian dari A.
9. Buktikan bahwa
   $$\boldsymbol{Q}(\sqrt[3]{2}) = \{ a + b\sqrt[3]{2} + (\sqrt[3]{2})^2 \mid a, b, c \text{ dalam } \boldsymbol{Q} \}$$
   merupakan bagian dari $\boldsymbol{R}$.
10. Tentukan semua pembagi nol dan semua *unit* (elemen yang mempunyai invers) dalam Z_{10}.
11. Tentukan semua unit dan pembagi nol dalam $\boldsymbol{Z}$.
12. Tentukan semua unit dan pembagi nol dalam Z_4.
13. Tentukan semua unit dan pembagi nol dalam Z_5.
14. Sebarang Z_p dengan p prima merupakan field.
    Tentukan invers terhadap perkalian dari 3, 7, 11, 16 dalam Z_{17}.
15. Tentukan penyelesaian dari $2x + 3 = 0$ dalam Z_7.
16. Tentukan penyelesaian dari $2x + 3 = 0$ dalam Z_{10}.

17. Buktikan bahwa $\boldsymbol{Z}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \text{ dalam } \boldsymbol{Z} \}$ merupakan daerah integral tetapi bukan field.
18. Jika A sebarang ring dan $A^* = \{ a \text{ dalam } A \mid x \text{ mempunyai invers terhadap perkalian dalam } A \}$ maka buktikan bahwa A^* grup terhadap perkalian.
19. Berikan contoh ring yang tidak komutatif dan tidak mempunyai elemen satuan.
20. Diketahui $\boldsymbol{R}$ ring dan a elemen $\boldsymbol{R}$. Buktikan bahwa himpunan $\{ x \in \boldsymbol{R} \mid a\,x = 0 \}$ merupakan ring bagian dari $\boldsymbol{R}$.

***

BAB XII
DAERAH INTEGRAL DAN FIELD

Dalam bab XI telah dijelaskan bahwa daerah integral adalah ring komutatif dengan elemen satuan dan tidak mempunyai pembagi nol sedangkan field adalah ring komutatif dengan elemen satuan dan setiap elemen yang tidak nol mempunyai invers. Dalam bab ini akan dibahas tentang sifat-sifat dasar dari daerah integral dan field.

Teorema XII.1

(1) Jika a dalam A dan a mempunyai invers maka a bukan pembagi nol.
(2) Jika A field maka A daerah integral.

Bukti :

(1) Misalkan $ab = 0$.
Karena a mempunyai invers maka dengan mengalikan kedua ruas dengan a^{-1} diperoleh

$$a^{-1}(ab) = a^{-1}\,0$$
$$(a^{-1}a)b = 0$$
$$1 \,.\, b = 0$$
$$b = 0.$$

Dengan cara yang sama, $ba = 0$ mengakibatkan $b = 0$.
Oleh karena itu, a bukan pembagi nol.

(1) Karena setiap field merupakan ring komutatif dengan elemen satuan maka tinggal dibuktikan bahwa dalam field tidak terdapat pembagi nol.
Karena setiap elemen field yang tidak nol mempunyai invers maka dengan mengingat sifat (1) sebarang field tidak mengandung pembagi nol.
Berarti setiap field merupakan suatu daerah integral.

Dapat dibuktikan bahwa ring dalam Contoh XI.2 merupakan field yang mempunyai 2 elemen.

Contoh XII.1

Himpunan bilangan kompleks $\boldsymbol{C}$ merupakan field karena untuk setiap elemen $a + b\ i$ yang tidak nol dengan $i = \sqrt{-1}$ mempunyai invers $\frac{a}{a^2+b^2}+\frac{-b}{a^2+b^2}i$. Berarti $\boldsymbol{C}$ juga sekaligus daerah integral.

Contoh XII.2

Dapat dibuktikan bahwa

$$\boldsymbol{Q}(\sqrt{2}) = \{\, a + b\sqrt{2} \mid a, b \text{ dalam } \boldsymbol{Q}\}$$

merupakan ring bagian dari $\boldsymbol{R}$. Dapat juga diuji bahwa $1 + 0\sqrt{2}$ elemen satuan dalam $\boldsymbol{Q}(\sqrt{2})$. Karena $\boldsymbol{Q}(\sqrt{2})$ ring bagian, komutatif dan tidak mempunyai pembagi nol maka $\boldsymbol{Q}(\sqrt{2})$ daerah integral. Misalkan diambil $a + b\sqrt{2} \neq 0$ maka $a - b\sqrt{2}$ juga tidak nol.
Akibatnya dengan merasionalkan penyebutnya didapat

$$\frac{1}{a+b\sqrt{2}}\frac{a-b\sqrt{2}}{a-b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-b^2}+\frac{-b}{a^2-b^2}\sqrt{2}.$$

Dalam hal ini $a^2 - 2b^2$ bilangan rasional dan tidak nol sehingga

$$\frac{a}{a^2-2b^2}+\frac{-b}{a^2-b^2}\sqrt{2}$$

merupakan elemen $\boldsymbol{Q}(\sqrt{2})$. Hal itu berarti setiap elemen $\boldsymbol{Q}(\sqrt{2})$ mempunyai invers terhadap perkalian dalam $\boldsymbol{Q}(\sqrt{2})$ dan berarti $\boldsymbol{Q}(\sqrt{2})$ field.

Dalam kedua kasus di atas, jika diberikan field ($\boldsymbol{R}$ atau $\boldsymbol{Q}$) maka dapat dibentuk field lebih besar yang memuat field tersebut. Hal ini nantinya dapat diperluas dengan membentuk

$$F(\sqrt{c})=\{a+b\sqrt{c} \mid a, b \in F\ \}$$

yang mengandung field F.

Catatan :
Field tak berhingga : $\boldsymbol{Q}$, $\boldsymbol{Q}(\sqrt{2})$, $\boldsymbol{R}$ dan $\boldsymbol{C}$.
Field berhingga : Z_p dengan p prima.
Daerah integral yang bukan field : $\boldsymbol{Z}$.
Ring komutatif dengan elemen satuan yang bukan daerah integral : Z_n dengan n bukan prima.

Telah dijelaskan di atas bahwa setiap field merupakan daerah integral, tetapi tidak setiap daerah integral merupakan field. Sebagai contoh, himpunan bilanagan bulat $\boldsymbol{Z}$ merupakan daerah integral tetapi bukan field karena $2 \in \boldsymbol{Z}$ tidak mempunyai invers dalam $\boldsymbol{Z}$. Teorema di bawah ini menyatakan kaitan antara daerah integral berhingga dan field.

Teorema XII.2

Jika A daerah integral berhingga maka field.
Bukti :
Untuk latihan.

Teorema XII.3

Diketahui D daerah integral dan a, b dan c elemen dalam D dengan $a \neq 0$.
Sifat – sifat berikut ini berlaku :
(1) Jika $ab = ca$ maka $b = c$ (kanselasi kiri).
(2) Jika $ba = ca$ maka $b = c$ (kanselasi kanan).
(3) Persamaan $ax + b = 0$ dengan x tidak diketahui, paling banyak mempunyai satu penyelesaian.

Bukti :

(1) Karena $ab = ac$ mengakibatkan $ab - ac = 0$ sehingga $a(b\text{-}c) = 0$. Karena a tidak nol dan dalam D tidak ada pembagi nol sejati maka $b - c = 0$ atau $b = c$.
(2) Analog dengan (1) (Untuk latihan).

(3) Misalkan s dan t merupakan elemen D yang merupakan penyelesaian dari persamaan $ax + b = 0$.
Akibatnya $as + b = at + b$ atau $as = at$.
Dengan menggunakan kanselasi kiri diperoleh $s = t$.

Meskipun teorema tersebut di atas dinyatakan berlaku pada daerah integral tetapi sebenarnya juga berlaku pada sebarang ring yang tidak mempunyai pembagi nol sejati. Persamaan $ax + b = 0$ tidak perlu mempunyai suatu penyelesaian dalam $\boldsymbol{Z}$ tetapi bila a dan b elemen suatu field dan tidak nol maka teorema berikut ini menjamin adanya persamaan $ax + b = 0$.

Teorema XII.4

Diketahui F field dan a, b dalam F dengan $a \neq 0$. Persamaan $ax + b = 0$ mempunyai tepat satu penyelesaian dalam F.

Bukti:

Karena a dalam F dan a tidak nol maka terdapatlah a^{-1} sehingga persamaan $ax + b = 0$ menjadi

$ax = - b$
$x = a^{-1}(-b)$
$x = - a^{-1} b$.

Contoh XII.3

Persamaan kuadratik $ax^2 + bx + c = 0$ dengan $a \neq 0$ dapat diselesaikan dengan rumus kuadratik yang dikenal dengan rumus *ABC* bila a, b dan c elemen-angota dalam field F sehingga a mempunyai invers terhadap perkalian. Dalam hal ini akar dari persamaan kuadrat dinyatakan dengan

$$x = 2a^{-1}\left(-b \pm \sqrt{b^2 - 4ab}\right).$$

Sayangnya rumus ini tidak bekerja dalam sebarang field seperti Z_2 sebagai ring bagian dan juga mengandung akar polinomial

$$p(x) = x^2 + x + 1.$$

Karena $p(0) = p(1) = 1$ maka polinomial $p(x)$ tidak mempunyai akar dalam Z_2.

Oleh karena itu diperkenalkan simbol α yang memenuhi

$$\alpha^2 + \alpha + 1 = 0$$

seperti layaknya $i = \sqrt{-1}$ sebagai akar polinomial $x^2 + 1 = 0$ dengan koefisien-koefisien dalam $\boldsymbol{R}$.

Perlu dicatat bahwa $\alpha^2 = -\alpha - 1 = \alpha + 1 \bmod 2$.

Dibentuk suatu sistim aljabar $Z_2(\alpha) = \{ a + b\,\alpha \mid a \text{ dan } b \text{ dalam } Z_2 \}$ yang mengandung 4 elemen.

Operasi penjumlahan dalam $Z_2(\alpha)$ didefinisikan sebagai

$$(a + b\,\alpha) + (c + d\,\alpha) = (a + c) + (b + d)\,\alpha$$

dengan $a + c$ dan $b + d$ dievaluasi pada mod 2.

Dianggap bahwa hukum komutatif dan hukum assosiatif berlaku (sebagai aksioma) dan mengganti α^2 dengan $\alpha + 1$ bila α^2 muncul. Hal ini analog dengan penggantian i^2 dengan -1 bila mengalikan $a + bi$ dan $c + di$. Berikut ini hasil perkalian elemen-elemen $Z_2(\alpha)$.

	0	1	α	$1 + \alpha$
0	0	0	0	0
1	0	1	α	$1 + \alpha$
α	0	α	$1 + \alpha$	1
$1 + \alpha$	0	$1 + \alpha$	1	α

Dengan mengecek tabel tersebut maka dapat dibuktikan bahwa $Z_2(\alpha)$ merupakan field yang mempunyai 4 elemen. Field berhingga seperti $Z_2(\alpha)$ sangat penting dalam teori penyandian.

Contoh XII.4

Konstruksikan suatu field yang mempunyai tiga elemen.

Jawab

Misalkan ring tersebut mempunyai 3 elemen yang berbeda yaitu $\{ 0, e, a \}$.

Tabel operasi penjumlahan dapat dibuat dengan langkah berikut ini.

+	0	e	A
0	0	e	A
e	e		
a	a		

Perhatikan kotak $e + e$. Hasil dari $e + e$ tidak mungkin sama dengan 0. Andaikan jika $e + e = 0$ maka $e + a = a$ sehingga dengan hukum kanselasi diperoleh $e = 0$. Kontradiksi dengan A ring yang mempunyai 3 elemen. Akibatnya $e + e = a$.
Lebih lanjut, diperoleh $e + a = 0$. Demikian juga dapat dibuktikan dengan mudah bahwa $a + e = 0$ dan $a + a = e$.

+	0	e	a
0	0	e	a
e	e	a	0
a	a	0	E

Akan dikonstruksikan tabel untuk perkalian :

.	0	e	a
0	0	0	0
e	0	e	a
a	0	a	e

Tabel tersebut dikonstruksikan dengan mengingat bahwa

$$a\ 0 = 0\ a = 0, e\ 0 = 0\ e = 0, 0\ 0 = 0.$$

Selanjutnya dengan mengingat e sebagai elemen identitas maka berlaku $e\ e = e$, $e\ a = a$ dan $a\ e = a$. Oleh karena itu haruslah $a\ a = e$ sehingga diperoleh tabel lengkap seperti di atas.

Contoh XII.5

Buktikan bahwa satu-satunya elemen nilpoten dalam suatu daerah integral adalah elemen netral terhadap operasi penjumlahan atau 0.

Jawab

Misalkan a elemen nilpoten dalam suatu daerah integral maka terdapat bilangan bulat positif n sehingga $a^n = 0$. Jika $n = 1$ maka jelas $a = 0$ dan jika $n > 1$ maka $a^n = a\, a^{n-1} = 0$ dan karena dalam daerah integral tidak ada pembagi nol sejati maka $a = 0$. Terbukti satu-satunya elemen nilpotent dalam suatu daerah integral adalah elemen netral 0.

Contoh XII.6

Buktikan bahwa selain 0 hanya elemen e yang merupakan elemen idempoten dalam suatu daerah integral.

Jawab

Misalkan $a \neq 0$ dan $a^2 = a$ (a elemen idempoten). Karena $ea = a$ maka $ea = a^2 = a$ sehingga $ea - a^2 = 0$. Diperoleh $(a - e)\, a = 0$. Karena daerah integral tidak mempunyai pembagi nol sejati maka $a - e = 0$ sehingga $a = e$.

Contoh XII.7

Diketahui $U = \{ a, b \}$.
Himpunan pangkat dari U adalah $P(U) = \{ \varnothing, A, B, U \}$ dengan $A = \{ a \}$ dan $B = \{ b \}$.
Operasi penjumlahan X, Y dalam P(U) didefinisikan sebagai

$$X + Y = (X \cup Y) - (X \cap Y)$$

dan operasi perkalian didefinisikan sebagai

$$X \,.\, Y = X \cap Y$$

sehingga diperoleh tabel operasi penjumlahan berikut ini:

+	$\varnothing$	A	B	U
$\varnothing$	$\varnothing$	A	B	U
A	A	$\varnothing$	U	B
B	B	U	$\varnothing$	A
U	U	B	A	$\varnothing$

dan tabel operasi perkalian:

.	$\varnothing$	A	B	U
$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$	$\varnothing$
A	$\varnothing$	A	$\varnothing$	A
B	$\varnothing$	$\varnothing$	B	B
U	$\varnothing$	A	B	U

Hal itu berarti P(U) merupakan ring komutatif dengan elemen satuan U.

Contoh XII.8

Himpunan $P(\boldsymbol{Z})$ adalah himpunan yang elemennya adalah semua himpunan bagian dari himpunan bilangan bulat $\boldsymbol{Z}$.
Operasi penjumlahan X, Y dalam P($\boldsymbol{Z}$) didefinisikan sebagai

$$X + Y = (X \cup Y) - (X \cap Y)$$

dan operasi perkalian didefinisikan sebagai

$$X \,.\, Y = X \cap Y.$$

Dalam hal ini, $X + X = (X \cup X) - (X \cap X) = X - X = \varnothing$ dengan $\varnothing$ elemen nol dalam P(Z).
Akibatnya P(Z) mempunyai karakteristik 2.

Latihan:

1. Tentukan semua pembagi nol dan semua unit (elemen yang mempunyai invers) dalam Z_{10}.
2. Generalisasi pertanyaan nomor 1 untuk Z_n.
3. Tentukan elemen idempoten dan elemen nilpoten dalam Z_6.
4. Tentukan elemen idempoten dan elemen nilpoten dalam Z_{10}.
5. Tentukan semua unit dan pembagi nol dalam $M_{2\times2}(\boldsymbol{R})$ dengan $\boldsymbol{R}$ bilangan real.
6. Apakah Z_6 field ? Beri alasan.
7. Apakah Z_7 field? Beri alasan.
8. Tentukan invers perkalian dari 3, 7, 11, dan 16 dalam Z_{17}.
9. Dalam field bilangan kompleks $\boldsymbol{C}$ mempunyai tepat satu penyelesaian untuk persamaan $a\,x + b = 0$. Jika diketahui $a = a_1 + a_2\,i$ dengan $a \neq 0$ dan $b = a_1 + a_2\,i$ maka tentukan penyelesaian dari $a\,x + b = 0$.
10. Tentukan penyelesaian dari $x^2 + 3\,x + 2 = 0$ dalam Z_5.
11. Misalkan A sebarang ring dan A^* adalah himpunan semua elemen tidak nol dalam A. Buktikan bahwa A field jika dan hanya jika A^* grup abelian di bawah operasi perkalian.
12. Misalkan A sebarang ring bagian dari bilangan real R dan misalkan n sebarang bilangan bulat positif. Buktikan $M_{n\times n}(A)$ ring bagian dari $M_{n\times n}(R)$.
13. Misalkan F field. Didefinisikan determinan pada $M_{2\times2}(F)$ dengan aturan $\det(A) = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$.

    a. Buktikan bahwa jika $D = \det(A) \neq 0$ maka $A^{-1} = D^{-1}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

    b. Jika $\det(A) = 0$ maka A^{-1} tidak ada.
14. Diketahui S adalah himpunan semua matriks berbentuk

$$\begin{pmatrix} x & 0 \\ x & 0 \end{pmatrix}$$

dengan x bilangan real. S merupakan ring terdahap operasi penjumlahan dan perkalian matriks. Apakah S field ?

15. Diketahui S adalah himpunan semua matriks berbentuk

$$\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

dengan x bilangan real. S merupakan ring terdahap operasi penjumlahan dan perkalian matriks. Apakah S field ?

***

BAB XIII
IDEAL DAN RING KUOSEN

Dalam teori grup dikenal grup normal dan analog dengan grup normal, dalam teori ring didefinisikan ideal dalam suatu ring. Berikut ini diberikan definisi ideal dari suatu ring.

Definisi XIII.1

Diketahui A ring dan I himpunan bagian tidak kosong dari A.
Himpunan A dinamakan suatu ideal dari A jika :

(1) Himpunan I tertutup di bawah operasi pengurangan.
(2) Himpunan I mengandung semua hasil kali xa dan ax dengan x dalam I dan a sebarang elemen dalam A.

Berdasarkan syarat (2) maka terlihat bahwa setiap ideal dari suatu ring merupakan ring bagian.

Definisi XIII.2

Diketahui A ring komutatif dengan elemen satuan dan x elemen tertentu dari A. Jika didefinisikan $(x) = \{ ax \mid \text{dalam } A \}$ maka (x) ideal dalam A dan dinamakan ideal utama (*principal ideal*) yang dibangun oleh x.

Contoh XIII.1

Diketahui himpunan bilangan $\boldsymbol{Z}$ merupakan ring komutatif dengan elemen satuan.
Dibentuk $(2)=\{a.2 \mid a \in \mathrm{Z}\}=2\boldsymbol{Z}$ yaitu himpunan bilangan genap merupakan ideal dalam $\boldsymbol{Z}$. Secara umum untuk $b \in \boldsymbol{Z}$ maka $(b) = \{ ab \mid a \in \boldsymbol{Z} \} = b\boldsymbol{Z}$ adalah ideal yang dibangun oleh b.

Contoh XIII.2

Diketahui Z_6 merupakan ring komutatif dengan elemen satuan terhadap operasi penjumlahan dan perkalian modulo 6.
Dibentuk (2) = { a.2 | $a \in Z_6$ } = { 0, 2, 4} dan berdasarkan definisi tersebut di atas (2) merupakan ideal dalam Z_6. Ideal-ideal lain dalam Z_6 adalah (1) = (3) = (5) = Z_6 dan ideal yang dibentuk oleh 3 yaitu (3) = { 0, 3 }.

Teorema XIII.1

(1) Jika F field maka hanya {0} dan F yang merupakan ideal dalam F.

(2) Sebaliknya, jika A ring komutatif dengan elemen satuan dan hanya memiliki ideal {0} dan A maka A field.

Bukti :

(1) Misalkan I ideal dalam F.
Jika I = {0} maka jelas bahwa I ideal.
Jika $I \neq \{0\}$ maka I mengandung suatu elemen tidak nol x.
Karena x juga dalam F maka terdapat x^{-1} dalam F sehingga untuk sebarang a dalam F berlaku $(ax^{-1})x = a\ (x\ x^{-1}) = a\ 1 = a$ dalam I (karena I ideal).
Berarti untuk setiap a dalam F maka a juga dalam I atau $F \subseteq I$.
Karena I ideal dari F maka juga $I \subseteq F$ sehingga diperoleh $F = I$.

