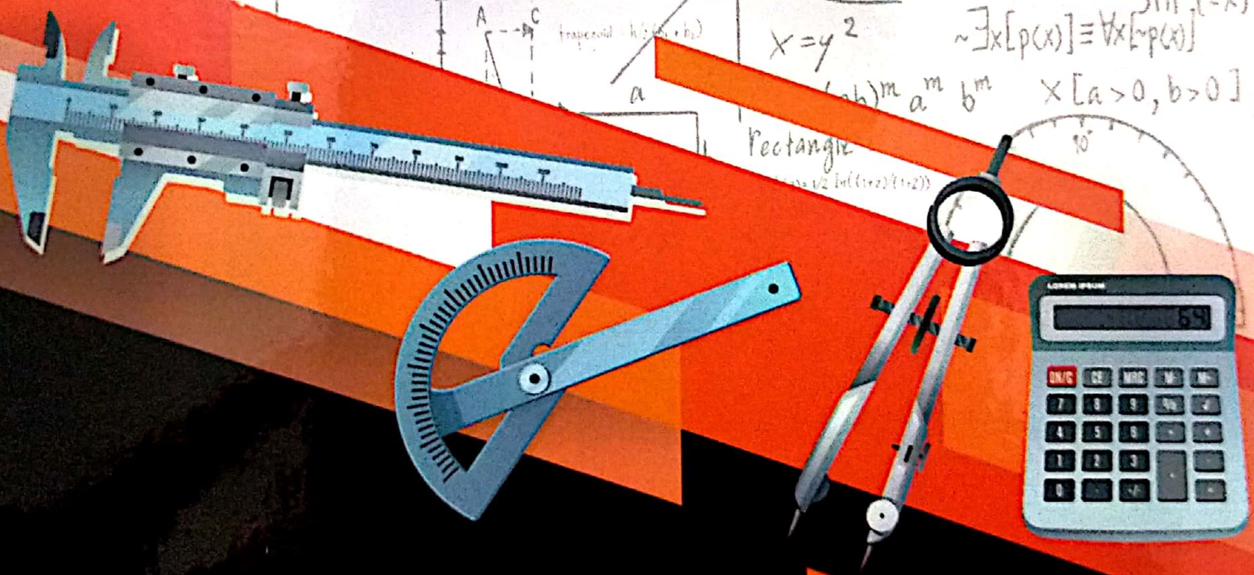
STRUKTUR ALJABAR RING



KENCANA

Siti Maysarah, M.Pd.

STRUKTUR ALJABAR RING

STRUKTUR ALJABAR RING

Siti Maysarah, M.Pd.

Editor:

Dr. Indra Jaya, M.Pd.

KENTANA

STRUKTUR ALJABAR RING

Edisi Pertama

ISBN 978-623-218-699-6
ISBN (E) 978-623-218-697-2
15.5 x 23 cm
xii, 202 hlm.

Cetakan ke-1, November 2020

Kencana 2020.1355

Penulis
Siti Maysarah, M.Pd.

Editor
Dr. Indra Jaya, M.Pd.

Diterbitkan Oleh Kencana
Bekerja sama dengan Fakultas Ilmu Tarbiyah dan Keguruan
Universitas Islam Negeri Sumatera Utara

Desain Sampul
Irfan Fahmi

Penata Letak
Suwito & Iam

Penerbit
KENCANA
Jl. Tambra Raya No. 23 Rawamangun - Jakarta 13220
Telp: (021) 478-64657 Faks: (021) 475-4134

Divisi dari PRENADAMEDIA GROUP
e-mail: pmg@prenadamedia.com
www.prenadamedia.com
INDONESIA

KATA PENGANTAR

Assalamu'alaikum Wr.Wb.

Puji syukur ke hadirat Allah Swt. atas segala rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan penulisan buku ajar dengan judul *Struktur Aljabar Ring* ini sesuai dengan waktu yang telah direncanakan. Selawat dan salam senantiasa tercurah kepada Nabi Muhammad saw. beserta kerabat, sahabat, dan para pengikutnya sampai akhir zaman, sosok yang telah membawa manusia dari zaman kegelapan sampai saat ini sehingga kita menjadi manusia beriman, berilmu, dan beramal saleh.