(2) Jika x sebarang elemen tidak nol dalam A maka (x) ideal yang mengandung $1x = x$ sehingga $(x) \neq \{0\}$.
Karena ideal yang tidak nol dalam A hanyalah A maka $(x) = A$.
Karena A mengandung elemen satuan maka I dalam (x) sehingga terdapat a dalam A sehingga $ax = 1$.
Berarti A ring komutatif dengan elemen satuan dan setiap elemen yang tidak nol mempunyai invers.
Terbukti A field.

Contoh XIII.3

Himpunan bilangan real $\boldsymbol{R}$ merupakan field. Dengan menggunakan sifat pada Teorema XIII.1 maka mempunyai ideal {0} dan $\boldsymbol{R}$. Himpunan bilangan $\boldsymbol{Q}$ mempunyai sifat tertutup terhadap operasi perkalian dan pengurangan sehingga $\boldsymbol{Q}$ merupakan ring bagian dalam $\boldsymbol{R}$. Akan tetapi $\boldsymbol{Q}$ bukanlah ideal dalam $\boldsymbol{R}$ karena $\boldsymbol{Q} \neq \boldsymbol{R}$. Berarti $\boldsymbol{Q}$ merupakan salah satu contoh ring bagian dalam $\boldsymbol{R}$ yang bukan merupakan ideal. Contoh lain ring bagian yang bukan ideal adalah Z, nZ dengan n bilangan bulat.

Berdasarkan pada ideal dari suatu ring dapat didefinisikan suatu sistim aljabar yang dikenal dengan nama ring kuosen (*quotient ring*) dan secara formal dinyatakan dalam definisi berikut ini.

Definisi XIII.3

Diketahui A ring dan I sebarang ideal dalam A. Sistim aljabar A/I didefinisikan sebagai berikut :

(1) $A/I = \{ a + I \mid a \text{ dalam } A \}$

(2) Operasi penjumlahan dalam A/I didefinisikan sebagai

$$(a + I) + (b + I) = (a + b) + I$$

dan operasi perkalian dalam A/I didefinisikan sebagai

$$(a + I) (b + I) = ab + I.$$

Teorema XIII.2

Sistim aljabar A/I yang didefinisikan di atas merupakan ring.

Bukti :

Untuk latihan.

Definisi XIII.4

Diketahui A ring komutatif.

(1) Suatu ideal I dalam A dengan sifat bahwa ab dalam I berakibat salah satu dari a dalam I atau b dalam I dinamakan ideal prima (*prime ideal*) dalam A.

(2) Suatu ideal $\{0\} \subset I \subset A$ sehingga tidak ada ideal sejati dalam A yang mengandung I dinamakan ideal maksimal (*maximal ideal*) dalam A.

Teorema XIII.3

(1) Jika A komutatif dan I sebarang ideal dalam A maka A/I komutatif.

(2) Jika A mempunyai elemen satuan I dan ideal $I \neq A$ maka A/I mempunyai elemen satuan $1 + I$.

(3) Jika A komutatif dan mempunyai elemen satuan dan I ideal prima dengan $I \neq A$ maka A/I daerah integral.

Bukti :

(1) & (2) Untuk latihan.

(3) Karena A ring komutatif dengan elemen satuan maka dengan mengingat (1) dan (2) diperoleh A/I ring komutatif dengan elemen satuan.
Tinggal dibuktikan bahwa A/I tidak mempunyai pembagi nol.
Misalkan $(a + I)(b + I) = 0 + I$.
Diperoleh $ab + I = 0 + I$ sehingga berakibat ab dalam I.
Karena I ideal prima maka berlaku salah satu a dalam I atau b dalam I.
Hal ini berarti berlaku salah satu $a + I = 0 + I$ atau $b + I = 0 + I$.
Terbukti A/I daerah integral.

Contoh XIII.1

Diketahui himpunan bilangan bulat Z dan p prima. Akan ditentukan sifat-sifat dari ring kuosen $Z/(p)$.

Jika $ab \in (p)$ maka ab kelipatan dari p dan karena p prima maka a membagi p atau b membagi p sehingga $a \in (p)$ atau $b \in (p)$. Akibatnya dengan Teorema XIII.3, diperoleh $Z/(p)$ daerah integral.

Contoh XIII.2

Himpunan Z_8 = { 0, 1, 2, ..., 7} merupakan ring terhadap operasi penjumlahan dan perkalian modulo 8.
Ideal-ideal dalam Z_8 adalah
(0) = { 0 }, (1) = (3) = (5) = (7) = Z_8, (2) = { 0, 2, 4, 6 } dan (4) = { 0, 4 }.
Ideal I = (2) merupakan ideal maksimal sehingga ring kuosen yang terbentuk adalah

$$Z_8/I = \{ I ,\ 1 + I \}.$$

Hal itu berarti Z_8/I merupakan field yang hanya berisi 2 elemen.
Jika diambil ideal J = (4) maka ring kuosen yang terbentuk adalah

$$Z_8/J = \{ J, 1+J, 2+J, 3 + J \}$$

yang mempunyai elemen netral J dan elemen satuan $1 + J$. Dalam hal ini Z_8/J mempunyai pembagi nol sejati yaitu ada elemen Z_8/J yang tidak nol yaitu $2+J$ dan $(2+J)(2+J) = J$ sehingga Z_8 merupakan ring komutatif dengan elemen satuan yang bukan daerah integral.

Contoh XIII.3

Himpunan Z_{10} = { 0, 1, 2, ..., 10} merupakan ring terhadap operasi penjumlahan dan perkalian modulo 10.
Ideal-ideal dalam Z_{10} adalah
(0) = { 0 }, (1) = (3) = (7) = (9) = Z_{10},
(2) = (4) = (6) = (8) = { 0, 2, 4, 6, 8 }
dan (5) = { 0, 5 }. Ideal I = (2) merupakan ideal maksimal sehingga terbentuk ring kuosen

$$Z_{10}/I = \{ I ,\ 1 + I \}.$$

Hal itu berarti Z_{10}/I merupakan field yang hanya berisi 2 elemen.
Jika diambil ideal J = (5) maka ring kuosen yang terbentuk adalah

$$Z_{10}/J = \{ J, 1+J, 2+J, 3 + J, 4+J \}$$

yang mempunyai sifat field yang berisi 5 elemen.

Contoh XIII.4

Diketahui Z_8 = { 0, 1, 2, 3, 4, 5, 6, 7 } merupakan ring komutatif terhadap operasi penjumlahan dan perkalian modulo 8. Misalkan didefinisikan

$N = \{ a \in Z_8 \mid a^n = 0$ untuk suatu bilangan bulat positif $n \}$.

Jelas $0^1 = 0$, $2^3 = 0$, $4^2 = 0$ dan $6^3 = 0$ sehingga N = { 0, 2, 4, 6 } yang merupakan ideal dalam Z_8. Secara umum dapat dibuktikan bahwa jika A ring komutatif dan

$N = \{ a \in A \mid a^n = 0$ untuk suatu bilangan bulat positif $n \}$

maka N ideal dalam A.

Contoh XIII.5

Diketahui

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in Z \right\}$$

ring dengan elemen satuan tetapi tidak komutatif. Buktikan bahwa

$$I = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in Z \right\}$$

ideal dalam S.

Bukti :

Jelas bahwa $I \neq \varnothing$.

Ambil sebarang $A, B \in S$.

Akibatnya

$$A + B = \begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & y \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & x+y \\ 0 & 0 \end{pmatrix} \in S$$

$$-A = -\begin{pmatrix} 0 & x \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -x \\ 0 & 0 \end{pmatrix} \in S$$

.

Untuk sebarang $C = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in S$ berlaku

$$AC = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} 0 & bz \\ 0 & 0 \end{pmatrix} \in I$$

$$CA = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & xb \\ 0 & 0 \end{pmatrix} \in I$$

.

Hal itu berarti I ideal dalam *S*.

Latihan

1. Buktikan bahwa jka A ring komutatif dan I sebarang ideal dalam A maka A/I ring komutatif.
2. Jika A mempunyai elemen satuan I dan ideal $I \neq A$ maka A/I mempunyai elemen satuan $1 + I$. Buktikan!
3. Diketahui Z_6 merupakan ring. Tentukan semua ideal dalam Z_6. Pilih ideal maksimal I dalam Z_6 dan bentuk Z_6/I. Apakah sifat-sifat dari Z_6/I ?
4. Diketahui Z_7 merupakan ring. Tentukan semua ideal dalam Z_7. Pilih salah satu ideal I dalam Z_7 dan bentuk Z_7/I. Apakah sifat-sifat dari Z_7/I ?
5. Diketahui Z_9 merupakan ring. Tentukan semua ideal dalam Z_9. Pilih salah satu ideal I dalam Z_9 dan bentuk Z_9/I. Apakah sifat-sifat dari Z_9/I ?
6. Tentukan semua ring bagian dalam Z_{12} dan semua ideal dalam Z_{12}. Apakah semua ring bagian juga merupakan ideal?
7. Misalkan A ring komutatif dengan elemen satuan dan x elemen tertentu dalam A. Buktikan bahwa $(x) = \{ ax \mid a \in A \}$ ideal dalam A.
8. Tunjukkan bahwa $S = \{ 2z \mid z \in Z \}$ ring bagian tetapi bukan ideal dalam
$$Z[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in Z \}.$$
9. Misalkan I dan J ideal dalam ring A dan didefinisikan
$$I + J = \{ x + y \mid x \in I \ \& \ y \in J \}.$$
Buktikan $I + J$ ideal dalam A.
10. Misalkan I dan J ideal dalam ring A dan didefinisikan
$$I \cap J = \{ x \mid x \in I \ \& \ x \in J \}$$
Buktikan $I \cap J$ ideal dalam A.

11. Diketahui himpunan bilangan bulat ***Z***. Apakah dalam ***Z*** berlaku bahwa setiap ring bagian merupakan ideal ?
12. Diketahui himpunan bilangan real ***R*** merupakan ring. Apakah dalam ***R*** berlaku bahwa setiap ring bagian merupakan ideal ?
13. Diketahui A ring komutatif dan b elemen tertentu dalam A. Jika didefinisikan

$$N_b = \{\, x \in A \mid xb = 0 \,\}$$

maka buktikan bahwa N_b ideal dalam A.

14. Diketahui

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in Z \right\}$$

ring terhadap operasi penjumlahan dan perkalian matriks. Buktikan bahwa

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in Z \right\}$$

ideal dalam S.

15. Diketahui

$$S = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in Z \right\}$$

ring terhadap operasi penjumlahan dan perkalian matriks. Apakah

$$I = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \mid a, b \in Z \right\}$$

ideal dalam S? Jelaskan jawaban anda.

***

BAB XIV
HOMOMORFISMA RING

Dalam matematika, fungsi digunakan dengan tujuan untuk mengaitkan elemen-elemen dari suatu sistim ke sistim lain dan untuk mentransformasikan suatu sistim yang diberikan ke dalam sistim yang lebih sederhana. Fungsi atau pemetaan $f : X \to Y$ yang mengawetkan operasi yang didefinisikan pada sistim-sistimnya mempunyai sifat yang menarik yaitu dengan menganalisis peta dari f dapat digunakan untuk melihat sifat dari X dan sebaliknya. Berikut ini diberikan definisi formal dari fungsi yang mengawetkan operasi penjumlahan dan perkalian yang didefinisikan pada ring.

Definisi XIV.1

Diketahui A dan B ring.
Pemetaan atau fungsi $f : A \to B$ dinamakan homomorfisma ring (*ring homomorphism*) jika

(1) f mengawetkan operasi penjumlahan :

$$f(a + b) = f(a) + f(b),$$

(2) f mengawetkan operasi perkalian : $f(ab) = f(a)\, f(b)$,

untuk semua a dan b dalam A.

Contoh XIV.1

Diketahui A ring dan definisikan fungsi identitas $f : A \to A$ dengan $f(a) = 0$ untuk semua a dalam A. Fungsi f merupakan homomorfisma ring karena $f(a + b) = 0 = 0 + 0 = f(a) + f(b)$ dan

$$f(ab) = 0 = 0 \,.\, 0 = f(a)\, f(b).$$

Contoh XIV.2

Diketahui A ring dan definisikan fungsi identitas $f : A \to A$ dengan $f(a) = a$ untuk semua a dalam A. Fungsi f merupakan homomorfisma ring karena $f(a + b) = a + b = f(a) + f(b)$ dan $f(ab) = ab = f(a)\, f(b)$.

Contoh XIV.3

Didefinisikan pemetaan $f : R \to M_{2\times 2}$ dengan $f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$.

Jika diambil sebarang $x, y \in \boldsymbol{R}$ maka berlaku sifat

$$f(x+y) = \begin{pmatrix} x+y & 0 \\ 0 & x+y \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x) + f(y)$$

$$f(xy) = \begin{pmatrix} xy & 0 \\ 0 & xy \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x)\, f(y).$$

Hal itu berarti f homomorfisma.

Contoh XIV.4

Didefinisikan pemetaan $f : R \to M_{2\times 2}$ dengan $f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$.

Jika diambil sebarang $x, y \in \boldsymbol{R}$ maka berlaku sifat

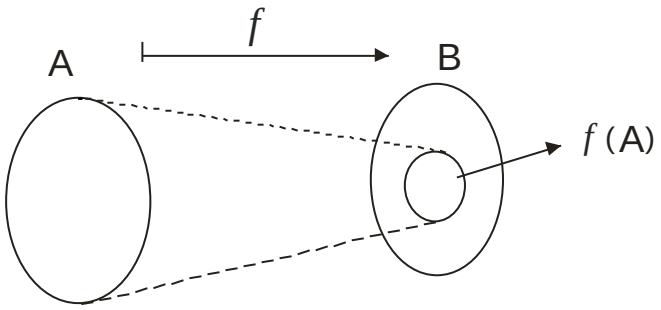
$$f(x+y) = \begin{pmatrix} x+y & 0 \\ 0 & x+y \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} + \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x) + f(y)$$

$$f(xy) = \begin{pmatrix} xy & 0 \\ 0 & xy \end{pmatrix} = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix} = f(x)\, f(y).$$

Hal itu berarti f homomorfisma.

Teorema XIV.1

Jika $f : A \to B$ homomorfisma ring maka $f(A)$ ring bagian dari B.



Bukti :

Karena $f(0) = 0'$ maka paling tidak $f(A)$ mengandung $f(0)$ sehingga $f(A)$ bukan himpunan kosong.
Karena f mengawetkan operasi + maka f merupakan homomorfisma grup dari $< A, + >$ ke $< B, + >$.
Oleh karena itu $f(A)$ tertutup di bawah operasi penjumlahan dan berlaku juga

$$f(x) - f(y) = f(x) + (-f(y))$$

terletak dalam $f(A)$ untuk semua $f(x), f(y)$ dalam $f(A)$.
Berarti $f(A)$ tertutup terhadap operasi penjumlahan.
Karena f mengawetkan operasi perkalian maka $f(x)\, f(y) = f(xy)$ untuk semua $f(x), f(y)$ dalam $f(A)$ dan dengan mengingat A tertutup maka xy dalam A sehingga $f(x)\, f(y)$ dalam $f(A)$. Berarti $f(A)$ tertutup terhadap operasi perkalian.

Contoh XIV.5

Berdasarkan Contoh IV.1, pemetaan $f : R \to M_{2\times 2}$ dengan

$$f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

merupakan homomorfisma ring sehingga $f(R)$ merupakan ring bagian dari $M_{2\times 2}$. Dalam hal ini,

$$f(R) = \left\{ \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} | r \in R \right\}.$$

Teorema XIV.2

Diketahui A ring dan B suatu sistim aljabar dengan dua operasi yaitu penjumlahan (+) dan perkalian (.) .
Jika $f : A \to B$ mengawetkan kedua operasi maka $f(A)$ ring yang termuat dalam sistim aljabar B.

Bukti :

Untuk latihan.

Teorema XIV.3

Diketahui $f : A \to B$ homomorfisma ring dengan peta $f(A)$.

(1) Jika A komutatif maka $f(A)$ komutatif.

(2) Jika A mempunyai elemen satuan 1 dan $f(1) \neq 0$ maka satuan untuk $f(A)$.
Jika $f(1) = 0$ maka $f(A) = \{ 0 \}$ ring yang sepele.

(3) Jika A daerah integral maka $f(A)$ tidak perlu daerah integral.

(4) Jika A field dan $f(1) \neq 0$ maka $f(A)$ field.

Bukti :

(1) Jika A komutatif maka untuk sebarang $f(x)$, $f(y)$ dalam $f(A)$ berlaku

$$f(x)\, f(y) = f(xy) = f(yx) = f(y)\, f(x)$$

sehingga $f(A)$ komutatif.

(2) Jika $f(1) = 0$ maka untuk sebarang $f(x)$ dalam $f(A)$ berlaku

$$f(x) = f(x \,.\, 1) = f(x)\, f(1) = f(x)\, 0 = 0$$

sehingga $f(A) = \{ 0 \}$ dan akibatnya $f(A)$ tidak mempunyai elemen satuan.
Jika $f(1) \neq 0$ maka $f(1)\, f(x) = f(1\ x) = f(x)$ dan $f(x)\, f(1) = f(x\ 1) = f(x)$ sehingga $f(1)$ merupakan elemen satuan dalam $f(A)$.

(3) Jika didefinisikan pemetaan $f : Z \to Z_6$ dengan n dalam Z dipetakan ke sisa pembagian dari n dengan 6, maka f merupakan homomorfisma yang surjektif sehingga $f(Z) = Z_6$.
Dalam hal ini Z_6 bukan daerah integral karena $2.3 = 0$ dengan 2,3 dalam Z_6 sedangkan $\boldsymbol{Z}$ daerah integral.

(4) Diketahui A field.
Jika $f(1) \neq 0$ maka $f(A)$ mempunyai elemen satuan $f(1)$.
Diambil sebarang $f(x) \neq 0$.
Karena f homomorfisma grup terhadap penjumlahan maka $f(0) = 0$.

Karena A field maka untuk x dalam A dan x tidak nol maka terdapat x^{-1} sehingga $f(x^{-1})$ merupakan invers terhadap perkalian dari $f(x)$ dan berlaku

$$f(x)\, f(x^{-1}) = f(x\, x^{-1}) = f(1).$$

Berarti juga $f(x^{-1}) = (f(x))^{-1}$.
Dengan cara yang sama diperoleh $f(x^{-1})\, f(x) = f(1)$.
Berarti $f(x^{-1}) = (f(x))^{-1}$.

Contoh XIV.5

Berdasarkan Contoh IV.3, pemetaan $f : \boldsymbol{R} \to M_{2\times 2}$ dengan

$$f(x) = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$$

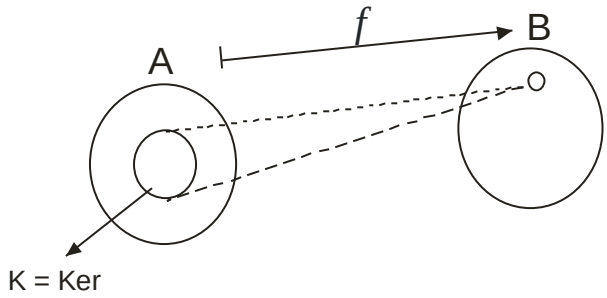
merupakan homomorfisma ring dan $\boldsymbol{R}$ merupakan ring komutatif sehingga $f(\boldsymbol{R})$ merupakan ring bagian dari $M_{2\times 2}$ yang juga komutatif. Selanjutnya, $\boldsymbol{R}$ ring dengan elemen satuan sehingga $f(\boldsymbol{R})$ merupakan ring yang mempunyai elemen satuan. Demikian juga, karena $\boldsymbol{R}$ field maka $f(\boldsymbol{R})$ juga merupakan field.

Teorema XIV.4

Jika $f : A \to B$ homomorfisma ring dengan inti

$$\text{Ker}(f) = K = \{\, x \text{ dalam } A \mid f(x) = 0 \,\}$$

maka K ideal dalam A.