Buku ajar ini disusun berdasarkan pada rumusan Capaian Pembelajaran Program Studi (CP-Prodi) dan rumusan Capaian Pembelajaran Matakuliah (CP-MK) yang tertuang pada Rencana Pembelajaran Semester (RPS) pada Program Studi Pendidikan Matematika Fakultas Ilmu Tarbiyah dan Keguruan UIN Sumatera Utara Medan. Buku ajar ini terdiri dari 10 (sepuluh) bab, yang terdiri dari: Ring (Gelanggang), Daerah Integral dan *Field*, Subring, Ideal, Ring Faktor, Ring Homomorfisma, Ring Faktor dari Ring Polinomial, Lapangan Perluasan (*Extension Field*), Daerah Faktorisasi Tunggal dan Daerah Euclid.

Buku ajar ini ditulis dalam rangka melengkapi perangkat pembelajaran pada matakuliah struktur aljabar ring, yang merupakan matakuliah inti dari Program Studi Pendidikan Matematika UIN Sumatera Utara Medan. Setiap materi disajikan dalam bentuk definisi, teorema, lemma, contoh dan bukan contoh, serta diakhiri dengan latihan untuk mengukur pemahaman mahasiswa dalam menguasai materi pada matakuliah ini.

Penulis berharap dengan adanya buku *Struktur Aljabar Ring* ini, dapat membantu mahasiswa dalam menguasai materi pada matakuliah ini. Sehingga nantinya dapat melahirkan pemikiran mahasiswa yang logis, kritis, sistematis, dan inovatif dalam menyelesaikan masalah.

Penulis mengucapkan terima kasih kepada segala pihak yang telah mendukung tersusunnya buku ajar ini terkhusus kepada pimpinan Fakultas Ilmu Tarbiyah dan Keguruan UIN Sumatera Utara Medan, **Dr. Amiruddin Siahaan, M.Pd.** yang telah memotivasi penulis dalam penyusunan buku ajar ini. Selain itu, penulis mengucapkan terima kasih kepada pimpinan Program Studi Pendidikan Matematika Fakultas Ilmu Tarbiyah dan Keguruan UIN Sumatera Utara, **Dr. Indra Jaya, M.Pd.** yang selalu memberikan motivasi dan saran dalam penulisan buku ajar ini. Penulis juga mengucapkan terima kasih kepada suami tercinta, **Zuhdi Al Faisal Nasution, S.E.** yang senantiasa memberikan dukungan dan semangat, sehingga penulis dapat menyelesaikan buku ajar ini.

Penulis menyadari bahwa masih banyak kekurangan dan perlu perbaikan yang ditemukan dalam buku ajar ini. Sumbangan pemikiran yang membangun sangat penulis harapkan dari rekan sejawat terutama dosen-dosen senior yang terhimpun dalam matakuliah serumpun. Selain itu, usulan dari para pengguna buku ajar ini terutama mahasiswa Program Studi Pendidikan Matematika UIN Sumatera Utara, semoga buku ajar ini dapat diperkaya melalui evaluasi secara terus menerus. Semoga buku ajar ini bermanfaat dalam memperkaya ilmu pengetahuan dan menjadi ladang amal ibadah bagi penulis.

Medan, September 2020

Penulis

Siti Maysarah, M.Pd.

DAFTAR ISI

DAFTAR TABEL DAN GAMBAR

DAFTAR TABEL

DAFTAR GAMBAR

PENDAHULUAN

1. DESKRIPSI MATAKULIAH

Pembahasan pada matakuliah ini adalah ring (gelanggang), daerah integral (*integral domain*) dan *field*, subring, ideal, ring faktor (*quotient ring*), ring homomorfima, ring polinomial dan algoritma pembagian (faktorisasi) polinom, ring faktor dari ring polinomial, *field* perluasan (*extension field*), daerah faktorisasi tunggal dan daerah Euclid. Seluruh materi pada matakuliah ini membutuhkan pemikiran tingkat tinggi, sehingga setelah mempelajari matakuliah ini mahasiswa diharapkan mampu berpikir secara kritis, logis, dan sistematis dalam menyelesaikan permasalahan. Selain itu, juga memberikan persiapan kepada mahasiswa untuk studi lanjut, baik dalam ilmu pendidikan matematika ataupun ilmu terapan lainnya.