Bukti :

Karena $f(0) = 0$ maka 0 dalam K sehingga K tidak kosong.
Ambil sebarang x, y dalam K dan sebarang a dalam A.

$$f(x - y) = f(x) - f(y) = 0 - 0 = 0$$
$$f(ax) = f(a)\, f(x) = f(a) \,.\, 0 = 0$$
$$f(xa) = f(x)\, f(a) = 0 \,.\, f(a) = 0.$$

Hal itu berarti $x - y$, $a\,x$ dan $x\,a$ dalam K sehingga dengan mengingat Definisi XIII.1 , K ideal.

Contoh XIV.6

Diketahui $\boldsymbol{Z}_6$ ring komutatif dengan elemen satuan 1.
Misalkan $f : \boldsymbol{Z}_6 \to \boldsymbol{Z}_6$ pemetaan dengan $f(a) = 4a$.
Karena $f(a + b) = 4(a + b) = 4a + 4b = f(a) + f(b)$ dan

$$f(ab) = 4(ab) = 16ab = (4a)(4b) = f(a)\, f(b)$$

maka f homomorfisma ring.
Akibatnya $f(0) = 0$, $f(1) = 4$, $f(2) = 2$, $f(3) = 0$, $f(4) = 4$, $f(5) = 2$. Hal itu berarti Ker(f) = { 0, 3} dan Im(f) = $f(\boldsymbol{Z}_6)$ = { 0, 2, 4 }.

Suatu isomorfisma ring (*ring isomorphism*) adalah homomorfisma ring yang bijektif. Jika $f : A \to B$ isomorfisma ring maka A dan B secara esensial sama (*essentially the same*) dan juga mempunyai sifat-sifat aljabar yang sama. Masalah-masalah dalam ring A sering kali dapat dipecahkan dengan perhitungan yang lebih mudah dalam ring B dan penyelesaiannya dibawa ulang dengan menggunakan f^{-1}. Isomorfisma dari A ke dirinya sendiri dinamakan **automorfisma**.

Sifat dari inti (*kernel*) dalam homomorfisma ring seperti dalam grup. Bila Ker(f) mempunyai k elemen maka homomorfisma f tepat k ke 1 yaitu untuk setiap koset a + Ker(f) dibawa ke $f(a)$. Khususnya, jika f homomorfisma surjektif dan Ker(f) = {0} maka A isomorfis dengan $f(A)$.

Teorema XIV.5

Jika F field dan $f : F \to B$ homomorfisma ring maka berlaku salah satu.
(i) f isomorfisma antara F dan peta dari f, atau

(ii) f merupakan homomorfisma sepele (*trivial*) yaitu $f(x) = 0$ untuk semua x.

Bukti :

Karena $\text{Ker}(f) \subseteq F$ merupakan ideal dari field F dan dengan mengingat teorema maka berlaku salah satu $\text{Ker}(f) = \{ 0 \}$ atau $\text{Ker}(f) = F$.
Jika $\text{Ker}(f) = \{ 0 \}$ maka f injektif dan akibatnya f isomorfisma dari F ke $f(F)$ (karena f pasti surjektif dari F ke $f(F)$).
Jika $\text{Ker}(f) = F$ maka jelas bahwa untuk setiap x dalam F berlaku $x \in \text{Ker}(f)$ atau $f(x) = 0$.

Contoh XIV.7

Diketahui $\boldsymbol{Z}_5$ ring komutatif dengan elemen satuan 1.

Misalkan $f : \boldsymbol{Z}_5 \to \boldsymbol{Z}_5$ homomorfisma ring.

Berdasarkan Teorema IV.6, f yang mungkin hanyalah fungsi nol atau fungsi identitas.

Contoh XIV.8

Akan dibuktikan bahwa $f : \boldsymbol{Q}(\sqrt{2}) \to \boldsymbol{Q}(\sqrt{2})$ dengan

$$f(a + b\sqrt{2}) = a - b\sqrt{2}$$

merupakan automorfisma dari $\boldsymbol{Q}(\sqrt{2})$.
Misalkan $a + b\sqrt{2}$, $c + d\sqrt{2}$ dalam $\boldsymbol{Q}(\sqrt{2})$.
Akibatnya

$$\begin{aligned} f((a + b\sqrt{2}) + (c + d\sqrt{2})) &= f((a + c) + (b + d)\sqrt{2}) \\ &= (a + c) - (b + d)\sqrt{2} \\ &= a - b\sqrt{2} + c - d\sqrt{2} \\ &= f(a + b\sqrt{2}) + f(c + d\sqrt{2}) \\ f((a + b\sqrt{2})(c + d\sqrt{2})) &= f((ac + 2bd) + (ad + bc)\sqrt{2}) \\ &= (ac + 2bd) - (ad + bc)\sqrt{2} \\ &= (a - b\sqrt{2})(c - d\sqrt{2}) \\ &= f(a + b\sqrt{2})\, f(c + d\sqrt{2}). \end{aligned}$$

Hal itu berarti f homomorfisma ring.

Karena Ker(f) ≠ $\boldsymbol{Q}(\sqrt{2})$ maka f bukan homomorfisma sepele dan $\boldsymbol{Q}(\sqrt{2})$ field maka f isomomorfisma dari $\boldsymbol{Q}(\sqrt{2})$ ke $f(\boldsymbol{Q}(\sqrt{2}))$.
Mudah dibuktikan bahwa $f(\boldsymbol{Q}(\sqrt{2})) = \boldsymbol{Q}(\sqrt{2})$.
Terbukti bahwa f automorfisma.

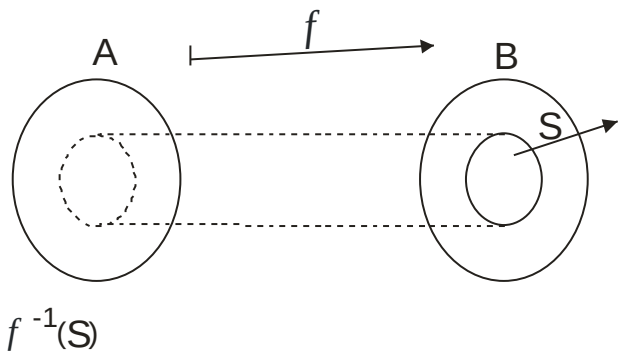
Dalam teorema terdahulu sudah dibuktikan bahwa jika $f : A \to B$ homomorfisma ring maka untuk setiap ideal I dalam A akan mengakibatkan $f(I)$ ideal dalam $f(A)$. Pandangan ini merupakan pandangan ke depan (*forward*) sedangkan pandangan ke belakang bertujuan untuk melihat apakah untuk setiap S ideal dalam $f(A)$ mengakibatkan invers f terhadap himpunan S (disimbolkan dengan $f^{1}(S)$) juga ideal dalam A ?

Definisi XIV.2

Diketahui $f : A \to B$ sebarang fungsi dan S sebarang himpunan bagian dari B.
Himpunan $f^{-1}(S)$ didefinisikan sebagai semua elemen A yang dibawa f ke elemen S.

$$f^{-1}(S) = \{ x \text{ dalam } A \mid f(x) \text{ dalam } S \}.$$

Himpunan $f^{-1}(S)$ dinamakan prapeta (*invers image*) dari S di bawah f.



Contoh XIV.9

Diketahui $\boldsymbol{Z}_6$ ring komutatif dengan elemen satuan 1.
Misalkan $f : \boldsymbol{Z}_6 \to \boldsymbol{Z}_6$ pemetaan dengan $f(a) = 4a$.
Telah dibuktikan bahwa f homomorfisma ring.
Jika S = { 0 } ring bagian dari daerah kawan $\boldsymbol{Z}_6$ maka $f^1(S)$ = { 0, 3 } yaitu ring bagian dari daerah asal $\boldsymbol{Z}_6$ dan jika T = { 0, 2, 4 } ring bagian dari daerah kawan $\boldsymbol{Z}_6$ sehingga $f^1(T)$ = { 0, 1, 2, 3, 4, 5 } = $\boldsymbol{Z}_6$ yaitu ring bagian dari daerah asal $\boldsymbol{Z}_6$.

Teorema XIV.6

Diketahui $f : A \to B$ homomorfisma ring.
(1) Jika S ideal dalam $f(A)$ maka $f^{-1}(S)$ ideal dalam A.
(2) Jika S ring bagian dari B maka $f^{-1}(S)$ ring bagian dari A.

Bukti :

(1) Jika diambil sebarang x, y dalam $f^{-1}(S)$ maka $f(x) = s' \in S$ dan $f(y) = s'' \in S$.
Akibatnya
$$f(x - y) = f(x) - f(y) = s' = s'' \in \mathrm{S}$$
(karena S ideal dalam $f(A)$).
Berarti x – y dalam $f^{-1}(S)$.
Jika diambil sebarang a dalam A maka
$$f(a\,x) = f(a)\,f(x) = f(a)\,.\,s'$$
dan
$$f(x\,a) = f(x)\,f(a) = s'\,.\,f(a)$$
dalam S karena $f(a)$ dalam $f(A)$ dan S ideal dalam $f(A)$.
Berarti $a\,x$ dan $x\,a$ dalam $f^{-1}(S)$. Terbukti bahwa $f^{-1}(S)$ ideal dalam A.
(2) Jika diambil sebarang x, y dalam $f^{-1}(S)$ maka $f(x) = s' \in S$ dan $f(y) = s'' \in S$.
Akibatnya $f(x - y) = f(x) - f(y) = s' - s'' \in S$ (karena S ring bagian dalam B) dan di samping itu
$$f(x\,y) = f(x)\,f(y) = s'\,.\,s'' \in S$$
dan
$$f(y\,x) = f(y)\,f(x) = s''.\,s' \in S.$$

Berarti $x - y$, xy dan yx dalam $f^{-1}(S)$.

Contoh XIV.9

Diketahui $\boldsymbol{Z}_6$ ring komutatif dengan elemen satuan 1.
Misalkan $f : \boldsymbol{Z}_6 \to \boldsymbol{Z}_6$ pemetaan dengan $f(a) = 4a$.
Telah dibuktikan bahwa f homomorfisma ring.
Jika $S = \{ 0 \}$ ideal dari daerah kawan $\boldsymbol{Z}_6$ maka $f^1(S) = \{ 0, 3 \}$ yaitu ideal dari daerah asal $\boldsymbol{Z}_6$ dan jika $T = \{ 0, 2, 4 \}$ ideal dari daerah kawan $\boldsymbol{Z}_6$ sehingga $f^1(T) = \{ 0, 1, 2, 3, 4, 5 \} = \boldsymbol{Z}_6$ yaitu ideal dari daerah asal $\boldsymbol{Z}_6$.

Contoh XIV.10

Pemetaan $f : \boldsymbol{Q}(\sqrt{2}) \to \boldsymbol{Q}(\sqrt{2})$ dengan

$$f(a + b\sqrt{2}) = a - b\sqrt{2}$$

merupakan automorfisma dari $\boldsymbol{Q}(\sqrt{2})$. Himpunan bilangan rasional $\boldsymbol{Q}$ merupakan ring bagian dalam $\boldsymbol{Q}(\sqrt{2})$ sehingga $f^{-1}(\boldsymbol{Q}) = \boldsymbol{Q}$ yang merupakan ring bagian dari dalam daerah asal.

Contoh XIV.11

Misalkan F field dalam mana setiap elemen x memenuhi

$$2 \,.\, x = x + x = 0.$$

Himpunan Z_2 merupakan salah satu contoh dari field yang mempunyai sifat tersebut dan demikian juga field dalam Contoh XII.3. Didefinisikan $f : F \to F$ dengan $f(x) = x^2$.
Akan dibuktikan bahwa bahwa f automorfisma.
Diambil sebarang x, y dalam F, maka berlaku sifat

$$f(x + y) = (x + y)^2 = x^2 + xy + yx + y^2$$

(karena F field maka $xy = yx$) sehingga

$$\begin{aligned} f(x + y) &= x^2 + 2\,xy + y^2 \\ &= x^2 + 0 + y^2 \\ &= f(x) + f(y) \end{aligned}$$

dan karena F field maka

$$f(xy) = (xy)^2 = x^2 y^2$$
$$= x^2 y^2$$
$$= f(x) f(y).$$

Dalam $Z_2(\alpha) = \{ a + b\alpha \mid a, b \in Z_2 \}$ juga berlaku sifat $2 . x = x + x = 0$. Berarti

$f(\alpha) = \alpha^2 = \alpha + 1$ dan $f(\alpha + 1) = (\alpha + 1)^2 = \alpha^2 + 2\alpha + 1 = \alpha + 1 + 0 + 1 = \alpha$.

Latihan

1. Tentukan apakah f homomorfisma ring atau bukan
   (i) $f: Z \to Z$ dengan $f(x) = 2x$.
   (ii) $f: Z_6 \to Z_5$ dengan $f(x) = 3x$.
   (iii) $f: \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = x^2$.
   (iv) $f: \boldsymbol{R} \to \boldsymbol{R}$ dengan $f(x) = e^x$.
2. Diketahui $f: Z \to Z_n$. Buktikan f homomorfisma surjektif.
3. Diketahui pemetaan $f: C \to C$ dengan $f(a + b\,i) = a - b\,i$. Buktikan f isomorfisma.
4. a. Jika $f: A \to B$ pemetaan dengan $f(x) = 0$ untuk setiap x dalam A dan A, B ring maka buktikan bahwa f homomorfisma (dan dinamakan homomorfisma sepele *trivial homomorphism*).
   b. Tunjukkan bahwa untuk sebarang ring A, fungsi identitas I yang didefinisikan dengan aturan $I(x) = x$ untuk sebarang x dalam A merupakan automorfisma.
5. Jika $f: A \to B$ dan $g: B \to C$ homomorfisma ring maka fg homomorfisma ring dari A ke C dan jika f dan g injektif maka gf juga injektif.
6. Diketahui $f: A \to B$ homomorfisma ring.
   Jika didefinisikan $f: A[x] \to B[x]$ dengan $f\left(\sum_i a_i\, x^i\right) = f(a_i)\, x^i$
   maka buktikan f homomorfisma.
7. Buktikan bahwa jika $f: A \to B$ homomorfisma ring maka untuk sebarang ring S dalam B berlaku bahwa $f^{-1}(S)$ ring bagian dari A.
8. Misalkan F field dalam mana setiap elemen x memenuhi
   $$3.x = x + x = 0.$$
   Himpunan Z_3 merupakan salah satu contoh dari field yang mempunyai sifat tersebut. Didefinisikan $f: F \to F$ dengan $f(x) = x^3$. Buktikan bahwa f automorfisma.
9. Diketahui $f: A \to B$ homomorfisma ring.
   a. Buktikan bahwa untuk sebarang ideal I dalam A, $f(I)$ ideal dalam $f(A)$.

b. Tunjukkan dengan contoh bahwa $f(I)$ tidak perlu ideal dalam B.

10. Tentukan semua homomorfisma ring dari himpunan bilangan real $\boldsymbol{R}$ ke $\boldsymbol{R}$.

11. Diketahui

$$S=\left\{\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a,b,\, c \in Z \right\}$$

ring terhadap operasi penjumlahan dan perkalian matriks.

a. Buktikan bahwa pemetaan $f : S \rightarrow \boldsymbol{Z}$ yang didefinisikan dengan

$$f\left(\begin{pmatrix} x & 0 \\ y & 0 \end{pmatrix}\right)=x$$

adalah epimorfisma.

b. Tentukan Ker(f) dan dan tunjukkan suatu isomorfisma dari S/Kerf(f) ke $\boldsymbol{Z}$.

12. Jika F_1 dan F_2 field maka tentukan semua homomorfisma dari F_1 ke F_2.

13. Misalkan f epimorfisma dari $\boldsymbol{R}$ ke $\boldsymbol{R}$. Buktikan bahwa jika $\boldsymbol{R}$ komutatif maka $\boldsymbol{R}$ juga komutatif.

14. Diketahui pemetaan $f : \boldsymbol{Q} \rightarrow \boldsymbol{R}$ dengan $f(x) = x$. Buktikan bahwa f homomorfisma yang injektif. Apakah f surjektif ?

15. Diketahui $f : R \rightarrow R'$ epimorfisma. Buktikan bahwa :

a. Jika I ideal dari R maka $f(I)$ ideal dari R.

b. Jika I ideal dari R' maka $f^1(I)$ ideal dari R.

***

BAB XV
RING POLINOMIAL

Dalam bab ini dibahas suatu himpunan yang elemen-elemennya berbentuk

$$a_n\, x^n + a_{n\text{-}1}\, x^{n-1} + \ldots\ldots\ldots + a_1 x^1 + a_0\, x^0$$

dengan koefisien-koefisien a_k dalam ring A untuk $k = 0, 1, 2, \ldots\ldots, n$. Himpunan itu disimbolkan dengan $A[x]$ dan elemen-elemennya dinamakan polinomial. Setiap polinomial dalam $A[x]$ adalah jumlahan dari suku-suku (terms) berbentuk $a_k x^k$. Nilai a_k dinamakan koefisien (*coefficient*) dari polinomial. Derajat dari polinomial

$$p(x) = a_n\, x^n + a_{n\text{-}1}\, x^{n-1} + \ldots\ldots\ldots + a_1 x^1 + a_0$$

sama dengan j maksimum sehingga a_j tidak nol dan a_j dinamakan koefisien pemimpin (*leading coefficient*) dari $p(x)$. Dalam hal ini dibuat perkecualian bahwa

$$0\, x^n + 0\, x^{n-1} + \ldots\ldots\ldots + 0\, x^1 + 0\, x^0$$

mempunyai derajat $-\infty$. Polinomial yang mempunyai koefisien pemimpin sama dengan 1 dinamakan polinomial monik (*monic polynomial*). Suku konstan (*constant term*) dari suatu polinomial yaitu $a_0\ x^0$ sering ditulis dengan a_0. Polinomial konstan (*constant polynomial*) adalah polinomial yang mempunyai derajat nol atau $-\infty$. Secara formal himpunan $A[x]$ didefinisikan sebagai berikut.

Definisi XV.1

Diketahui A ring.
Sistim aljabar $A[x]$ didefinisikan sebagai berikut :

(1) himpunan

$A[x] = \{\, a_n\, x^n + a_{n\text{-}1}\, x^{n-1} + \ldots\ldots + a_1 x^1 + a_0 \mid a_j$ dalam A dan n suatu bilangan bulat tidak negatif $\}$

(2) operasi :

- penjumlahan didefinisikan sebagai

$(a_n\, x^n + a_{n\text{-}1}\, x^{n-1} + \ldots + a_1 x^1 + a_0) + (b_n\, x^n + b_{n\text{-}1}\, x^{n-1} + \ldots + b_1 x^1 + b_0)$

$= (a_n + b_n)\, x^n + \ldots\ldots\ldots + (a_k + b_k)\, x^k + \ldots\ldots\ldots + (a_0 + b_0)\, x^0$

- perkalian didefinisikan sebagai

$(a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots\ldots + a_1 x^1 + a_0) \,.\, (b_n x^n + b_n\text{-}1\, x^{n-1} + \ldots\ldots\ldots + b_1 x^1 + b_0)$
$= \sum_k c_k x^k$

dengan x^k mempunyai koefisien c_k sama dengan

$$a_0\, b_k + a_1\, b_{k-1} + \ldots + a_k\, b_0$$

untuk $k = 0, 1, 2, \ldots, m + n$.

Teorema XV.1

Himpunan $A[x]$ merupakan ring.

Bukti :

Untuk latihan.

Monomial adalah polinomial $a_n x^n$ dengan tepat satu suku yang tidak nol. Berikut ini diberikan sifat dari perkalian dua monomial.

Teorema XV.2

Dalam sebarang polinomial $A[x]$ berlaku

$$(a_n x^n)\, (b_m x^m) = (a_n b_m)\, x^{n+m}.$$

Bukti :

Dengan menggunakan definisi formal dari perkalian didapat :
$(a_n x^n + 0\, x^{n-1} + \ldots\ldots + 0\, x^1 + 0\, x^0) \,.\, (b_m x^m + 0\, x^{n-1} + \ldots\ldots + 0\, x^1 + 0\, x^0) =$
$\sum_{k=0}^{m+n} c_k x^k$

dengan $c_k = a_0 b_k + a_1 b_{k-1} + \ldots\ldots + a_k b_0$.
Karena untuk setiap a_i nol kecuali a_n dan untuk setiap b_i nol kecuali b_m maka $a_i b_i = 0$ untuk setiap i dan j kecuali $a_n\, b_m$.
Akibatnya koefisien c_{m+n} tidak harus nol dan

$$c_{m+n} = a_0\, b_k + a_1\, b_{k-1} + \ldots\ldots + a_n\, b_m + \ldots + a_{n+m}\, b_0$$
$$= 0 + \ldots\ldots + 0 + a_n\, b_m + 0 + \ldots\ldots + 0$$

$= a_n\, b_m$.