2. PRASYARAT MATAKULIAH

Sebelum mahasiswa mengambil matakuliah struktur aljabar ring, maka mahasiswa terlebih dahulu harus lulus pada matakuliah struktur aljabar grup (Sruktur Aljabar *I*) dengan nilai minimal *C*.

3. RENCANA PEMBELAJARAN

Pertemuan ke-1 : Silabus dan kontrak matakuliah
Pertemuan ke-2 : Teori gelanggang (ring), ring komutatif, dan ring dengan unsur kesatuan
Pertemuan ke-3 : Gelanggang dengan unsur kesatuan
Pertemuan ke-4 : Daerah integral
Pertemuan ke-5 : Lapangan (*field*)

Pertemuan ke-6 : Subring
Pertemuan ke-7 : Ideal
Pertemuan ke-8 : UTS
Pertemuan ke-9 : Ring faktor
Pertemuan ke-10 : Ring homomorfisma
Pertemuan ke-11 : Ring Polinomial
Pertemuan ke-12 : Ring faktor dari ring polinomial
Pertemuan ke-13 : Lapangan perluasan (*extension field*)
Pertemuan ke-14 : Daerah faktorisasi tunggal
Pertemuan ke-15 : Daerah euclid
Pertemuan ke-16 : UAS

4. PETUNJUK PENGGUNAAN BUKU AJAR

a. Bagi Mahasiswa

Buku ini dimulai dari uraian penjelasan setiap materi. Setelah itu, dilanjutkan dengan pembuktian teorema bahkan lemma, pemberian contoh dan bukan contoh pada setiap materi, rangkuman materi, dan diakhiri dengan latihan soal sebagai penguatan terhadap penguasaan mahasiswa terhadap materi yang telah disajikan.

b. Bagi Dosen

Peran dosen dalam pembelajaran ini adalah selain sebagai penyaji, juga sebagai fasilitator.

5. CAPAIAN PEMBELAJARAN (CP)

a. Capaian Pembelajaran Program Studi (CP-Prodi)

S-1 : Bertakwa kepada Tuhan Yang Maha Esa dan mampu menunjukkan sikap religius.

S-3 : Menunjukkan sikap bertanggung jawab atas pekerjaan di bidang keahliannya secara mandiri.

KU1 : Mampu menerapkan pemikiran logis, kritis, sistematis, dan inovatif dalam konteks pengembangan atau implementasi ilmu pengetahuan dan teknologi yang memperhatikan dan menerapkan nilai humaniora yang sesuai dengan bidang keahliannya.

KU2 : Mampu menunjukkan kinerja mandiri, bermutu, dan terukur.

KU5 : Mampu mengambil keputusan secara tepat dalam konteks penyelesaian masalah di bidang keahliannya, berdasarkan hasil analisis informasi dan data.

Pengetahuan : Mahasiswa dapat memahami ring (gelanggang), daerah integral dan *field*, subring, ideal, ring faktor (*quotient ring*), ring homomorfima, ring polinomial dan algoritma pembagian (faktorisasi) polinom, ring faktor dari ring polinomial, *field* perluasan (*extension field*), daerah faktorisasi tunggal dan daerah Euclid.

Keterampilan Khusus : Mahasiswa mampu menerapkan teori ring (gelanggang), daerah integral dan *field*, subring, ideal, ring faktor (*quotient ring*), ring homomorfima, ring polinomial dan algoritma pembagian (faktorisasi) polinom, ring faktor dari ring polinomial, *field* perluasan (*extension field*), daerah faktorisasi tunggal dan daerah Euclid.

b. Capaian Pembelajaran Matakuliah (CP-MK)

M1 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan teori gelanggang (ring) dan ring komutatif dalam pemecahan masalah.

M2 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan gelanggang dengan unsur kesatuan dalam pemecahan masalah.

M3 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan daerah integral dalam pemecahan masalah.

M4 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan lapangan (*field*) dalam pemecahan masalah.

M5 : Mahasiswa dapat memahami, menganalisis dan mengaplikasikan sub-gelanggang (subring) dan Sentral suatu gelanggang dalam pemecahan masalah.

M6 : Mahasiswa dapat memahami, menganalisis dan mengaplikasikan ideal dalam pemecahan masalah.

M7 : Mahasiswa dapat memahami, menganalisis dan mengaplikasikan ideal principal, ideal prima, dan ideal maksimal dalam pemecahan masalah.

M8 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan ring faktor dalam pemecahan masalah.

M9 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan homomorfisma ring dalam pemecahan masalah.

M10 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan isomorfisma ring dalam pemecahan masalah.

M11 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan ring polinomial dalam pemecahan masalah.

M12 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan algoritma pembagian (faktorisasi) polinom dalam pemecahan masalah.

M13 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan ring faktor dari ring polinomial dalam pemecahan masalah.

M14 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan lapangan perluasan (*extension field*) dalam pemecahan masalah.

M15 : Mahasiswa dapat memahami, menganalisis, dan mengaplikasikan daerah faktorisasi tunggal dan daerah Euclid dalam pemecahan masalah.

EVALUASI DAN UMPAN BALIK PROSES PEMBELAJARAN

a. Evaluasi dari proses pembelajaran ini adalah berupa tes tertulis (uraian).

b. Pengukuran tingkat penguasaan terhadap materi dapat menggunakan rumus sebagai berikut:

$$\boxed{\textit{Tingkat penguasaan} = \frac{\textit{Banyak jawaban yang benar}}{\textit{Banyak soal}} \times 100\%}$$

c. Jika tingkat penguasaan materi yang diperoleh mahasiswa $< 70\%$, maka mahasiswa tersebut dianjurkan untuk mengulang kembali pada topik pembahasan yang belum dikuasai.

d. Akan tetapi, jika tingkat penguasaan materi yang diperoleh mahasiswa $\geq 70\%$, maka mahasiswa tersebut dapat melanjutkan pada bab berikutnya.

DAFTAR SIMBOL

Z	Himpunan semua bilangan bulat
R	Himpunan semua bilangan real
Q	Himpunan semua bilangan rasional
Z^+	Himpunan semua bilangan bulat positif
$Z^\#$	Himpunan semua bilangan bulat yang tidak negatif
R^+	Himpunan semua bilangan real positif
R^*	Himpunan semua bilangan real tidak nol
C	Himpunan semua bilangan kompleks
$\langle R, + \cdot \rangle$	Ring R terhadap operasi $+$ dan $\cdot$
$\langle a \rangle$	Ideal yang dibangun oleh a
$M_n\ (A)$	Himpunan semua matriks atas elemen-elemen dari A
$M_{m \times n}\ (R)$	Himpunan semua matriks atas bilangan real berukuran $m \times n$
$\cong$	Isomorfik
$\Phi : A \rightarrow B$	Pemetaan dari A ke B
$\Phi(a)$	Bayangan a terhadap Φ
$t \mid s$	t membagi habis s
$t \nmid s$	t tidak membagi habis s
gcd(a,b)	Faktor Persekutuan Terbesar (greatest common divisor dari a dan b)
KerΦ	Kernel dari homomorfisma Φ
$f'\ (x)$	Turunan dari $f(x)$
deg $f(x)$	Derajat dari polinomial $f(x)$
deg $g(x)$	Derajat dari polinomial $g(x)$
$R[x]$	Ring polinomial pada R
$F(x)$	*Field faktor* dari $F[x]$
$\langle a \rangle$	Ideal principal dari a
$Z[x]$	Ring Polinomial dengan koefisisen bilangan bulat
R/A	Ring Faktor
$Z\left[\sqrt{n}\right]$	$Z\left[\sqrt{n}\right] = \left\{a + b\sqrt{n} \mid a, b \in Z\right\}$, n adalah sebuah bilangan bulat positif
$Z[i]$	$Z\left[i\right] = \left\{a + bi \mid a, b \in Z\right\}$