Dalam aljabar elementer, bila

$$p(x) = a_n\, x^n + a_{n\text{-}1}\, x^{n\text{-}1} + \ldots + a_1\, x^1 + a_0\, x^0$$

polinomial dalam $A[x]$ dan s sebarang elemen dengan mensubstitusikan s pada x dalam polinomial $p(x)$ dituliskan dengan $p(s)$ sehingga

$$p(s) = a_n\, s^n + a_{n\text{-}1}\, s^{n\text{-}1} + \ldots\ldots + a_1\, s^1 + a_0\, s^0.$$

Dalam hal ini $p(s)$ merupakan polinomial dalam A. Jika $p(s) = 0$ maka s dinamakan akar (*root*) dari $p(x)$. Sebagai contoh 2 merupakan akar dari polinomial $p(x) = x^3 + 3x + 1$ dalam $Z_5[x]$ karena $p(2) = 0$.

Contoh XV.2

Polinomial $2x^2 - 4x - (5/2)$ irredusibel (*irreducible*) yaitu polinomial yang tidak dapat difaktorkan lagi, karena mempunyai faktor

$$(2x - 5)\,(x + 1/2)$$

dalam $\boldsymbol{Q}[x]$ sedangkan dengan menggunakan rumus ABC dapat diperlihatkan bahwa $3x^2 - x - 7$ redusibel atas $\boldsymbol{Q}$.

Ring $\boldsymbol{Q}[x]$ merupakan ring bagian dari ring $\boldsymbol{R}[x]$ karena himpunan $\boldsymbol{Q}$ ring bagian dari $\boldsymbol{R}$. Polinomial $x^2 + 2x - 2$ irredusibel atas $\boldsymbol{Q}[x]$ tetapi redusibel atas $\boldsymbol{R}[x]$ karena

$$p(x) = (x + (1 - \sqrt{3}\,))\,(x + (1 + \sqrt{3}\,)).$$

Contoh XV.3

Dalam $Z_5[x]$ berlaku sifat-sifat berikut ini :

Jika $q(x) = x^3 + x$, $p(x) = x^3 + x + 1$ maka $q(x) + p(x) = 2x^3 + 2x + 1$.

Polinomial $q(x) = x^3 + x$ merupakan polinomial redusibel atas $Z_5[x]$ karena $q(0) = q(4) = 0$ sehingga $q(x)$ dapat difaktorkan menjadi

$$q(x) = x^3 + x = x(x+1).$$

Di samping itu polinomial $p(x) = x^3 + x + 1$ merupakan polinomial irredusibel atas $Z_5[x]$ karena tidak ada elemen Z_5 yang merupakan akar polinomial $p(x)$.

Dengan kata lain $p(0), p(1), p(2), p(3), p(4)$ tidak nol.

Hal itu berarti polinomial berderajat tiga dalam Z_5 [x] tidak selalu dapat difaktorkan.

Contoh XV.4

Dalam $Z_5[x]$, $f(x) = x^2 + 1$ merupakan polinomial redusibel dalam $Z_5[x]$ karena $f(2) = 0$ sehingga $f(x) = x^2 + 1 = (x+2)(x+3)$. Berarti polinomial $f(x)$ dapat difaktorkan menjadi polinomial yang berderajat lebih kecil.

Contoh XV.5

Diketahui $f(x) = 3x^5 - 4x^2$ dan $g(x) = x^2 + 3x$ dalam $Z_5[x]$.
Dalam hal ini

$$f(0) = 0 = g(0),\ f(3) = 3 = g(3),$$
$$f(1) = 4 = g(1),\ f(4) = 3 = g(4),$$
$$f(2) = 0 = g(2).$$

Berarti $f(c) = g(c)$ untuk semua $c \in Z_5$ tetapi $f(x) \neq g(x)$ dalam $Z_5[x]$.

Teorema XV.3

(1) Jika A komutatif maka $A[x]$ komutatif.
(2) Jika A mempunyai elemen satuan maka $A[x]$ mempunyai elemen satuan.
(3) Jika A daerah integral maka $A[x]$ daerah integral.
(4) Jika A field maka $A[x]$ daerah integral yang bukan field.

Bukti :

(1) Jika $f(x)$ dalam $A[x]$ maka $f(x)$ dan $g(x)$ dapat dinyatakan sebagai
$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x^1 + a_0 x^0$
$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots\ldots + b_1 x^1 + b_0 x^0$
sehingga koefisien x^k dari
$f(x)\, g(x) = (a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x^1 + a_0 x^0)(b_n x^n + b_{n-1} x^{n-1} + \ldots\ldots + b_1 x^1 + b_0 x^0)$
adalah $a_0 b_k + a_1 b_{k-1} + \ldots\ldots + a_k b_0$.
Pada sisi lain koefisien dari x^k dalam $g(x) f(x)$ sama dengan
$a_0 b_k + a_1 b_{k-1} + \ldots\ldots + a_k b_0$
dan hal ini sama dengan $b_0 a_k + b_1 a_{k-1} + \ldots\ldots + b_k a_0$ karena A ring komutatif.

Berarti $f(x)\, g(x) = g(x)\, f(x)$ untuk semua $f(x), g(x)$ dalam $A[x]$.

(2) Misalkan $p(x) = \sum_{k=0}^{m} b_k x^k$ dalam $A[x]$.

Sifat ini berlaku

$$1\, x^0 \,.\, p(x) = 1\, x^0 \,.\, \sum_{k=0}^{m} b_k x^k = \sum_{k=0}^{m} \left((1x^0)(b_k x^k) \right)$$

$$= \sum_{k=0}^{m} (1b_k) x^{0+k}$$

$$= \sum_{k=0}^{m} b_k x^k$$

$$= p(x).$$

Dengan cara yang sama diperoleh $p(x) \,.\, 1\, x^0 = p(x)$.

(3) Misalkan A daerah integral.

Dengan menggunakan sifat (1) dan (2) maka $A[x]$ komutatif dan mempunyai elemen satuan.

Tinggal ditunjukkan bahwa tidak ada pembagi nol dalam $A[x]$.

Misalkan $f(x)$, g(x) polinomial tidak nol dalam $A[x]$ dan $f(x)$, g(x) dinyatakan sebagai

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x^1 + a_0 x^0$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \ldots\ldots + b_1 x^1 + b_0 x^0 \,.$$

Karena $f(x)$ dan $g(x)$ polinomial tidak nol maka koefisien pemimpin polinomial $f(x)$ yaitu a_n tidak nol dan b_m juga tidak nol.

Karena A daerah integral maka $a_n\, b_m$ tidak nol sehingga koefisien pemimpin dari $f(x)\, g(x)$ juga tidak nol.

Berarti $f(x)\, g(x)$ tidak nol atau $A[x]$ tidak mempunyai pembagi nol.

(4) Untuk latihan.

Polinomial ring yang biasa digunakan seperti $\boldsymbol{Z}[x]$, $\boldsymbol{Q}[x]$, $\boldsymbol{R}[x]$, $\boldsymbol{C}[x]$ dan $Z_p[x]$ dengan p prima merupakan daerah integral yang bukan field, sedangkan $Z_n[x]$ dengan $n > 2$ bukan prima merupakan ring dengan elemen satuan yang bukan daerah integral.

Teorema V.4

Dalam daerah integral $A[x]$ berlaku bahwa jika $f(x)$, g(x) dalam $A[x]$ dan masing-masing berderajat m dan n maka $f(x)$ g(x) berderajat $m + n$.

Teorema V.5 (*Algoritma Pembagian – The Division Algorithm*)

Diketahui F field.
Jika $a(x)$, $b(x)$ dalam $F(x)$ dengan $b(x) \neq 0$ maka terdapatlah dengan tunggal polinomial $q(x)$ dan $r(x)$ dengan derajat($r(x)$) < derajat($b(x)$) sehingga

$$a(x) = b(x)\, q(x) + r(x).$$

Khususnya, jika $r(x) = 0$ maka $b(x)$ dan $q(x)$ dinamakan faktor (*factor*) dari $a(x)$.

Contoh XV.6

Dalam Z_7[x] berlaku bahwa jika $a(x) = 2x^3 + 3x^2 + 20$, $b(x) = x + 3$ dalam $Z_7[x]$ maka terdapatlah $q(x) = 2x^2 + 4x + 2$ dan $r(x) = 3$ dalam $Z_7[x]$ sehingga

$$2x^3 + 3x^2 + 2 = (x + 3)\,(2x^2 + 4x + 2) + 3.$$

Teorema XV.6

Jika A ring dan $p(x) = f(x) + g(x)$ dalam $A[x]$ maka untuk sebarang s dalam A berlaku

$$p(s) = f(s) + g(s).$$

Bukti :

Untuk latihan.

Teorema XV.7

Jika A ring komutatif dan $p(x)$ dalam $A[x]$ mempunyai faktorisasi $f(x)$ $g(x)$ maka untuk sebarang s dalam A berlaku

$$p(s) = f(s)\, g(s).$$

Bukti :

Kasus 1 : $f(x)$ monomial $a_t x^t$.
Misalkan $g(x) = b_m x^m + \ldots\ldots + b_1 x + b_0$.
Perkalian $f(x)$ dan $g(x)$ adalah

$$\begin{aligned} p(x) = f(x)\, g(x) &= a_t x^t (b_m x^m + \ldots\ldots + b_1 x + b_0) \\ &= a_t x^t\, b_m x^m + \ldots\ldots + a_t x^t\, b_1 x + a_t x^t\, b_0 \\ &= a_t b_m\, x^{t+m} + \ldots\ldots + a_t\, b_1\, x^{t+1} + a_t\, b_0\, x^t . \end{aligned}$$

Dengan mensubstitusi s pada x diperoleh :

$$p(s) = a_t b_m\, x^{t+m} + \ldots\ldots + a_t\, b_1\, x^{t+1} + a_t\, b_0\, x^t .$$

Pada sisi lain

$$\begin{aligned} f(s)\, g(s) &= (a_t s^t)\, (b_m s^m + \ldots\ldots + b_1 s + b_0 s^0) \\ &= (a_t s^t)\, (b_m s^m + \ldots\ldots + a_t s^t\, b_1 s^1 + a_t s^t\, b_0 s^0) \\ &= a_t b_m s^{t+m} + \ldots\ldots + a_t\, b_1\, s^t s^1 + a_t\, b_0\, s^t s^0 \\ &= a_t b_m s^{t+m} + \ldots\ldots + a_t\, b_1\, s^{t+1} + a_t\, b_0\, s^t . \end{aligned}$$

Terlihat bahwa $p(s) = f(s)\, g(s)$.
(Ingat bahwa dalam hal ini sifat komutatif dari ring sangat diperlukan).

Kasus 2 : $f(x) = \sum_{i=0}^{n} a_i x^i$

Untuk latihan.
(Dengan menggunakan kasus 1, hukum distributif dan Teorema XV.6).

Dua teorema di atas berakibat pada teorema berikut ini.

Teorema XV.8

Jika A ring komutatif dan $a(x)$ dalam $A[x]$ sehingga memenuhi

$$a(x) = b(x)\, q(x) + r(x)$$

maka untuk sebarang s dalam A berlaku $a(s) = b(s)\, q(s) + r(s)$.

Bukti :

Untuk latihan.

Teorema XV.9

Diketahui A ring komutatif dengan satuan dan $a(x)$ dalam $A[x]$ tidak konstan.
Elemen s dalam A merupakan akar dari $a(x)$ jika dan hanya jika $x - s$ merupakan faktor dari $a(x)$.

Bukti :

$\Rightarrow$
Diketahui s akar dari $a(x)$.
Misalkan $b(x) = x - s$.
Dengan menggunakan algoritma pembagian diperoleh

$$a(x) = (x - s)\, q(x) + r(s)$$

untuk suatu $q(x)$, $r(x)$ dalam $A[x]$ dan derajat ($r(x)$) < 1 sehingga $r(x)$ merupakan polinomial konstan r_0 dan berarti

$$a(x) = (x - s)\, q(x) + r_0.$$

Kesamaan di atas tetap berlaku bila s disubstitusikan pada x sehingga

$$a(s) = (s - s)\, q(s) + r_0$$
$$0 = 0\, q(s) + r_0$$
$$0 = 0 + r_0 .$$

Berarti $r_0 = 0$ dan $x - s$ merupakan faktor dari $a(x)$.
$\Leftarrow$
Diketahui bahwa $a(x) = (x - s)\, q(x)$ untuk suatu $q(x)$.
Dengan mensubstitusikan s pada x diperoleh $a(s) = (s - s)\, q(s)$ sehingga $a(s) = 0\, q(s) = 0$.
Berarti s dalam A merupakan akar dari $a(x)$.

Teorema XV.10

Diketahui A sebarang field dan $p(x)$ sebarang polinomial berderajat dua dan tiga dalam $A[x]$.
Polinomial $p[x]$ redusibel atas A jika dan hanya jika $p(x)$ mempunyai akar dalam A.

Bukti :

$\Rightarrow$

Dengan mengingat Teorema XIV.4, faktorisasi $p(x)$ ke dalam faktor-faktor dengan derajat yang lebih rendah juga termasuk faktor dengan derajat satu, misalkan $(ax + b)\ q(x)$.

Karena a dalam F dan F field maka a^{-1} ada sehingga dapat dibentuk

$$[\ a^{-1}\ (ax + b)\ ]\ [\ a.\ q(x)\ ]$$

atau

$$[\ x - (-a^{-1}\ b)\ ]\ [\ a\ q(x)\ ]$$

Hal ini berarti bahwa $-a^{-1}$ merupakan akar dari $p(x)$ dalam A.

$\Leftarrow$

Misalkan s dalam A merupakan akar dari $p(x)$.

Akibatnya $x - s$ merupakan faktor dari $p(x)$ sehingga $p(x)$ mempunyai faktor berderajat satu.

Dalam hal ini polinomial irredusibel dengan derajat dua atau tiga atas Z_2 hanyalah $x^2 + x + 1$, $x^3 + x + 1$ dan $x^3 + x^2 + 1$.

Oleh karena itu, tidak ada faktor dari $p(x)$.

Dalam hal ini tidak diperlukan pengecekan apakah $p(x)$ habis dibagi dengan polinomial irredusibel $f(x)$ dengan derajat 4 atau lebih tinggi.

Jika $p(x) = f(x)\ q(x)$ maka derajat $q(x)$ adalah 2 atau kurang dan untuk derajat 2 atau kurang sudah dilakukan pengecekan.

Terbukti bahwa $p(x)$ irredusibel.

Contoh XV. 7

Polinomial $h(x) = x^2 - 1$ redusibel atas $\boldsymbol{Z}$ karena ada elemen $\boldsymbol{Z}$ yang merupakan akar dari $h(x)$ sehingga $h(x) = x^2 - 1 = (x+1)(x-1)$.

Polinomial $s(x) = 4x^2 - 1$ irredusibel atas $\boldsymbol{Z}$ karena tidak ada elemen $\boldsymbol{Z}$ yang merupakan akar dari $s(x)$ tetapi $4x^2 - 1$ redusibel atas $\boldsymbol{Z}$.

Polinomial $p(x) = x^2-4$ redusibel atas $\boldsymbol{Q}$ karena terdapat $2 \in \boldsymbol{Q}$ sehingga $p(2)=0$. Hal itu berarti $q(x) = x^2-2$ sedangkan polinomial merupakan polinomial irredusibel atas $\boldsymbol{Q}$ karena tidak ada elemen $\boldsymbol{Q}$ yang merupakan akar dari $q(x)$. Pada sisi lain, polinomial $p(x) = x^2-4$ dan

$q(x) = x^2-2$ redusibel atas R karena kedua polinomial mempunyai akar dalam $\boldsymbol{R}$ sehingga $p(x) = x^2-4 = (x+2)(x-2)$ dan

$$q(x) = x^2-2 = (x-\sqrt{2})(x+\sqrt{2}).$$

Teorema XV.11

Jika $p(x)$ polinomial berderajat $n \geq 0$ dengan koefisien dalam suatu daerah integral D maka $p(x)$ paling banyak mempunyai n akar dalam D.

Bukti :

Dalam pembuktian ini digunakan prinsip induksi pada derajat dari $p(x)$.

Polinomial derajat 0 merupakan konstan tidak nol $a\ x^0 = a$ dan jelas bahwa mempunyai 0 akar.

Misalkan $p(x)$ mempunyai derajat $n > 0$.

Jika D mengandung akar t_1 dari $p(x)$ mempunyai faktor $x - t_1$ dan

$$p(x) = (x - t_1)\ q(x)$$

dengan $q(x)$ mempunyai derajat n-1.

Anggapan induksinya adalah bahwa $q(s)$ dan sebarang polinomial derajat n-1 yang lain mempunyai paling banyak n-1 akar.

Misalkan $t_2, t_3, \ldots\ldots, t_k$ dengan $k \leq n$ (t_1 mungkin termasuk dalam akar yang sama).

Berarti $q(x)$ mempunyai faktorisasi

$$q(x) = (x - t_2)\ (x - t_3)\ \ldots\ldots\ (x - t_k)\ g(x).$$

Dalam hal ini $g(x)$ mempunyai derajat $n - k$ yang tidak mempunyai akar dalam D.

Akibatnya $p(x) = (x - t_1)\ q(x) = (x - t_1)\ (x - t_2)\ (x - t_3)\ \ldots\ldots\ (x - t_k)\ g(x)$.

Misalkan s sebarang elemen dalam D yang berbeda dari $t_1, t_2, \ldots\ldots, t_k$.

Dengan mengingat Teorema XV.7 diperoleh

$$p(s) = (s - t_1)\ (s - t_2)\ (s - t_3)\ \ldots\ldots\ (s - t_k)\ g(s).$$

Terlihat bahwa $p(s)$ merupakan perkalian dari $k + 1$ angota tidak nol dalam suatu daerah integral sehingga $p(s)$ tidak nol.

Hal itu berarti $p(x)$ paling banyak mempunyai k akar $t_1, t_2, \ldots\ldots, t_k$ dengan $k \leq n$.

Contoh XV.8

Akan dicari faktorisasi dari polinomial

$$f(x) = 2x^4 + x^3 + 3x^2 + 2x + 4$$

atas field Z_5.

Jawab

Terlebih dahulu akan ditentukan akar-akar dari $f(x)$ dalam Z_5.
Karena $f(0) = 4, f(1) = 2, f(2) = 0, f(3) = 1$ dan $f(4) = 1$ maka 2 adalah akar dari $f(x)$ dalam Z_5 sehingga

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

dengan $g(x)=2x^3 + 3x + 3$. Selanjutnya $g(0) = 3, g(1) = 3$ dan $g(2) = 0$ sehingga diperoleh

$$g(x) = 2x^3 + 3x + 3 = (x-2)(2x^2 + 4x + 1).$$

Dalam hal ini, $h(x) = 2x^2 + 4x + 1$ irredusibel karena $h(0)=1, h(1)=2, h(2) = 2, h(3) = 1, h(4) = 4$. Akibatnya $f(x)$ dapat difaktorkan menjadi

$$\begin{aligned} f(x) &= 2x^4 + x^3 + 3x^2 + 2x + 4 \\ &= (x-2)^2 (2x^2 + 4x + 1) \\ &= 2(x+3)^2 (x^2 + 2x + 3). \end{aligned}$$

Latihan

1. Tentukan $(3x^2 + 5x + 4) + (4x^2 + 3x + 2)$ dalam $Z_6[x]$.
2. Tentukan $(3x^2 + 5x + 2)(4x + 4)$ dalam $Z_6[x]$.
3. Tentukan $(3x^2 + 5x + 6) + (4x^2 + 3x + 6)$ dalam $Z_7[x]$.
4. Tentukan $(3x^2 + 5x + 2)(4x + 4)$ dalam $Z_7[x]$.
5. Tunjukkan bahwa $x^3 - x = 0$ tepat mempunyai 5 akar dalam Z_8.
6. Tentukan polinomial derajat 2 yang irredusibel atas Z_2.
7. Tentukan polinomial derajat 3 atas Z_2.
8. Tunjukkan bahwa hanya polinomial $x^3 + x + 1$ dan $x^3 + x^2 + 1$ yang irredusibel atas Z_2.
9. Tentukan semua polinomial derajat dua yang irredusibel atas Z_3.
10. Tunjukkan bahwa $x^4 + x^2 + 2$ iredusibel atas Z_3.
11. Tentukan semua polinomial derajat 2 yang irredusibel atas Z_4.
12. Buktikan bahwa $p(x) = x^2 + \begin{pmatrix} 3 & 2 \\ 1 & 0 \end{pmatrix} x + \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}$ polinomial redusibel dalam $M_{2x2}[x]$.
13. Nyatakan $a(x)$ dalam $b(x)$, $q(x)$ dan $r(x)$ sehingga
$$a(x) = b(x)\, q(x) + r(x)$$
jika $a(x) = x^3 + 5x^2 + x + 1$ dan b(x) = 2 x + 3 dan koefisien-koefisien polinomial dalam Z_6.
14. Nyatakan $a(x)$ dalam $b(x)$, $q(x)$ dan $r(x)$ sehingga
$$a(x) = b(x)\, q(x) + r(x)$$
jika $a(x) = x^3 + 5x^2 + x + 1$ dan b(x) = 2 x + 3 dan koefisien koefisien polinomial dalam Z_7.
15. a. Berapa banyak polinomial derajat 2 dalam $Z_n[x]$?
    b. Jika m bilangan bulat positif, berapa banyak polinomial derajat m dalam $Z_n[x]$?