$Z\left[i\sqrt{n}\right]$	$Z\left[i\sqrt{n}\right]=\left\{a+bi\sqrt{n}\mid a,b\in Z\right\}$ n adalah sebuah bilangan bulat positif
$Q\left[\sqrt{n}\right]$	$Q\left[\sqrt{n}\right]=\left\{a+b\sqrt{n}\mid a,b\in Q\right\}$, n adalah sebuah bilangan bulat positif
$Q[i]$	$Q\left[i\right]=\left\{a+bi\mid a,b\in Q\right\}$
$Q\left[i\sqrt{n}\right]$	$Q\left[i\sqrt{n}\right]=\left\{a+bi\sqrt{n}\mid a,b\in Q\right\}$, n adalah sebuah bilangan bulat positif

BAB 1

RING (GELANGGANG)

Tujuan Instruksional Umum

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan dapat memahami dan mengaplikasikan aksioma-aksioma terbentuknya ring (gelanggang), ring komutatif, dan ring dengan unsur kesatuan.

Tujuan Instruksional Khusus

Setelah diberikan penjelasan mengenai aksioma-aksioma terbentuknya ring, ring komutatif, dan ring dengan unsur kesatuan, maka mahasiswa diharapkan dapat:

a. Menjelaskan definisi terkait ring (gelanggang), ring komutatif, dan ring dengan unsur kesatuan.
b. Mengidentifikasikan suatu grup apakah merupakan ring atau bukan.
c. Mengidentifikasikan suatu ring apakah merupakan ring komutatif atau bukan.
d. Mengidentifikasikan suatu ring apakah merupakan ring dengan unsur kesatuan atau bukan.
e. Memberikan contoh dan bukan contoh dari suatu ring, ring komutatif, maupun ring dengan unsur kesatuan.

Deskripsi Singkat

Ring (gelanggang) merupakan suatu himpunan yang tidak kosong dan memenuhi dua operasi biner yaitu, penjumlahan dan perkalian. Pada bab ini, akan dibahas mengenai sifat-sifat terbentuknya suatu ring, ring komutatif, dan ring dengan unsur kesatuan.

1.1 RING

Pada pembahasan sebelumnya, kita telah mempelajari struktur aljabar grup yang hanya menggunakan sebuah operasi biner. Namun, pada bab ini, kita akan membahas tentang struktur aljabar yang melibatkan dua operasi biner atau lebih, misalnya ring (gelanggang) yang akan didefinisikan sebagai berikut:

Definisi 1.1.

Sebuah himpunan R yang tidak kosong dengan operasi biner $+$ dan $\cdot$ dikatakan sebuah Ring (Gelanggang) jika memenuhi aksioma-aksioma sebagai berikut:

i) $\langle R, +\rangle$ merupakan sebuah grup komutatif (abelian)
   a) Memenuhi sifat tertutup (*closure*)
   b) Bersifat asosiatif terhadap operasi biner $+$
   c) Memiliki unsur identitas
   d) Setiap unsur memiliki invers
   e) Berlaku komutatif $+$

ii) $\langle R, \cdot\rangle$ merupakan sebuah semigrup (assosiatif terhadap operasi biner $\cdot$)

iii) $\forall\ a, b, c \in R$ berlaku $a\cdot(b+c) = ab + ac$ dan $(a+b)\cdot c = ac + bc$

Dari aksioma-aksioma di atas dapat kita turunkan menjadi:

i) $\langle R, +\rangle$ sebuah grup abelian

ii) Assosiatif terhadap operasi $\cdot$

iii) Memenuhi hukum distributif kiri dan kanan

Contoh 1.1:

Misalkan $\langle Z_8, +, \cdot\rangle$ merupakan himpunan bilangan bulat modulo 8 dengan operasi penjumlahan dan perkalian. Buktikan bahwa $\langle Z_8, +, \cdot\rangle$ membentuk sebuah ring (gelanggang).