***

BAB XVI
RING KUOSEN DARI RING POLINOMIAL

Polinomial irredusibel dalam suatu ring polinomial dapat dianalogikan dengan bilangan prima. Di samping itu dalam himpunan bilangan $\boldsymbol{Z}$ setiap ideal merupakan ideal utama (m). Dalam bab ini akan dibahas untuk kelas ring manakah dari koefisien-koefisien dari polinomial yang berada dalam A sehingga setiap ideal dalam $A[x]$ merupakan ideal utama? Sifat yang tertulis dalam teorema ini sangat penting dalam pembahasan selanjutnya.

Teorema XVI.1

Jika diketahui F field maka setiap ideal dalam $F[x]$ merupakan ideal utama.

Bukti :

Misalkan I ideal dalam $F[x]$.

Kasus 1
Jika I ideal sepele { 0 } maka I = (0).

Kasus 2
Jika I mengandung suatu polinomial konstan c maka terdapatlah c^{-1} dalam F sehingga $c^{-1}\,c = 1$ berada dalam I (karena I ideal).
Akibatnya I mengandung setiap polinomial yang kelipatan dari 1 sehingga $I = F = (1)$.

Kasus 3
Misalkan I tidak sepele dan tidak mengandung konstanta yang tidak nol.
Akibatnya I mengandung paling sedikit polinomial berderajat positif.
Misalkan $b(x)$ polinomial berderajat terkecil dalam ideal I.
Ideal I mengandung ideal ($b(x)$).
Akan ditunjukkan bahwa ($b(x)$) mengandung I.

Misalkan $a(x)$ dan $b(x)$ dalam $F(x)$ maka terdapatlah dengan tunggal $q(x)$ dan $r(x)$ dalam $F(x)$ sehingga $a(x) = b(x)\ q(x) + r(x)$ dengan derajat ($r(x)$) < derajat ($b(x)$).
Akibatnya $r(x) = a(x) - b(x)\ q(x)$.
Karena $b(x)$ dalam I maka dengan mengingat I ideal diperoleh $b(x)\ q(x)$ dalam I sehingga $r(x)$ dalam I.
Karena $b(x)$ merupakan polinomial berderajat terkecil dalam I maka $r(x)$ haruslah merupakan polinomial konstan dan dengan mengingat anggapan bahwa I tidak mengandung polinomial konstan yang tidak nol maka $r(x) = 0$.
Akibatnya $a(x) = b(x)\ q(x)$ untuk suatu $q(x)$ dalam $F(x)$.
Berarti I termuat dalam ($b(x)$).

Contoh XVI.1

Diketahui ring $R[x]$ dan ideal

$$(x^2 + 1) = \{ f(x)\ (x^2 + 1) \mid f(x) \text{ dalam } R[x] \}$$

Akan ditentukan sifat-sifat dari $R[x] / (x^2 + 1)$.
Karena R ring komutatif dan mempunyai elemen satuan maka $R[x]$ juga ring komutatif dengan satuan $1x^0$. Karena $x^2 + 1$ tidak mempunyai akar real maka $x^2 + 1$ irredusibel dalam $R[x]$ sehingga $x^2 + 1$ tidak mempunyai faktor dengan derajat satu.
Misalkan J sebarang ideal dalam R[x] yang memuat $(x^2 + 1)$ secara sejati.
Dengan mengingat teorema maka $J = (p(x))$ untuk suatu $p(x)$.
Karena $x^2 + 1$ dalam J maka $(x^2 + 1) = p(x)\ q(x)$ untuk suatu $q(x)$ dalam $R[x]$.
Karena $x^2 + 1$ irredusibel dalam $R[x]$ maka $p(x)$ atau $q(x)$ suatu konstan.
Jika $q(x)$ konstan maka $J = (x^2 + 1)$ sehingga hal ini kontradiksi dengan kenyatan bahwa J mengandung $x^2 + 1$ secara sejati.
Akibatnya $p(x)$ merupakan suatu polinomial konstan dan tidak nol karena J mengandung $x^2 + 1$ secara sejati.

Dengan mengingat alasan pada kasus 2 Teorema XVI.1 diperoleh bahwa $J = R[x]$.
Bila Teorema XIII.3 (4) digunakan maka diperoleh $R[x]/(x^2 + 1)$ field. Karena $R[x]/(x^2 + 1)$ field maka juga merupakan daerah integral.

Sifat yang terdapat dalam teorema tersebut di atas tidak dipenuhi bila A hanya merupakan daerah integral dan bukan field. Hal itu berarti dalam $A[x]$ dengan A daerah integral yang bukan field maka $A[x]$ akan mengandung suatu ideal yang bukan ideal utama.

Teorema XVI.2

Jika F field dan polinomial $p(x)$ irredusibel dalam $F[x]$ maka ring kuosen $F[x]$ / ($p(x)$) merupakan field.

Bukti :

Untuk latihan.

Teorema berikut ini memperlihatkan hubungan yang erat antara ring kuosen dan homomorfisma ring. Teorema ini analog dengan teorema fundamental dari homomorfisma grup.

Teorema XVI.3 (*Teorema fundamental dari homomorfisma ring*)

Jika diketahui $f : A \rightarrow B$ homomorfisma ring dengan peta $f(A)$ dan inti K maka ring kuosen A/K isomorfisma dengan $f(A)$.

Bukti :

Karena inti K dari homomorfisma ring ideal maka ring kuosen A/I terdefinisikan.
Karena K juga inti dari homomorfisma grup $f : < A, + > \rightarrow < B, + >$ maka dengan mendefinisikan pemetaan

$$g : A/K \rightarrow f(A)$$

dengan $g(a+I)=f(a)$ dan dengan mengingat Teorema IX.8, g merupakan fungsi yang injektif, surjektif dan mengawetkan operasi +. Karena

$$g(\,(a+I)\,(b+I)\,) = g\,(ab+I)$$
$$= f(ab)$$
$$= f(a)\,f(b)$$
$$= g(a+I)\,g(b+I)$$

maka g mengawetkan operasi perkalian sehingga g merupakan isomorfisma ring.

Contoh XVI.2

Himpunan bilangan rasional $\boldsymbol{Q}$ merupakan field dan polinomial $q(x)=x^2-2$ irredusibel atas $\boldsymbol{Q}$ maka ring kuosen $\boldsymbol{Q}[x]/(x^2-2)$ merupakan field. Field tersebut akan isomorfis dengan

$$Q(\sqrt{2}) = \{\, a + b\sqrt{2} \mid a, b \in Q \,\}.$$

Contoh XVI.3

Dalam contoh ini akan diperlihatkan bahwa $\boldsymbol{R}[x]/(x^2+1)$ isomorfisma dengan himpunan bilangan kompleks $\boldsymbol{C}$.

Untuk menggunakan teorema di atas diperlukan suatu fungsi untuk mendefinisikan suatu homomorfisma ring dengan daerah asal $\boldsymbol{R}[x]$ dan intinya adalah (x^2+1).

Didefinisikan suatu pemetaan $f_i : \boldsymbol{R}[x] \rightarrow \boldsymbol{C}$ dengan $f_i(\,p(x)\,) = p(i)$.

Jelas bahwa peta dari f_i adalah $\boldsymbol{C}$?

Inti dari f_i adalah $\{\, f_i(x) \mid f_i(i) = 0 \,\}$ meliputi x^2+1 dan oleh karena itu mengandung (x^2+1).

Karena sebarang ideal yang mengandung (x^2+1) secara sejati adalah $\boldsymbol{R}[x]$ dan karena $K \neq \boldsymbol{R}[x]$ maka K haruslah sama dengan (x^2+1).

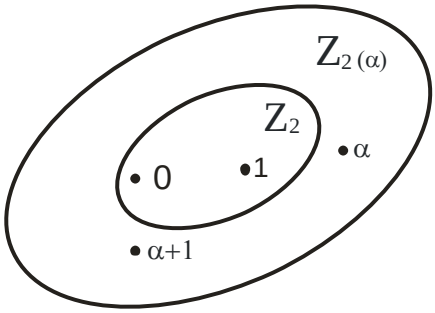
Dengan menggunakan teorema fundamental homomorfisma ring diperoleh $\boldsymbol{R}[x]/K = \mathrm{Im}(f_i)$ atau $\boldsymbol{R}[x] / (x^2+1)$.

Contoh XVI.4

Himpunan bilangan rasional Z_2 merupakan field dan polinomial $q(x) = x^2+x+1$ irredusibel atas Z_2 sehingga ring kuosen $Z_2[x]/(\,x^2+x+1\,)$ merupakan field. Field tersebut akan isomorfis dengan

$$Z_2(\alpha) = \{\, a + b\,\alpha \mid a, b \in Z_2 \,\}$$

yaitu field yang mempunyai 4 elemen.



Contoh XVI.5

Misalkan diketahui polinomial monik irredusibel

$$p(x) = x^2 + 2x + 2$$

atas field Z_3. Akan ditentukan semua elemen dari field $Z_3[x]/(p(x))$ dan pada saat yang sama mengkonstruksikan tabel penjumlahan dan perkalian dari field ini.

Misalkan $P = (p(x))$ dan $\alpha = x + P$ dalam $Z_3[x]/(p(x))$.

Elemen-elemen dalam $Z_3[x]/(p(x))$ adalah

$$0 = 0 + P, 1 = 1 + P, 2 = 2 + P$$

dan α dan seterusnya sehingga diperoleh

$$\{ 0, 1, 2, \alpha, \alpha + 1, \alpha + 2, 2\alpha, 2\alpha + 1, 2\alpha + 2 \}.$$

Tabel penjumlahan dalam $Z_3[x]/(p(x))$ dapat dinyatakan sebagai berikut :

+	0	1	2	α	α + 1	α + 2	2α	2α + 1	2α + 2
0	0	1	2	α	α + 1	α + 2	2α	2α + 1	2α + 2
1	1	2	0	α + 1	α + 2	2α	2α + 1	2α + 2	2α
2	2	0	α + 1	α + 2	2α	2α + 1	2α + 2	2α	2α + 1
α	α	α + 1	α + 2	2α	2α + 1	2α + 2	2α	2α + 1	2
α + 1	α + 1	α + 2	2α	2α + 1	2α + 2	2α	2α + 1	2α + 2	0
α + 2	α + 2	2α	2α + 1	2α + 2	2α	2α + 1	2α + 2	0	1
2α	2α	2α + 1	2α + 2	2α	2α + 1	2α + 2	0	1	α + 2
2α + 1	2α + 1	2α + 2	2α	2α + 1	2α + 2	0	1	α + 2	α
2α + 2	2α + 2	2α	2α + 1	2α + 2	0	1	α + 2	α	α + 1

Untuk mendapatkan tabel perkalian, digunakan kenyataan bahwa α merupakan akar polinomial $p(x)$ sehingga $p(\alpha) = 0$ atau

$$\alpha^2 + 2\alpha + 2 = 0$$

atau $\alpha^2 = -2\alpha - 2 = \alpha + 1$. Sebagai gambaran diperoleh

$$(2\alpha + 1)(\alpha + 2) = 2\alpha^2 + 2\alpha + 2$$
$$= 2(\alpha + 1) + 2\alpha + 2 = 2\alpha + 2 + 2\alpha + 2 = \alpha + 1.$$

sehingga diperoleh tabel

.	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
2	0	2	1	2α	$2\alpha+2$	$2\alpha+1$	α	$\alpha+2$	$\alpha+1$
α	0	α	2α	$\alpha+1$	$2\alpha+1$	1	$2\alpha+2$	2	$\alpha+2$
$\alpha+1$	0	$\alpha+1$	$2\alpha+2$	$2\alpha+1$	2	α	$\alpha+2$	2α	1
$\alpha+2$	0	$\alpha+2$	$2\alpha+1$	1	α	$2\alpha+2$	2	$\alpha+1$	2α
2α	0	2α	α	$2\alpha+2$	$\alpha+2$	2	$\alpha+1$	1	$2\alpha+1$
$2\alpha+1$	0	$2\alpha+1$	$\alpha+2$	2	2α	$\alpha+1$	1	$2\alpha+2$	α
$2\alpha+2$	0	$2\alpha+2$	$\alpha+1$	$\alpha+2$	1	2α	$2\alpha+1$	α	2

Contoh XVI.6

Misalkan diketahui polinomial redusibel

$$p(x) = x^2 + 1$$

atas field Z_2.

Akan ditentukan semua elemen dari ring kuosen $Z_2[x]/(p(x))$ dan pada saat yang sama mengkonstruksikan tabel penjumlahan dan perkalian dari ring kuosen ini.

Misalkan $P = (p(x))$ dan $\alpha = x + P$ dalam $Z_2[x]/(p(x))$.

Elemen-elemen dalam $Z_2[x]/(p(x))$ adalah

$$\{0, 1, \alpha, \alpha + 1\}.$$

Tabel operasi penjumlahan dalam $Z_2[x]/(p(x))$ adalah sebagai berikut

+	0	1	α	α + 1
0	0	1	α	α + 1
1	1	0	α + 1	α
α	α	α + 1	0	1
α + 1	α + 1	α	1	0

Untuk membuat tabel operasi perkalian dalam $Z_2[x]/(\ p(x)\ )$ dengan memperhatikan kenyataan bahwa $p(\alpha)=0$ atau $\alpha^2+1=0$ atau

$$\alpha^2 = -1 = 1$$

sehingga diperoleh tabel perkalian sebagai berikut :

.	0	1	α	α + 1
0	0	0	0	0
1	0	1	α	α + 1
α	0	α	1	α + 1
α + 1	0	α + 1	α + 1	0

Hal itu berarti $Z_2[x]/(\ p(x)\ )$ bukan merupakan suatu field tetapi hanyalah ring kumutatif dengan elemen satuan.

Contoh XVI.7

Dalam $Z_5(\alpha)$ akan dicari invers perkalian dari elemen $\alpha^2 + 3\alpha + 1$ dalam field $Z_5(\alpha)$.

Polinomial $f(x) = x^2 + 3x + 1$ dan merupakan prima relatif atas $Z_5[x]$ sehingga ada $s(x)$ dan $t(x)$ dalam sehingga

$$f(x)s(x)+p(x)t(x)=1.$$

Karena $p(\alpha) = 0$ maka $f(\alpha)\ s(\alpha) = 1$ sehingga

$$(\alpha^2+3\alpha+1)^{-1}=\big(f(\alpha)\big)^{-1}=s(\alpha).$$

Dalam upaya mencari $s(x)$ dan $t(x)$ dapat digunakan algoritma Euclid

$$p(x) = f(x)\ (x + 4) + x + 3$$

$$f(x) = (x + 3)x + 1$$

$$1 = f(x) - x(x + 3)$$

$$1 = f(x) - x(p(x) - f(x)(x+4))$$
$$1 = f(x)[1 + x(x+4)] + p(x)(-x)$$

sehingga diperoleh $s(x) = x^2 + 4x + 1$ dan $t(x) = -x$.

Oleh karena itu,

$$(\alpha^2 + 3\alpha + 1)^{-1} = s(\alpha) = \alpha^2 + 4\alpha + 1$$

sehingga

$$(\alpha^2 + 3\alpha + 1)(\alpha^2 + 4\alpha + 1) = 1$$

dalam $Z_5(\alpha)$.

Latihan

1. Apakah 43 + (5) dan - 12 + (5) merupakan elemen yang sama dalam ring kuosen Z_{60} /(5) ?
2. Apakah 197 + (3) dan 84 + (3) merupakan elemen yang sama dalam ring kuosen $\boldsymbol{Z}$/(3) ?
3. Apakah 87 + (11) dan - 45 + (11) merupakan elemen yang sama dalam ring kuosen $\boldsymbol{Z}$/(11) ?
4. Apakah $x^3 + (x^2-1)$ dan $x^3 + (x^2-1)$ merupakan elemen yang sama dalam ring kuosen $\boldsymbol{Z}[x]/(x^2-1)$?
5. Apakah $x^3 + (x^2+1)$ dan $x + (x^2+1)$ merupakan elemen yang sama dalam ring kuosen $\boldsymbol{R}[x]/(x^2+1)$?
6. Hitunglah operasi dalam ring kuosen Z_{60}/ (5) berikut ini :
   a. [43 + (5)] + [7 + (5)].
   b. [2 + (5)]^5.
   c. [- 3 + (5)] + [14 + (5)].
   d. [2 + (5)]$^{-1}$.
7. Berikan sifat-sifat dari ring kuosen $Z_5[x] / (x^2 + 1)$.
   Berapa banyak elemen yang dimilikinya?
8. Tunjukkan bahwa $Z_5[x] / (x^2 + 1)$ mempunyai 4 elemen dan berikan sifat-sifatnya.
9. a. Tunjukkan bahwa $x^2 + 1$ irredusibel atas $Z_3[x]$.
   b. Berikan sifat-sifat dari $Z_3/(x^2 + 1)$.
   c. Tunjukkan bahwa $Z_3[x]/(x^2 + 1)$ mempunyai tepat 9 elemen.
10. Berikan sifat-sifat dari $Z[x]/(x^2)$.
11. Tunjukkan bahwa $(x^2 + 1)$ merupakan ideal prima tetapi bukan ideal maksimal dalam $Z[x]$ dan kemudian gunakan Teorema XIII.3 untuk memberikan sifat-sifat dari ring kuosen
    $$Z[x] / (x^2 + 1).$$
12. Tunjukkan bahwa jika A ring komutatif dengan elemen satuan maka setiap ideal maksimal M dalam A merupakan ideal prima.
13. Diketahui A daerah integral yang bukan field dan b suatu elemen tidak nol dalam A dan b mempunyai invers.
    Dibentuk $I = \{ b f(x) + x g(x) \mid f(x), g(x)$ dalam $A[x] \}$.

a. Buktikan bahwa I ideal dalam $A[x]$.

b. Buktikan bahwa I bukan ideal utama.

14. Tunjukkan bahwa jika $f(x)$ polinomial redusibel atas field A maka $A[x]/(f(x))$ mengandung pembagi nol.

15. Hitunglah operasi dalam $Z_5[x]/(x^2+1)$ berikut ini :

a. $[x+(x^2+1)]^2$.

b. $[x+2+(x^2+1)][2x+1+(x^2+1)]$.

c. $[x+(x^2+1)][-x+(x^2+1)]$.

d. $[x^3+(x^2+1)][x^3+1+(x^2+1)]$.

***

BAB XVII
FIELD PERLUASAN

Sejarah aljabar mencatat bahwa sistim bilangan baru dibuat dan dikonstruksikan bertujuan untuk menyimpan akar-akar dari polinomial tertentu. Sebagai contoh, polinomial $2x + 4$ tidak mempunyai akar dalam sistim bilangan positif N tetapi polinomial mempunyai akar dalam sistim bilangan bulat $\boldsymbol{Z}$. Polinomial $2x + 3$ tidak mempunyai akar dalam Z tetapi mempunyai akar bila sistim bilangan rasional $\boldsymbol{Q}$ dikonstruksikan. Polinomial $x^2 - 2$ tidak mempunyai akar bila sistim bilangan rasional $\boldsymbol{Q}(\sqrt{2})$ dapat digunakan untuk mengkonstruksikan sistim $\boldsymbol{Q}(\sqrt{2})$. Ternyata sistim bilangan kompleks $\boldsymbol{C}$ belum dikonstruksikan sampai abad ke 18 dan juga beberapa waktu sesudah polinomial $x^2 + 1$ mempunyai akar.

Field $\boldsymbol{Q}(\sqrt{2})$ mengandung $\boldsymbol{Q}$ sebagai field bagian dan demikian juga field $\boldsymbol{C} = \boldsymbol{R}(i)$ mengandung $\boldsymbol{R}$ sebagai field bagian. Field $\boldsymbol{Q}(\sqrt{2})$ dan $\boldsymbol{C}$ merupakan contoh dari field perluasan (*extension field*) yaitu field yang dikonstruksikan dan mengandung suatu field yang diberikan sebagai suatu field bagian.

Contoh lain dari field perluasan adalah $Z_2[\alpha]$ dengan α dibuat sehingga $x^2 + x + 1$ mempunyai akar atas Z_2. Dalam bab ini akan dijelaskan bagaimana α dapat dikonstruksikan. Pengkonstruksian dan perumumannya merupakan hal penting dalam teori field.

Teorema XVII.1

Jika F field dan $p(x)$ polinomial derajat lebih dari atau sama dengan 2 dan irredusibel atas F maka terdapatlah field perluasan E dari F yang mengandung suatu akar dari $p(x)$.

Bukti :

Misalkan E ring kuosen $F[x] / (p(x))$.

(1) Dengan mengingat Teorema XVI.2, E merupakan field.

(2) Fungsi $f : F \rightarrow E$ dengan $f(a) = a + (p(x))$ merupakan homomorfisma ring dengan inti $\{ 0 \}$.
Oleh karena itu Im(f) (yang terdiri dari semua koset-koset dari polinomial konstan) merupakan suatu field yang isomorfis dengan F.
Akibatnya E merupakan suatu field perluasan dari F.
Untuk keseimbangan bukti diidentifikasikan bahwa koset

$$a + (p(x))$$

dalam E berkaitan dengan a dalam F.

(3) Misalkan a adalah koset $x + (p(x))$.
Akan ditunjukkan bahwa α akar dari $(p(x))$.
Misalkan $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots\ldots + a_1 x + a_0$.
Akibatnya $p(\alpha) = a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots\ldots + a_1 \alpha + a_0$

$$\begin{aligned} &= a_n (x + (p(x))^n + \ldots\ldots + a_1 (x + (p(x))) + a_0 \\ &= a_n (x^n + (p(x))) + \ldots\ldots + a_1 x + (p(x)) + a_0 \\ &= (a_n x^n + \ldots\ldots + a_1 x + a_0) + (p(x)) \\ &= p(x) + (p(x)) \\ &= 0 + (p(x)). \end{aligned}$$

Berarti $p(\alpha)$ sama dengan elemen nol dari E dan α merupakan akar dari $p(x)$.

Bila diberikan sebarang daerah integral D, suatu field

$$Q_D = \{ a/b \mid a, b \text{ dalam } A \text{ dengan } b \neq 0 \}$$

dapat dikonstruksikan dan Q_D mengandung D sebagai daerah integral bagian. Teorema XVI.1 menjamin bahwa suatu perluasan dari Q_D mengandung suatu akar untuk semua polinomial dalam $D[x]$ yang diberikan. Hal ini tidak bisa dilakukan jika D bukan daerah integral. Sebagai contoh, dimisalkan terdapat suatu perluasan E dari Z_6 sehingga $p(x) = 2x + 3$ mempunyai akar α. Akibatnya $2\alpha + 3 = 0$ dan dengan menggandakan kedua ruas dengan 3 diperoleh

$$0\ \alpha + 3 \,.\, 3 = 0$$

atau 3 = 0. Hal ini berarti terdapat suatu kontradiksi.

Contoh XVII.1

Akan dikonstruksikan suatu field perluasan dari $\boldsymbol{Q}$ yang mengandung satu akar dari polinomial irredusibel $p(x) = x^3 - 2$ dalam $\boldsymbol{Q}[x]$.
Dengan menggunakan Teorema XVI.1 maka diperoleh field

$$E = \boldsymbol{Q}[x] \,/\, (x^3 - 2)$$

mengandung $\boldsymbol{Q}$ dan berbentuk $\{ a + (x^3 - 2) \mid a$ dalam $\boldsymbol{Q} \}$ dan

$$s = x + (x^3 - 2)$$

merupakan akar dari $p(x)$.

Dalam hal ini E isomorfis dengan field bagian $Q(\sqrt[3]{2})$ dari $\boldsymbol{R}$ dengan

$$\boldsymbol{Q}(\sqrt[3]{2}) = \{ a + b\,(\sqrt[3]{2}) + c\,(\sqrt[3]{2})^2 \mid a, b, c \text{ dalam } \boldsymbol{Q} \}.$$

Teorema XVII.2

Jika $p(x)$ polinomial irredusibel derajat $n > 1$ atas F dan $\alpha = x + (p(x))$ dan $c + (p(x))$ dengan c berlaku untuk semua c dalam F maka field perluasan $E = F[x] \,/\, (p(x))$ terdiri dari semua elemen berbentuk $c_{n-1}\ \alpha^{n-1} + \ldots\ldots + c_1\ \alpha + c_0$ dengan semua c_j dalam F.

Bukti :

Untuk sebarang elemen $f(x) + (p(x))$ dari E, $f(x)$ dapat ditulis sebagai

$$f(x) = p(x)\, q(x) + r(x)$$

dengan derajat $(r(x)) <$ derajat $(p(x)) = n$.
Akibatnya

$$f(x) + (p(x)) = [\, p(x)\, q(x) + r(x) \,] + (p(x))$$
$$= r(x) + (p(x))$$

karena $[\, p(x)\, q(x) + r(x) \,] - r(x) = p(x)\, q(x)$ dalam $(p(x))$.
Polinomial $r(x)$ ditulis sebagai $r(x) = c_{n-1}\ x^{n-1} + \ldots\ldots + c_1\ x + c_0$ dan terlihat bahwa elemen-elemen E mereduksi menjadi berbentuk

$$c_{n-1}\ x^{n-1} + \ldots\ldots + c_1\ x + c_0 + (p(x)).$$

Karena $\alpha = x + (p(x))$ maka mudah dibuktikan bahwa

$$c_{n-1}\, x^{n-1} + \ldots\ldots + c_1\, x + c_0 + (\, p(x)\,)$$

dapat ditulis sebagai $c_{n-1}\ \alpha^{n-1} + \ldots\ldots + c_1 + \alpha + c_0$ dengan c_i diidentifikasi-kan dengan $c_i + (\, p(x)\,)$.

Dengan menggunakan dasar Teorema VII.2 maka dapat digunakan notasi $F(\alpha)$ dengan

$$F(\alpha) = \{\, c_{n-1}\ \alpha^{n-1} + \ldots\ldots + c_1\ \alpha + c_0 \mid c_i \in F \,\}$$

untuk suatu field perluasan yang mengandung F dan suatu akar α dari $p(x)$. Dalam hal ini, $F(\alpha)$ dinamakan perluasan sederhana (*simple extension*) dari F. Proses ini dapat diulangi dan dibentuk $(F(\alpha))\ (\beta) = F(\alpha, \beta)$ yaitu suatu perluasan berulang (*iterated extension*) dari F. Elemen s dikatakan aljabar atas F (*algebraic*) karena memenuhi

$$= s^4 + (s + 1) + s^2 + 1 = s^4 + s^2 + s$$
$$= s\,(s^3 + s + 1)$$
$$= 0.$$

Berarti s^2 merupakan akar dan dengan cara *trial and error* diperoleh juga $s^2 + s$ merupakan akar dari $p(x)$ yang lain. Jadi semua akar-akar s, s^2 dan $s^2 + s$ dari $p(x)$ terletak dalam E.

Berdasarkan contoh di atas terlihat bahwa suatu polinomial dengan koefisien-koefisien dalam suatu field F mungkin difaktorkan atau tidak mungkin difaktorkan secara lengkap yaitu sebagai hasil kali dari $x - u$ dalam $E = F[x] / (\, p(x)\,)$. Jika tidak maka diperlukan suatu proses yang berulang untuk mendapatkan semua akar-akarnya sehingga diperoleh suatu cara untuk memfaktorkan $p(x)$ secara lengkap ke dalam suatu perluasan berulang dari F.

Definisi XVII.1

Diketahui F field dan polinomial $p(x)$ berderajat 2 atau lebih dengan koefisien-koefisien dalam F.
Suatu field perluasan E dari F dikatakan field pemisah (*splitting field*) untuk $p(x)$ asalkan $p(x)$ dapat difaktorkan secara lengkap atas E dan $p(x)$

tidak dapat difaktorkan secara lengkap ke dalam sebarang field bagian sejati dari E.

Sebagai contoh, field $E=Z_2[x]/(x^3 + x + 1)$ yang dikonstruksikan dalam contoh merupakan field pemisah untuk $x^3 + x + 1$ dan tidak ada field bagian yang sejati yang dapat memfaktorkan secara lengkap. Field E ini juga dapat dituliskan sebagai $Z_2(\alpha)$. Secara umum, field pemisah untuk suatu polinomial $p(x)$ atas F dapat selalu dinyatakan sebagai

$$F(\alpha_1, \alpha_2, \alpha_3, ..., \alpha_k)$$

dengan α_i untuk suatu himpunan bagian dari akar-akar dari $p(x)$.

Definisi XVIII.3

Diketahui A ring.

1. Jika tidak ada bilangan positif m yang memenuhi $m.a = 0$ untuk semua a dalam A maka dikatakan A mempunyai karakteristik (*characteristic*) 0.
2. Jika ada dan misalkan k bilangan bulat positif terkecil sehingga $k.a = 0$ untuk semua a dalam A maka dikatakan A mempunyai karakteristik k.

Contoh XVII.3

1. Karena $6 . a = 0$ untuk semua a dalam Z_6 dan 6 merupakan bilangan bulat positif terkecil yang mempunyai sifat itu maka Z_6 mempunyai karakteristik 6.
2. Karena $4.2k = 0$ $k = 0$ dalam $2Z_8=\{ 0, 2, 4, 6 \}$ maka $2Z_8$ mempunyai karakteristik 4.

Teorema XVII.4

1. Jika A ring berhingga dengan n elemen maka karakteristiknya merupakan pembagi n.
2. Diketahui A ring dengan elemen satuan 1.
   Ring A mempunyai karakteristik tidak nol jika dan hanya jika 1 mempunyai orde m dalam grup $< A, + >$.

3. Jika suatu daerah integral mempunyai karakteristik k maka k bilangan prima.

Bukti :

(1) Bila A mempunyai n elemen maka orde dari setiap angota dari grup $< A, + >$ merupakan pembagi n.
Akibatnya $n \,.\, a = 0$ untuk semua a dalam A.
Misalkan k karakteristik dari A yaitu bilangan bulat positif terkecil sehingga $k \,.\, a = 0$ untuk semua a dalam A.
Jika k bukan pembagi n maka dapat ditemukan q dan r sehingga $n = kq + r$ dengan $0 < r < k$.
Dengan mengingat definisi k maka

$$n \,.\, a = (\, kq + r \,) \,.\, a = q \,.\, (\, k \,.\, a \,) + r \,.\, a = q \,.\, 0 + r \,.\, a$$

haruslah tidak nol untuk suatu a.
Berarti terjadi suatu kontradiksi dan diperoleh k haruslah membagi n.

(2) Misalkan k bilangan positif sehingga $k.\, 1 = 0$.
Sifat ini berlaku,

$$k \,.\, a = a + a + \ldots + a = (\, 1 + 1 + \ldots + 1 \,)\, a = (\, k \,.\, 1 \,)\, a = 0\, a = 0$$

untuk semua a dalam A.
Oleh karena itu, A mempunyai karakterisrik tidak nol m jika dan hanya jika $m \,.\, 1 = 0$ dan tidak ada bilangan positif yang lebih kecil yang mempunyai sifat ini.
Berarti hal itu dipenuhi jika dan hanya jika 1 mempunyai orde berhingga m dalam grup terhadap penjumlahan.

(3) Misalkan D daerah integral dengan karakteristik tidak nol k.
Dengan menggunakan sifat (2), maka elemen satuan 1 dalam D mempunyai orde k dalam $< D, + >$.
Jika k mempunyai suatu faktorisasi sejati $k = r \,.\, s$ maka diperoleh

$$(r \,.1)\, (s.1) = (1 + 1 + \ldots + 1)\, (1 + 1 + \ldots + 1)$$

$$\underset{r \text{ suku}}{} \qquad \underset{s \text{ suku}}{}$$

$$= (1 + 1 + \ldots + 1)\, 1 + (1 + 1 + \ldots)\, 1 + \ldots + (1 + 1 + \ldots + 1)\, 1$$

$$= \underset{rs \text{ suku}}{1 + 1 + \ldots + 1}$$

$$= (rs) \,.\, 1$$

$$= k \,.\, 1 = 0.$$

Hal itu berarti $r \,.\, 1$ dan $s \,.\, 1$ yang tidak nol (karena $0 < r < k$ dan $0<s<k$) dan hasil perkaliannya nol sehingga terdapat kontradiksi karena D daerah integral.
Terbukti bahwa k haruslah prima.

Teorema berikut ini menyatakan kaitan antara karakteristik dari suatu field dan konsep field perluasan.

Teorema XVII.4

1. Jika F field dengan karakteristik p yang tidak nol maka F suatu field perluasan dari Z_p .
2. Sebarang field dengan karakteristik nol merupakan suatu perluasan $\boldsymbol{Q}$.

Bukti :

(1) Teorema menjamin bahwa p prima dan elemen satuan dalam F yaitu 1 mempunyai orde p di bawah operasi perkalian.
Grup bagian (1) dari F terhadap operasi penjumlahan adalah
{ 0, 1, 2, 1, 3, 1, ……, (p-1), 1}.
Dapat ditunjukkan dengan mudah bahwa fungsi $f : \boldsymbol{Z} \rightarrow F$ dengan $f(k) = k \,.\, 1$ mengawetkan operasi penjumlahan dan perkalian dan mempunyai peta $\text{Im}(f) = (1)$ dan $\text{Ker}(f) = (p)$.
Dengan menggunakan teorema fundamental homomorfisma ring diperoleh bahwa peta dari f yaitu $\text{Im}(f) = (1)$ isomorfis dengan $Z/(p)$ (yang isomorfis dengan Z_p). Oleh karena itu, F mengandung suatu field bagian (1) yang isomorfis dengan Z_p dan dengan kata lain F merupakan field perluasan dari Z_p.

(2) Dalam kasus ini, 1 membangun suatu grup bagian terhadap operasi penjumlahan Z' dari field F dan Z' isomorfis dengan ring Z.
Himpunan $\{ a\, b^{-1} \mid a, b$ dalam Z′ dengan $b \neq 0 \}$ membentuk suatu field bagian dari F yang isomorfis dengan Q.
(lanjutannya untuk latihan).

Misalkan F sebarang field berhingga. Field F haruslah mempunyai karakteristik prima p dan oleh karena itu suatu perluasan dari Z_p. Suatu field berhingga F haruslah mempunyai p^n elemen untuk suatu p prima dan suatu bilangan bulat positif n. Sebagai contoh, field $Z_2[x]/(x^2 + x + 1)$ merupakan field dengan $2^2 = 4$ elemen dan field $Z_2[x]/(x^3 + x + 1)$ merupakan field dengan $2^2 = 8$ elemen. Sebaliknya untuk setiap bilangan bulat positif n dan prima p terdapat suatu field yang mengandung tepat p^n elemen.

Contoh XVII.1

Polinomial $p(x) = x^3 + 2x^2 + 4x + 2$irredusibel atas Z_5 karena

$p(0)=2,\ p(1)=4,\ p(2)=1,\ p(3)=4$ dan $p(4) = 4$.

Field perluasan $Z_5(\alpha) = \{ a + b\alpha + c\alpha^2 \mid a, b, c \in Z_5 \}$ mempunyai $5^3 = 125$ elemen dan mempunyai sifat bahwa α merupakan akar dari polinomial $p(x)$ sehingga $p(\alpha) = 0$. Akibatnya

$$\alpha^3 + 2\alpha^2 + 4\alpha + 2 = 0$$

$$\alpha^3 = -2\alpha^2 - 4\alpha - 2$$

$$= 3\alpha^2 + \alpha + 3$$

dan

$$\alpha^4 = \alpha(\alpha^3)$$

$$= \alpha(3\alpha^2 + \alpha + 3)$$

$$= 3\alpha^3 + \alpha^2 + 3\alpha$$

$$= 3(3\alpha^2 + \alpha + 3) + \alpha^2 + 3\alpha$$

$$= 9\alpha^2 + 3\alpha + 9 + \alpha^2 + 3\alpha$$

$$= \alpha + 4.$$

Dengan hasil tersebut diperoleh

$$(a_0 + a_1\alpha + a_2\alpha^2)(b_0 + b_1\alpha + b_2\alpha^2) = a_0 b_0 + (a_0 b_1 + a_1 b_0)\alpha$$

$$+ (a_0 b_2 + a_1 b_1 + a_2 b_0)\alpha^2 + (a_1 b_2 + a_2 b_1)\alpha^3 + a_2 b_2 \alpha^4 .$$

$$= a_0 b_0 + (a_0 b_1 + a_1 b_0)\alpha + (a_0 b_2 + a_1 b_1 + a_2 b_0)\alpha^2$$

$$+ (a_1 b_2 + a_2 b_1)(3\alpha^2 + \alpha + 3) + a_2 b_2 (\alpha + 4) .$$

$$= a_0 b_0 + (a_0 b_1 + a_1 b_0)\alpha + (a_0 b_2 + a_1 b_1 + a_2 b_0)\alpha^2$$

$$+ (a_1 b_2 + a_2 b_1)(3\alpha^2 + \alpha + 3) + a_2 b_2(\alpha + 4).$$

$$= a_0 b_0 + 3 a_1 b_2 + 3 a_2 b_1 + 4 a_2 b_2 + (a_0 b_1 + a_1 b_0 + a_1 b_2 + a_2 b_1 + a_2 b_2)\alpha$$

$$+ (a_0 b_2 + a_1 b_1 + a_2 b_0 + 3 a_1 b_2 + 3 a_2 b_1)\alpha^2.$$

Latihan

1. Diketahui field $Z_2(\alpha) = Z_2[x] / (x^2 + x + 1)$.
   a. Buktikan bahwa $\alpha . \alpha = \alpha + 1$.
   b. Buktikan bahwa $(\alpha + 1)\,\alpha = \alpha\,(\alpha + 1) = 1$.
2. Misalkan s adalah akar polinomial $x^3 + x + 1$ atas Z_2.
   a. Buktikan bahwa ketika $x^3 + x + 1$ dibagi oleh $x - s$, kuosennya adalah
   $$q(x) = x^2 + s\,x + (s^2 + 1).$$
   b. Buktikan dengan substitusi secara langsung bahwa $q(s^2 + s) = 0$.
3. a. Kostruksikan suatu field $Z_5[s]$ yang mengandung suatu akar s dari polinomial $x^2 + x + 2$ atas Z_5.
   b. Berapa banyak elemen $Z_5(s)$? Bagaimana menuliskan elemen-elemennya?
   c. Tentukan suatu elemen yang membangun grup $[Z_5(s)]^*$.
4. Ulangi soal 3 untuk polinomial $x^2 + x + 3$ atas Z_5.
5. Ulangi soal 3 untuk polinomial $x^2 + 2$ atas Z_5.
6. Tentukan hasil dari pangkat berikut ini dalam $Z_2(\beta)$ dengan akar dari $x^3 + x^2 + 1$ atas Z_2.
   a. $\beta^2(\beta + 1)$. b. $(\beta^2 + \beta)(\beta^2 + 1)$. c. β^{-3}.
   d. β^5. e. β^{-1}. f. β^{777}.
7. Tunjukkan bahwa jika u adalah akar dari $x^2 + x + 2$ atas Z_3 maka u membangun grup $[Z_3(u)]^*$.
8. Jika s akar dari $x^3 + x + 1$ atas Z_2 maka $s + 1, s^2 + 1$ dan $s^2 + s + 1$ merupakan akar $x^3 + x^2 + 1$.
9. Diketahui $p(x) = x^5 - 2$ suatu polinomial dengan koefisien bilangan rasional. Tentukan field pemisah $Q(u, v)$ untuk $p(x)$.
10. a. Tentukan pembangun dari grup siklik $[Z_2(u)]^*$ dengan u adalah akar dari $x^4 + x + 1$.
    b. Tentukan pembangun dari grup siklik $[Z_2(v)]^*$ dengan v adalah akar dari $x^4 + x^2 + 1$.
11. Buktikan bahwa $Q[x] / (x^3 - 2) \cong Q(\sqrt[3]{2})$.
12. Diketahui F suatu field dengan karakteristik nol dan didefinisikan $f : Q \to F$ dengan aturan $f(a/b) = (a . 1)(b . 1)^{-1}$.

a. Tunjukkan bahwa f terdefinisi dengan baik.
b. Tunjukkan bahwa f homomorfisma ring.
c. Tunjukkan bahwa f injektif dengan menggunakan uji inti (*kernel test*).