Penyelesaian:

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Akan dibuktikan bahwa:

i) $\langle Z_8, +\rangle$ merupakan grup abelian
   a) Memenuhi sifat tertutup

TABEL 1.1. Tabel Cayley Z_8 dengan Operasi Biner Penjumlahan

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

Terbukti memenuhi sifat tertutup, karena tidak ada unsur lain selain unsur Z_8.

b) Asosiatif terhadap operasi biner $+$

Ambil sebarang unsur, misal $a=5, b=6, c=7, \forall a,b,c \in Z_8$

$$a+(b+c) = (a+b)+c$$
$$5+(6+7)=(5+6)+7$$
$$5+5=3+7$$
$$2=2$$

Terbukti asosiatif terhadap operasi biner $+$

c) Terdapat unsur identitas, yaitu $i=0$ sehingga $a+0=a$

d) Setiap unsur memiliki invers

$0^{-1}=0$ karena $0+0=0=i$
$1^{-1}=7$ karena $1+7=0=i$
$1^{-1}=7$ karena $1+7=0=i$
$2^{-1}=6$ karena $2+6=0=i$
$3^{-1}=5$ karena $3+5=0=i$
$4^{-1}=4$ karena $4+4=0=i$
$5^{-1}=3$ karena $5+3=0=i$
$6^{-1}=2$ karena $6+2=0=i$
$7^{-1}=1$ karena $7+1=0=i$

e) Berlaku komutatif $+$

$$a+b=b+a$$
$$5+6=6+5$$
$$3=3$$

Terbukti berlaku komutatif $+$

Terbukti $\langle Z_8, + \rangle$ merupakan grup abelian

ii) $\langle R, \cdot \rangle$ merupakan sebuah semigrup (asosiatif terhadap operasi biner $\cdot$)

Tabel 1.2. Tabel Cayley dengan Operasi Biner Perkalian

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Ambil sebarang unsur, misal $a=5$, $b=6$, $c=7, \forall a, b, c \in Z_8$

$$
\begin{aligned}
a \cdot (b \cdot c) &= (a \cdot b) \cdot c \\
5 \cdot (6 \cdot 7) &= (5 \cdot 6) \cdot 7 \\
5 \cdot 2 &= 6 \cdot 7 \\
2 &= 2
\end{aligned}
$$

Terbukti merupakan semigrup

iii) Memenuhi hukum distributif kiri dan kanan

Akan dibuktikan memenuhi hukum distributif kiri

$$
\begin{aligned}
a \cdot (b+c) &= ab+ac \\
5 \cdot (6+7) &= 5 \cdot 6+5 \cdot 7 \\
5 \cdot 5 &= 6+3 \\
1 &= 1
\end{aligned}
$$

Terbukti $\langle Z_8, +, \cdot \rangle$ memenuhi hukum distributif kiri

Akan dibuktikan memenuhi hukum distributif kanan

$$
\begin{aligned}
(a+b) \cdot c &= ac+bc \\
(5+6) \cdot 7 &= 5 \cdot 7+6 \cdot 7 \\
3 \cdot 7 &= 3+2 \\
5 &= 5
\end{aligned}
$$

Terbukti $\langle Z_8, +, \cdot \rangle$ memenuhi hukum distributif kanan

Oleh karenanya, terbukti bahwa $\langle Z_8, +, \cdot \rangle$ memenuhi hukum distributif kiri dan kanan

$\therefore$ Terbukti bahwa $\langle Z_8, +, \cdot \rangle$ membentuk sebuah ring (gelanggang)

Contoh 1.2:

Buktikan bahwa $M = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a, b \in Z \right\}$ yang didefinisikan pada operasi penjumlahan dan perkalian matriks merupakan suatu ring.

Penyelesaian:

i) Akan dibuktikan bahwa $\langle M, + \rangle$ membentuk grup abelian

(a) Bersifat tertutup terhadap operasi penjumlahan

$\forall A, B \in M \rightarrow A+B \in M$

Ambil sembarang unsur $\forall A, B \in M$

Misal:

$$A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \text{ dan } B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$$

$$A+B=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}+\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$$

$$=\begin{bmatrix} a+c & 0 \\ 0 & b+d \end{bmatrix} \text{dimana } a+c \text{ dan } b+d\in Z$$