13. Diketahui $F = Z_3(u)$ dengan u akar dari $x^2 + 1$ atas Z_3.
    a. Tunjukkan bahwa $p(x) = x^3 + u$ redusibel atas F dan faktor $p(x)$ secara lengkap.
    b. Tunjukkan $q(x) = x^3 + ux + 1$ irredusibel atas F dan konstruksikan suatu field E yang mengandung F dan suatu akar v dari $q(x)$.
14. Tentukan lapangan pemisah untuk $x^4 - 5$ atas Q.
15. Diketahui $F = Z_2(s)$ dengan s akar dari $x^2 + x + 1$.
    Tunjukkan bahwa $q(x) = x^2 + sx + 1$ irredusibel atas F dan konstruksikan suatu field E yang mengandung F dan suatu akar t dari polinomial $q(x)$.

***

BAB XVIII
DAERAH FAKTORISASI TUNGGAL, DAERAH IDEAL UTAMA DAN DAERAH EUCLID

Fenomena yang ditemui dalam himpunan bilangan bulat yang lebih dari atau sama dengan dua dapat difaktorkan sebagai hasil kali bilangan prima mengakibatkan penelitian untuk perumuman dari sifat faktorisasi. Definisi berikut ini digunakan untuk membuat perumuman itu.

Definisi XVIII.1

Misalkan A sebarang ring komuatatif dengan elemen satuan.
Jika a, b dalam A maka a dikatakan membagi b (dan ditulis dengan $a \mid b$) asalkan bahwa $b = a\,q$ untuk suatu q dalam A.
Di samping itu a merupakan faktor dari b.

Teorema XVIII.1

(1) Jika $a \mid b$ dan $a \mid c$ maka $a \mid (b + c)$ dan $a \mid (b - c)$.
(2) Jika $a \mid b$ dan $b \mid c$ maka $a \mid c$.

Bukti :

Untuk latihan.

Definisi XVIII.2

Diketahui $a = a(x)$ dan $b = b(x)$ elemen $F[x]$ yang tidak nol.
Faktor persekutuan terbesar – FPB (*greatest common divisor* – GCD) dari a dan b (dinotasikan dengan (a,b)) adalah polinomial monik $d = d(x)$ sehingga

1. d membagi a dan b,
2. jika c sebarang elemen $F[x]$ yang membagi a dan b maka c membagi d.

Akan ditunjukkan bahwa FPB selalu ada dalam $F[x]$. Faktor persekutuan terbesar tidak tunggal jika dilakukan pembatasan untuk polinomial monik. Sebagai contoh dalam $\boldsymbol{R}[x]$, FPB dari x dan $x^2 + x$ adalah x tetapi sebarang polinomial konstan kelipatan dari x seperti $-x$ dan $2x/3$ juga memenuhi syarat 1 dan syarat 2 dari definisi di atas.

Teorema XVIII.2

Jika diketahui $a(x)$ dan $b(x)$ dalam $F[x]$ maka $a(x)$ dan $b(x)$ mempunyai FPB dalam $F[x]$ dan terdapatlah polinomial $s(x)$ dan $t(x)$ dalam $F[x]$ sehingga

$$s(x)\, a(x) + t(x)\, b(x) = d(x).$$

Bukti :

Untuk mempermudah penulisan, dimisalkan $a = a(x)$ dan $b(x)$.
Dibentuk himpunan $J = \{ u\, a + v\, b \mid u, v \text{ dalam } F[x] \}$.
Mudah ditunjukkan bahwa J ideal dalam $F[x]$.
Tetapi karena setiap ideal dalam berbentuk $J = (d(x))$ untuk suatu $d(x)$ dalam $F[x]$ maka $d = s\, a + b\, t$ untuk suatu s dan t dalam $F[x]$.
Tanpa menghilangkan keumuman dianggap bahwa d monik.
Akan dirunjukkan bahwa d sebenarnya merupakan FPB dari a dan b.
Karena $a = 1 \,.\, a + 0.\, b$ dan $b = 0 \,.\, a + 1 \,.\, b$ maka a dan b dalam J.
Karena d membangun J maka d merupakan faktor dari s dan juga faktor dari b.
Misalkan g sebarang faktor persekutuan dari a dan b.
Karena $d = s\, a + t\, b$ dan g membagi kedua suku pada ruas kanan maka g membagi d.
Berarti d memenuhi syarat sebagai FPB dari a dan b.

Contoh XVIII.1

Polinomial $p(x) = x^2 - 2$ irredusibel atas field $\boldsymbol{Q}$. Dalam field yang diperoleh dengan cara menggabungkan akar dari polinomial $p(x)$ yaitu $\alpha = \sqrt{2}$ pada $\boldsymbol{Q}$.

Akan dicari invers perkalian dari elemen $4 + 3\sqrt{2}$.

Polinomial $f(x) = 3x + 4$ dan $p(x)$ prima relatif atas $\boldsymbol{Q}$.

Akan dicari $s(x)$ dan $t(x)$ sehingga

$$f(x)s(x) + p(x)t(x) = 1$$

$$p(x) = f(x)\left(\frac{1}{3}x - \frac{4}{9}\right) + \left(-\frac{2}{9}\right)$$

$$f(x)\left(\frac{3}{2}x - 2\right) + p(x)\left(-\frac{2}{9}\right) = 1.$$

Karena $p(\sqrt{2}) = 0$ maka diperoleh

$$f(\sqrt{2})\left(\frac{3}{2}\sqrt{2} - 2\right) = 1$$

sehingga $\left(4 + 3\sqrt{2}\right)^{-1} = f(\sqrt{2})^{-1} = \frac{3}{2}\sqrt{2} - 2$.

Berikut ini diberikan algoritma Euclid untuk polinomial (tanpa bukti).

Teorema XVIII.3

Algoritma Euclid berlaku dalam $F[x]$ yaitu untuk sebarang polinomial $a(x)$, $b(x)$ dengan $b(x)$ mempunyai koefisien pemimpin $b_n \neq 0$, barisan perulangan dari algoritma pembagian

$a(x) = b(x)\, q_1(x) + r_1(x)$,
$b(x) = r_1(x)\, q_2(x) + r_2(x)$,
$r_1(x) = r_2(x)\, q_3(x) + r_3(x)$,
……
……..

dengan $(a, b) = b_n{}^{-1}$ atau (a, b) sama dengan sisa pembagian yang terakhir yang tidak nol dibagi dengan koefisien pemimpin untuk membuat polinomialnya monik.

Contoh XVIII.1

Diketahui $a(x) = x^7 + x^3$ dan $b(x) = x^3 + x^2 + x$ polinomial atas Z_2.
Dengan algoritma Euclid diperoleh

$$x^7 + x^3 = (x^3 + x^2 + x) + x^2$$
$$x^3 + x^2 + x = x^2 (x + 1) + x$$
$$x^2 = x \cdot x + 0.$$

Akibatnya sisa pembagian terakhir yang tidak nol merupakan FPB yaitu $d(x) = x$. Untuk menemukan $s(x)$ dan $t(x)$ dalam $Z_2[x]$ sehingga $d(x) = s(x)\, a(x) + t(x)\, b(x)$ digunakan langkah-langkah berikut ini.
Misalkan $a = a(x)$ dan $a = b(x)$.

$$x^2 = a - (x^4 + x^3 + x)\, b$$

dan ekuivalen dengan

$$[1 - (x^4 + x^3 + x)]$$

kemudian

$$x = b - (x + 1)\, x^2$$

ekuivalen dengan

$$[0 \quad 1] - (x + 1)[1 \quad - (x^4 + x^3 + x)]$$

dan berarti ekuivalen dengan

$$[- (x +1) \quad 1 + (x + 1)\, (x^4 + x^3 + x)]$$

dan akhirnya ekuivalen dengan

$$[- (x + 1)\, x^5 + x^3 + x^2 + x +1] .$$

Karena $-(x + 1)$ sama dengan $x + 1 \bmod 2$ maka diperoleh

$$x = (x + 1)\, a + (x^5 + x^3 + x^2 + x +1)\, b.$$

Contoh XVIII.2

Akan ditentukan FPB dari $a = x^6 + 2\, x^5 + x^2 + 2$ dan $b = 2\, x^4 + x^3 + 2x + 1$ atas Z_3.

$$a = b \cdot (2\, x^2 + x + 2) + (2\, x^3 + 2x + 2)$$
$$b = (2\, x^3 + 2\, x^2 + 2) \cdot (x + 1) + (x^2 + 1)$$
$$(2\, x^3 + 2\, x^2 + 2) = (x^2 + 2) \cdot (2x + 2) + (2x+1)$$

$(x^2 + 2) = (2x+1) . (2x + 2) + 0.$

Sisa tidak nol yang terakhir yaitu $2x + 1$ digandakan dengan $2^{-1} = 2$ dan diperoleh $x + 2$.

Berarti FPB dari a dan b adalah $x + 2$.

Teorema XVIII.4

Jika $p(x)$ irredusibel atas F dan $p(x)$ tidak membagi $a(x)$ maka

$$(p(x) , a(x)) = 1.$$

Bukti :

Karena $p(x)$ irredusibel maka $p(x)$ hanya mempunyai faktor polinomial konstan yang tidak nol dan konstanta pengalinya.

Karena $p(x)$ tidak membagi $a(x)$ maka untuk sebarang $c.p(x)$ juga tidak membagi $a(x)$. Oleh karena itu, hanyalah suatu konstanta yang membagi $p(x)$ juga tidak membagi $a(x)$ dan faktor persekutuan monik hanyalah 1.

Berarti $(p(x), a(x)) = 1$.

Teorema XVIII.5

Diketahui $p = p(x)$ irredusibel atas F. Jika p membagi suatu hasil kali $a(x)$ $b(x)$ dari polinomial aras F maka salah satu berlaku p membagi $a(x)$ atau p membagi $b(x)$.

Bukti :

Jika p tidak membagi $a = a(x)$ maka $(a, p) = 1$.

Akibatnya $s\ a + t\ p = 1$ untuk suatu polinomial s dan t dalam $F[x]$.

Dengan mengalikan kedua ruas dengan b diperoleh $s\ a\ b + t\ p\ b = b$.

Karena p membagi $a\ b$ maka p membagi $s\ a\ b$ dan $t\ p\ b$ sehingga p membagi jumlahnya yaitu $s\ a\ b + t\ p\ b = b$.

Teorema XVIII.6

Jika $g(x)$ suatu polinomial monik tidak konstan dengan koefisien dalam suatu field F maka

1. $g(x)$ dapat difaktorkan sebagai hasil kali polinomial monik sebanyak berhingga $p_i(x)$:
$$g(x) = p_1(x), p_2(x) \ldots\ldots\ldots p_k(x)$$
2. faktorisasi tersebut tunggal yaitu jika
$$g(x) = q_1(x), q_2(x) \ldots\ldots\ldots p_k(x)$$
suatu faktorisasi yang lain dari $g(x)$ sebagai hasil kali polinomial monik irredusibel q_j maka q_j hanyalah p_i yang disusun ulang.

Bukti :

Untuk latihan.

Dengan pengelompokan faktor ganda maka $g(x)$ dapat ditulis sebagai

$$g(x) = c_1 [p_1(x)]^{a_1} [p_2(x)]^{a_2} \ldots\ldots [p_v(x)]^{a_v}$$

Jika $g(x)$ irredusibel maka faktorisasinya hanya terdiri dari satu faktor. Jika

$$g(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots.$$

bukan polinomial monik maka $g(x)$ dapat ditulis sebagai

$$g(x) = c_n [x^n + (c_n^{-1} c_{n-1}) x^{n-1} + \ldots\ldots]$$

sehingga $g(x)$ dapat difaktorkan menjadi

$$g(x) = c_1 [p_1(x)]^{a_1} [p_2(x)]^{a_2} \ldots\ldots [p_v(x)]^{a_v} .$$

Definisi XVIII.3

Diketahui *A* suatu ring komutatif dengan elemen satuan. Suatu unit (*unit*) dalam *A* adalah suatu elemen yang mempunyai invers terhadap perkalian dalam *A*. Elemen *a* dan *b* dari *A* dikatakan sekawan (*associates*) jika $a = u\ b$ untuk suatu unit *u*.

Dalam hal ini, bila *a* dikatakan suatu kawan dari *b* maka *b* juga suatu kawan dari *a* (karena $b = u^{-1}\ a$). Sebagai contoh -5 dan 5 bersekawan dalam *Z* karena -5 = -1 . 5 dan -1 unit dalam *Z*.

Contoh XVIII.3

Elemen -1 dalam Z merupakan unit karena -1 mempunyai invers terhadap perkalian yaitu dirinya sendiri.
Akibatnya -3 bersekawan dengan 3 dan juga -5 bersekawan dengan 5.
Hal itu berarti faktorisasi dari 15 menjadi

$$15 = 3 \,.\, 5$$

secara esensi sama dengan

$$15 = -3 \,.\, -5.$$

Contoh XVIII.4

Dalam $\boldsymbol{R}[x]$ sebarang polinomial konstan c merupakan unit karena

$$c \,.\, c^{-1} = 1 = 1\, x^0$$

yaitu elemen satuan dalam $\boldsymbol{R}[x]$.
Hal itu berarti bahwa $5x$ dan $3x$ bersekawan dengan x dan

$$(x/15) + (2/15) = (1/15)\,(x + 2)$$

merupakan suatu kawan dari $x + 2$.
Akibatnya polinomial $x^3 + 2x^2$ dapat difaktorkan sebagai

$$x^3 + 2x^2 = x^2\,(x + 2)$$

yang secara esensi sama dengan pemfaktoran

$$x^3 + 2x^2 = (5x) \,.\, (3x)\,(x/15 + 2/15).$$

Bila suatu elemen y dalam suatu ring dikatakan irredusibel maka dimaksudkan bahwa y tidak dapat difaktorkan kecuali sebagai hasil kali suatu unit dengan suatu kawan dari y. Sebagai contoh $7 = (-1)\,(-7)$ dalam $\boldsymbol{Z}$ merupakan faktorisasi tidak sejati dari 7 dan tidak merupakan penyimpangan dari kenyataan bahwa 7 merupakan irredusibel dalam $\mathbf{Z}$. Dengan cara yang sama, faktorisasi

$$x^2 + 1 = (1/2)\,(2\,x^2 + 2)$$

dalam $R[x]$ tidak merupakan penyimpangan dari irredusibilitas dari x^2+1. Sering kali terjadi kekeliruan pengertian bahwa sifat irredusibilitas sebagai suatu padanan dari sifat prima tetapi konsep ini tidak sama jika sifat faktorisasi tunggal tidak dipenuhi. Secara lengkap definisi untuk kedua hal ini dijelaskan dalam definisi berikut ini.

Definisi XVIII.4

Diketahui D daerah integral.
Suatu elemen tidak nol y dalam D dan y bukan unit dikatakan irredusibel jika untuk $y = ab$ maka salah satu berlaku $y \mid a$ atau y $\mid b$.

Dengan dasar Teorema XVIII.5 dan Definisi XVIII.4 maka dapat diambil kesimpulan bahwa jika $p(x)$ irredusibel dalam $F[x]$ maka $p[x]$ prima.

Definisi XVIII.5

Daerah integral dikatakan daerah faktorisasi tunggal – DFT (*unique factorization domain – UFD*) jika

1. setiap elemen tidak nol y dalam D yang bukan unit dapat difaktorkan sebagai hasil kali dari berhingga banyak elemen irredusibel, misalkan $y = p_1, p_2, ..., p_k$.
2. faktorisasi dalam bagian 1 ini tunggal artinya jika $q_1, q_2, ..., q_m$ merupakan faktorisasi elemen irredusibel yang lain maka q bersekawan dengan p yang diurutkan.

Daerah integral yang setiap idealnya merupakan ideal dinamakan daerah ideal utama – DIU (*principal ideal domain* – PID).

Teorema XVIII.7

Jika D daerah ideal utama maka D daerah faktorisasi tunggal.

Bukti :

Untuk latihan.

Contoh XVIII.5

Diketahui himpunan bilangan bulat Z.
Sebarang ideal J dalam Z merupakan suatu grup bagian dari Z di bawah + sehingga J siklik.
Oleh karena itu J sama dengan suatu grup bagian siklik

$$(a) = \{ k \,.\, a \mid k \text{ dalam } Z \}.$$

Dalam hal ini, J juga sama dengan ideal utama (a).
Hal ini berarti bahwa Z daerah ideal utama dan akibatnya Z daerah faktorisasi tunggal.
Akan ditunjukkan kemudian bahwa $Z[x]$ bukan daerah ideal utama dan juga berlaku bahwa untuk sebarang D daerah integral yang bukan field maka $D[x]$ bukan daerah ideal utama.
Akan ditunjukkan juga nantinya bahwa $Z[x]$ merupakan daerah faktorisasi tunggal.
Hal itu berarti bahwa tidak setiap daerah faktorisasi tunggal merupakan daerah ideal utama.

Definisi XVIII.6

Diketahui D daerah integral.
Jika suatu fungsi "ukuran" s didefinisikan untuk semua elemen D yang tidak nol sehingga nilai S merupakan bilangan bulat tidak negatif dan memenuhi dua syarat berikut :

1. $S(a) \leq S(ab)$ untuk sebarang a, b dalam D yang tidak nol.
2. untuk sebarang a, b dalam D dengan $b \neq 0$ diperoleh $a = bq + r$ untuk suatu q, r dalam D dengan $r = 0$ atau $S(r) < S(b)$.

maka D dikatakan daerah Euclid (*Euclidean domain*).

Dengan mengingat syarat 2 dari definisi di atas, jika d suatu elemen dengan ukuran terkecil dalam suatu ideal tidak nol J dalam suatu daerah Euclid maka $J = (d)$. Akibatnya daerah Euclid merupakan daerah ideal utama. Dapat diringkas bahwa

$$\text{daerah Euclid} \rightarrow \text{DIU} \rightarrow \text{DFT}$$

tetapi secara umum

$$\text{DFT} \not\rightarrow \text{DIU} \not\rightarrow \text{daerah Euclid.}$$

Contoh XVIII.6

Diketahui $\boldsymbol{Z}[i] = \{ a + b \mid a, b \text{ dalam } \boldsymbol{Z} \}$ ($\boldsymbol{Z}[i]$ dikenal dengan *bilangan Gauss*).
Mudah dibuktikan bahwa $\boldsymbol{Z}[i]$ merupakan ring bagian dari $\boldsymbol{C}$ dan $\boldsymbol{Z}[i]$ daerah integral.

Misalkan dipilih fungsi ukuran $S(a + b) = a^2 + b^2$.

(1) Misalkan z, w dalam $\boldsymbol{Z}[i]$.

Dengan menggunakan sifat De Moivre diperoleh :

$$S(z\,w) = |z\,w|^2 = (|z|\,|w|)^2 = |\,z\,|^2\,|\,w\,|^2 = S(z)\,S(w).$$

Karena $S(w) \geq 1$ untuk $w \neq 0$ maka jelas bahwa $S(z) \leq S(z\,w)$ dan berarti syarat 1 dipenuhi.

(2) Misalkan diamati ring yang lebih besar dari $\boldsymbol{Z}[i]$ yaitu

$$\boldsymbol{Q}[i] = \{\, a + b\,i \mid a, b \text{ dalam } \boldsymbol{Q} \,\}$$

yang juga merupakan field.

Jika diberikan $w = a + b\,i$ dan $z = c + d\,i$ (yang tidak nol) dalam $\boldsymbol{Z}[i]$ dan dapat juga dipandang sebagai elemen $\boldsymbol{Q}(i)$.

Dapat dibuktikan dengan mudah bahwa

$$wz^{-1} = (q_1 + s_1/(c^2 + d^2)) + (q_2 + s_2/(c^2 + d^2))\,i$$

dan dengan menyusun kembali diperoleh

$$wz^{-1} = (q_1 + q_2\,\mathrm{i}) + (s_1/(c^2 + d^2) + s_2/(c^2 + d^2)\,i)$$
$$= (q_1 + q_2\,i) + (t + u\,i).$$

Akhirnya dengan mengalikan kedua ruas dengan z diperoleh

$$w = z\,(q_1 + q_2\,i) + (t + u\,i)$$

atau $w = z\,q + r$.

Jelas bahwa $q = q_1 + q_2\,i$ dalam $\boldsymbol{Z}[i]$ dan karena w dan zq dalam $\boldsymbol{Z}[i]$ maka

$$r = z(t + ui)$$

dalam $\boldsymbol{Z}[i]$.

Akhirnya ukuran dari r memenuhi

$$S(r) = S(\mathrm{z})\,S(\,t + u\,i) \leq S(z)\,.\,(1/2) \leq S(z).$$

Terbukti bahwa $Z[i]$ daerah Euclid.

Karena $\boldsymbol{Z}[i]$ daerah Euclid maka $\boldsymbol{Z}[i]$ daerah ideal utama dan akibatnya daerah faktorisasi tunggal.

Sebagai contoh, $5=(1 + 2i)(1 - 2i)$ merupakan faktorisasi irredusibel tunggal secara esensi dari 5.

Contoh XVIII.7

Akan ditunjukkan bahwa $\boldsymbol{Z}[x]$ bukan daerah Euclid.
Andaikan $\boldsymbol{Z}[x]$ daerah Euclid.

Karena $\boldsymbol{Z}[x]$ daerah Euclid maka $\boldsymbol{Z}[x]$ haruslah merupakan daerah ideal utama.
Misalkan $J = \{ 3 . u(x) + x . v(x) \mid u(x). v(x)$ dalam $\boldsymbol{Z}[x] \}$.
Dapat ditunjukkan bahwa J ideal dalam daerah ideal utama $\boldsymbol{Z}[x]$ maka $J = (d(x))$ untuk suatu $d(x)$ dalam $\boldsymbol{Z}[x]$.
Karena 3 dalam $\boldsymbol{Z}[x]$ maka $3 = p(x)\ d(x)$ sehingga d suatu polinomial konstan.
Karena x dalam $\boldsymbol{Z}[x]$ maka $x = d . g(x)$ sehingga berakibat $d = 1$ atau $d = -1$.
Akibatnya $J = \boldsymbol{Z}[x]$.
Tetapi 2 dalam $\boldsymbol{Z}[x]$ sehingga haruslah dapat dinyatakan sebagai
$3 . u(x) + x . v(x)$
untuk suatu $u(x)$ dan $v(x)$ dalam $\boldsymbol{Z}[x]$.
Tetapi ternyata $u(x)$ dan $v(x)$ tidak dapat ditemukan dalam $\boldsymbol{Z}[x]$.
Berarti terdapat suatu kontradiksi dan pengandaian haruslah diingkar.
Terbukti $\boldsymbol{Z}[x]$ bukan daerah ideal utama sehingga $\boldsymbol{Z}[x]$ bukan daerah Euclid.

Contoh XVIII.8

Himpunan $\boldsymbol{Z}[\sqrt{3}\ i] = \{ a + b\sqrt{3}\ i \mid a, b$ dalam $\boldsymbol{Z} \}$ merupakan ring bagian dari $\boldsymbol{C}$ yang mengandung elemen satuan yaitu suatu daerah integral.
Fungsi ukuran didefinisikan pada $\boldsymbol{Z}[\sqrt{3}\ i]$ didefinisikan sebagai

$$S(a + b\sqrt{3}\ i) = a^2 + 3b^2.$$

Karena hukum De Moivre maka didapat $S(z\ w) = S(z)\ S(w)$ dan akibatnya unit dalam $\boldsymbol{Z}[\sqrt{3}\ i\ ]$ hanyalah -1 dan 1.
Ditemukan bahwa $4 = 2 . 2 = (1 + \sqrt{3}\ i\ ) (1 - \sqrt{3}\ i\ )$.
Tetapi elemen dengan ukuran 4 merupakan irredusibel karena tidak ada elemen dengan ukuran 2 dan $S(z\ w) = S(z)\ S(w)$.
Karena 2 dan $1 + \sqrt{3}\ i$ dan juga $1 - \sqrt{3}\ i$ mempunyai ukuran 4 dan elemen 2 jelas bukanlah suatu unit perkalian dari $1 + \sqrt{3}\ i$ maka

$$4 = 2 . 2 = (1 + \sqrt{3}\ i\ ) (1 - \sqrt{3}\ i\ )$$

merupakan faktorisasi sejati yang berbeda dari elemen 4 dalam $\boldsymbol{Z}[\sqrt{3}\ i]$.

Definisi XVIII.7

Diketahui $p(x)$ polinomial tidak konstan dalam $\boldsymbol{Z}[x]$.
Polinomial $p(x)$ dikatakan primitif (*primitive*) jika FPB dari semua koefisiennya sama dengan 1.

Sebagai contoh, polinomial $3x^2 + 6x + 2$ merupakan suatu primitif tetapi $3x^2 + 6x + 3$ bukanlah suatu polinomial primitif.

Teorema XVIII.8 (*Lemma Gauss*)

Jika $f(x)$ dan $g(x)$ polinomial primitif dalam $Z[x]$ maka hasil kalinya $f(x)$ $g(x)$ juga polinomial primitif.

Bukti :

Misalkan koefisien dari $f(x)$ disimbolkan dengan a_i dan koefisien dari $g(x)$ disimbolkan dengan b_j. Koefisien c_k dari x^k dalam $f(x)$ $g(x)$ didefinisikan dengan

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots\ldots + a_k b_0.$$

Andaikan kesimpulan dari teorema ini salah, maka terdapat suatu prima p yang membagi semua c_k.
Misalkan s bilangan bulat terkecil sehingga p tidak membagi a_s dan t bilangan bulat terkecil sehingga p tidak membagi b_t.
Keberadaan bilangan bulat ini dijamin oleh sifat primitif dari $f(x)$ dan $g(x)$.
Untuk membuktikan bahwa p tidak membagi c_{s+t} digunakan sebagai latihan.

Untuk membuktikan bahwa $\boldsymbol{Z}[x]$ merupakan suatu daerah faktorisasi tunggal terlebih dahulu didefinisikan polinomial primitif dan konten (*content*) dari suatu polinomial.

Definisi XVIII.8

Diketahui $f(x)$ polinomial tidak konstan dalam $\boldsymbol{Q}[x]$.
Konten (*content*) dari $f(x)$ adalah konstanta positif c_j sehingga

$$f(x) = c_j g(x)$$

dengan g(x) primitif dalam $\boldsymbol{Z}[x]$.

Sebagai contoh, konten dari

$$f(x) = (-5/8)\, x^2 + (10/9)\, x - (5/12)$$

adalah $5/72$ karena $f(x) = (5/72)\,(-9x^2 - 16x + 6)$ dan $-9x^2 - 16x + 6$ primitif.

Teorema XVIII.9

Konten c_j tunggal.

Bukti :

Untuk latihan.

Teorema XVIII.10

Himpunan polinomial $\boldsymbol{Z}[x]$ merupakan daerah faktorisasi tunggal.

Bukti :

Akan dibuktikan bahwa sebarang polinomial tidak konstan $f(x)$ dalam $\boldsymbol{Z}[x]$ dapat difaktorkan secara tunggal sebagai hasil kali polinomial irredusibel dan hasil pemfaktoran itu tunggal.

Kasus 1 *f(x) primitif*

Dalam $Q[x]$, $f[x]$ mempunyai faktor tunggal

$$f(x) = q_1(x)\, q_2(x) \ldots\ldots q_k(x).$$

Polinomial – polinomial $q_j(x)$ ini dapat ditulis sebagai $c_j\,.\,Q_j(x)$ dengan $Q_j(x)$ primitif dan diperoleh

$$f(x) = c_1\, c_2 \ldots c_k\; Q_1(x)\, Q_2(x) \ldots. Q_k(x).$$

Karena $Q_j(x)$ sekawan dengan $q_j(x)$ maka $Q_j(x)$ juga irredusibel.
Dengan mengingat lemma Gauss maka $Q_1(x)\, Q_2(x) \ldots. Q_k(x)$ primitif.
Karena $f(x)$ primitif dan sama dengan 1. $f(x)$ yaitu hasil kali dari c_j adalah 1 sehingga

$$f(x) = Q_1(x)\, Q_2(x) \ldots. Q_k(x).$$

Faktorisasi ini merupakan suatu faktorisasi ke dalam polinomial – polinomial irredusibel dalam $Z[x]$.

Misalkan dimiliki suatu faktorisasi irredusibel $f(x) = s_1(x)\ s_2(x)\ \ldots.\ s_m(x)$ dalam $Z[x]$ maka $s_i(x)$ haruslah primitif dan dengan membandingkan faktorisasi dalam $Q[x]$ diperoleh $m = k$ dan s_i dalam $Q[x]$ sekawan dengan Q_j.
Tetapi primitif - primitif ini haruslah memenuhi $Q_j(x) = s_i(x)$ (dengan Lemma Gauss).
Akibatnya s_i dan Q_j bersekawan dalam $Z[x]$ dan juga dalam $Q[x]$.
Hal itu berarti faktorisasi dalam $Z[x]$ tunggal.

Kasus 2 *f(x) tidak primitif*

Karena $f(x)$ tidak primitif maka $f(x) = c_j\ .\ F(x)$ dengan $F(x)$ primitif dan c_j bilangan bulat positif yang tunggal sehingga

$$f(x) = c_j\ .\ F(x)$$
$$= p_1\ p_2\ \ldots.\ p_u\ \ Q_1(x)\ Q_2(x)\ \ldots.\ Q_k(x).$$

Hal ini terjadi karena Z merupakan daerah faktorisasi tunggal dan bersama dengan kasus 1 disimpulkan bahwa terdapat faktorisasi tunggal untuk $f(x)$.

Contoh XVIII.7

Polinomial $p(x) = x^4 + 4\ x^3 - 3x - 2$ dapat difaktorkan menjadi

$$p(x) = x^4 + 4\ x^3 - 3x - 2 = (x+1)^2\ (x-1)(x+2)$$

dan pemfaktoran ini tunggal dan tidak ada bentuk pemfaktoran yang lain.

Kriteria yang ditemukan oleh F. G. M. Eisenstein (1823-1852) berikut ini digunakan untuk menentukan irredusibilitas dari polinomial atas Q.

Teorema XVIII.11 (Kriteria Irredusibilitas Eisenstein – *Eisenstein's Irreducibility Criterion*).

Diketahui $g(x) = \sum_{i=1}^{n} a_i\ x^i$ polinomial dengan koefisien bilangan bulat.

Jika elemen prima p membagi semua koefisien polinomial $g(x)$ kecuali a_n dan p^2 tidak membagi a_0 maka $g(x)$ irredusibel atas $\boldsymbol{Q}$.

Contoh XVIII.8

Polinomial $p(x) = x^2 + 2x + 2$ merupakan polinomial dengan koefisien bilangan bulat. Bilangan prima $p = 2$ membagi semua koefisien dari $p(x)$ kecuali a_2 dan $p^2=4$ tidak membagi koefisien $a_0=2$ maka berdasarkan kriteria Eisenstein $p(x)$ irredusibel.
Polinomial $q(x)=x^2 + 7x + 14$ merupakan polinomial dengan koefisien bilangan bulat. Bilangan prima $p=7$ membagi semua koefisien dari $q(x)$ kecuali a_2 dan $p^2 = 49$ tidak membagi koefisien $a_0 = 14$ sehingga berdasarkan kriteria Eisenstein $q(x)$ irredusibel.
Polinomial $h(x) = x^2 + 1$ irredusibel atas $\boldsymbol{Q}$ tetapi tidak memenuhi sifat kriteria Eisenstein. Hal ini berarti bahwa tidak setiap polinomial yang irredusibel atas $\boldsymbol{Q}$ harus memenuhi kriteria Eisenstein.

Contoh XVIII.9

Polinomial x^4+1 dapat difaktorisasi menjadi atas polinomial irredusibel atas $R[x]$ menjadi

$$x^4 + 1 = \left(x^2 - \sqrt{2}\,x + 1\right)\left(x^2 + \sqrt{2}x + 1\right)$$

tetapi tidak dapat difaktorkan menjadi polinomial atas $\boldsymbol{Q}[x]$ sehingga merupakan polinomial irredusibel dalam $\boldsymbol{Q}[x]$. Selanjutnya, polinomial x^4+1 dapat difaktorisasi menjadi atas polinomial irredusibel atas $\boldsymbol{C}[x]$ menjadi

$$x^4 + 1 =$$

$$\left[x - \left(\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right]\left[x - \left(\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right]\left[x - \left(-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i\right)\right]\left[x - \left(-\frac{\sqrt{2}}{2} - \frac{\sqrt{2}}{2}i\right)\right]$$

sehingga merupakan polinomial irredusibel dalam $\boldsymbol{Q}[x]$.

Latihan

1. Gunakan algoritma Euclid untuk menentukan FPB dari pasangan polinomial berikut ini :
   a. $x^5 - 4x$ dan $x^4 - 4$.
   b. $x^5 - 4x$ dan $x^4 - x^3 + 2x^2 - 2x$.
   c. $2x^5 + 6x^3 + x^2 + 4x + 2$ dan $x^4 - x^3 + 2x^2 - 2x$.
2. Tentukan FPB $d(x)$ jika diberikan $a(x)$ dan $b(x)$ atas Z_2 dan nyatakan $d(x)$ dalam bentuk
   $$s(x)\, a(x) + t(x)\, b(x).$$
   a. $a(x) = x^7 + 1$ dan $b(x) = x^3 + 1$.
   b. $a(x) = x^6 + x^3 + x^2 + x$ dan $b(x) = x^5 + x^4 + 1$.
   c. $a(x) = x^8 + x + 1$ dan $b(x) = x^5 + x + 1$.
3. Nyatakan faktorisasi dari polinomial $x^4 + x^3 + x + 1$ dan $x^5 + x + 1$ atas Z_2.
4. Nyatakan faktorisasi dari polinomial $2x^3 + 21x^2 - 5$ atas $\boldsymbol{Q}$.
5. Jika $a(x) = x^7 + 1$ dalam $Z_2[x]$ dan $b(x) = x^3 + 1$ dalam $Z_2[x]$ maka tentukan FPB $d(x)$ dan juga nyatakan $d(x) = s(x)\, a(x) + t(x)\, b(x)$ untuk suatu $s(x)$, $t(x)$ dalam $Z_2[x]$.
6. Misalkan a, b, b_i, c elemen ring komutatif A dengan satuan.
   a. Buktikan bahwa jika $a \mid b$ dan $a \mid c$ maka $a \mid (b + c)$ dan
   $$a \mid (b - c).$$
   b. Buktikan dengan menggunakan induksi bahwa jika a membagi $b_1, b_2, \ldots, b_n$ maka a membagi $b_1 + b_2 + \ldots + b_n$.
7. Misalkan a, b, c elemen ring komutatif A dengan elemen satuan.

a. Buktikan bahwa jika $a \mid b$ dan $b \mid c$ maka $a \mid c$.
b. Buktikan bahwa $a \mid a$ untuk semua a dalam A.
c. Jika A daerah integral maka buktikan bahwa a sekawan dengan b jika $a \mid b$ dan $b \mid a$.

8. Buktikan bahwa dalam ring komutatif dengan elemen satuan berlaku bahwa $ud \mid t$ jika $d \mid t$ dan u unit.
9. Tunjukkan bahwa unit dalam $\boldsymbol{Z}[\sqrt{3}\ i]$ hanyalah 1 dan -1.
10. Buktikan bahwa $\boldsymbol{Z}[\sqrt{2}\,]$ mempunyai tak berhingga banyak unit.

11. Tunjukkan bahwa dua faktorisasi dari 7 yang diberikan di bawah ini secara esensi sama yaitu

$$7 = (3 + \sqrt{2})(3 - \sqrt{2}) = (5 + 4\sqrt{2})(5 - 4\sqrt{2}).$$

12. Buktikan bahwa jika F field maka $F[x]$ daerah Euclid.

13. $Z[\sqrt{3}\,i]$ bukan daerah ideal utama karena bukan daerah faktorisasi tunggal.

    Tentukan suatu ideal dalam $Z[\sqrt{3}\ i]$ yang bukan ideal utama.

14. Tunjukkan bahwa $\boldsymbol{Z}[\sqrt{5}\,i]$ bukan daerah faktorisasi tunggal dengan langkah-langkah sebagai berikut :

    a. Tunjukkan bahwa $S(a + b\sqrt{5}\,i) = a^2 + 5b^2$ mendefinisikan suatu fungsi ukuran perkalian.

    b. Elemen $\boldsymbol{Z}[\sqrt{5}\,i]$ manakah yang merupakan unit ?

    c. Misalkan z dalam $\boldsymbol{Z}[\sqrt{5}\,i]$.
    Tunjukkan bahwa jika $S(z)$ sama dengan 4, 5, 6, atau 9 maka z irredusibel.

    d. Tentukan suatu integer a dengan $a \leq 10$ dan $a = a + 0\ \sqrt{5}$ yang mempunyai dua faktorisasi irredusibel yang berbeda dalam $\boldsymbol{Z}[\sqrt{5}\,i]$.

15. Dengan menggunakan kriteria irredusibilitas Eisenstein buktikan bahwa

$$x^4 + 3x^2 - 9x + 6$$

dan $2x^7 - 10x^2 + 25x - 70$ irredusibel atas Q.

***

BAB XIX
PENUTUP

Aljabar modern atau lebih dikenal dengan struktur aljabar seringkali dipandang mahasiswa sebagai mata kuliah yang cukup sulit (lihat Leron & Dubinsky, 1995 dan Carlson, 2003 dalam Arnawa, 2009). Namun demikian mata kuliah ini sangat penting dalam memberikan kemampuan berpikir secara logis bagi mahasiswa. Liku-liku berpikir pada pembuktian dalam aljabar abstrak perlu dipelajari dan diasah agar mahasiswa mempunyai *feeling* dalam pembuktian sifat-sifat, teorema dan pengerjaan soal-soal dalam mata kuliah aljabar abstrak. Hal itu akan sangat penting dalam penelitian dan pengembangan aljabar modern.

Dalam buku ini telah dipaparkan dasar-dasar aljabar modern khususnya tentang teori grup dan teori ring. Dengan mempelajari dasar-dasar aljabar modern, diharapkan dapat digunakan dalam mempelajari lebih lanjut tentang aljabar modern yang berkaitan dengan teori modul, teori Galois, teori penyandian (*coding theory*) dan aplikasi dari aljabar modern di berbagai bidang seperti bidang Ilmu Komputer (*Computer Science*), Fisika dan Kimia. Penggunaan *software* komputer (seperti **Maple** dan **Matlab**, lihat dalam Klima, dkk, 2006) juga akan sangat membantu dan mendukung dalam pembelajaran tentang aljabar modern. Di samping itu, penggunaan software juga sangat penting dalam penelitian aljabar modern beserta aplikasinya. Aljabar modern masih akan terus berkembang dan perkembangan itu akan makin maju dengan bantuan komputer dan makin menarik jika digabungkan dengan teori lain seperti aljabar *fuzzy* yang banyak sekali digunakan dalam aplikasi ilmu komputer dan dalam teknologi informasi.

DAFTAR PUSTAKA

1. Arnawa, I Made, 2009, Mengembangkan Kemampuan Mahasiswa dalam Memvalidasi Bukti pada Aljabar Abstrak melalui Pembelajaran Berdasarkan Teori APOS, *Jurnal Matematika & Sains*, Vol 14, No. 2 hal. 62-68.
2. Block, N. J , 1989, *Abstract Algebra with Applications*, Prentice-Hall Inc, New Jersey.
3. Gallian, Joseph A. 1990. *Contemporary Abstract Algebra 2nd Edition*. D.C. Heath and Company, Canada.
4. Gilbert, Jimmie & L. Gilbert, 2009, *Elements of Modern Algebra*, Brooks/Cole Cengage Learning, Belmont .
5. Klima, R., N. P. Sigmon, E. Stitzinger, 2006, *Applications of Abstract Algebra with Maple and MATLAB,* 2*nd Edition*, Chapman & Hall CRC, Boca Raton.
6. Raisinghani, M.D. & Aggarwal, R.S., 1980. *Modern Algebra*, S. Chand & Company Ltd, New Delhi.