Terbukti $A+B\in M$

(b) Bersifat Asosiatif

$\forall A, B, C \in M \rightarrow (A + B) + C = A + (B + C)$

Misal:

$$A=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix},\ B=\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}, \text{dan } C=\begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

$$(A+B)+C \qquad = A+(B+C)$$

$$\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}+\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}\right)+\begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}+\left(\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}+\begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}\right)$$

$$\begin{bmatrix} a+c+e & 0 \\ 0 & b+d+f \end{bmatrix} = \begin{bmatrix} a+c+e & 0 \\ 0 & b+d+f \end{bmatrix}$$

Terbukti $(A+B)+C = A+(B+C)$

(c) Mempunyai unsur identitas

$\exists I\in M$, sedemikian sehingga $\forall A\in M$, berlaku $A+I = I+A= A$

Yaitu: $I=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$

(d) Setiap unsur mempunyai invers

$\forall A\in M, \exists A^{-1} \in M$, sedemikian sehingga $A+A^{-1}=A^{-1}+A=I$ dimana A^{-1} adalah invers dari elemen A.

dalam hal ini $A^{-1}=-A=\begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix}$, sehingga

$$A+A^{-1}=\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}+\begin{bmatrix} -a & 0 \\ 0 & -b \end{bmatrix}$$

$$=\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

Terbukti $A+A^{-1}=A^{-1}+A=I$

(e) Bersifat komutatif

$$\forall A \in M, A + B = B + A$$

$$A + B = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}$$

$$= \begin{bmatrix} a + c & 0 \\ 0 & b + d \end{bmatrix}$$

$$= \begin{bmatrix} c + a & 0 \\ 0 & d + b \end{bmatrix}$$

$$= B + A$$

Terbukti $\langle M, \cdot \rangle$ merupakan grup abelian

ii) Akan dibuktikan bahwa $\langle M, \cdot \rangle$ membentuk semigrup (asosiatif perkalian).

$$\forall a, b, c \in Z \rightarrow (a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Ambil sembarang unsur, misal:

$$A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}, \text{ dan } C = \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

$$(A \cdot B) \cdot C = A \cdot (B \cdot C)$$

$$\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \right) \cdot \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \left(\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \cdot \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix} \right)$$

$$\begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \cdot \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} ce & 0 \\ 0 & df \end{bmatrix}$$

$$\begin{bmatrix} ace & 0 \\ 0 & bdf \end{bmatrix} = \begin{bmatrix} ace & 0 \\ 0 & bdf \end{bmatrix}$$

Terbukti asosiatif perkalian, maka $\langle M, \cdot \rangle$ membentuk semigrup

iii) Akan dibuktikan memenuhi hukum distributif kiri dan distributif kanan.

Ambil sembarang unsur, misal:

$$A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, B = \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix}, \text{ dan } C = \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

$$\forall a, b, c \in Z \rightarrow a \cdot (b + c) = a \cdot b + a \cdot c$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \left(\begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} + \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix} \right) = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} + \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} c+e & 0 \\ 0 & d+f \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} + \begin{bmatrix} ae & 0 \\ 0 & bf \end{bmatrix}$$

$$\begin{bmatrix} ac+ae & 0 \\ 0 & bd+bf \end{bmatrix} = \begin{bmatrix} ac+ae & 0 \\ 0 & bd+bf \end{bmatrix}$$

Terbukti memenuhi hukum distributif kiri.

$\forall a,b,c \in Z \to (a+b)\cdot c = a\cdot c + b\cdot c$

$$\left(\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \right) \cdot \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \cdot \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix} + \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \cdot \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix}$$

$$\begin{bmatrix} a+c & 0 \\ 0 & b+d \end{bmatrix} \cdot \begin{bmatrix} e & 0 \\ 0 & f \end{bmatrix} = \begin{bmatrix} ae & 0 \\ 0 & bf \end{bmatrix} + \begin{bmatrix} ce & 0 \\ 0 & df \end{bmatrix}$$

$$\begin{bmatrix} ae+ce & 0 \\ 0 & bf+df \end{bmatrix} = \begin{bmatrix} ae+ce & 0 \\ 0 & bf+df \end{bmatrix}$$

Terbukti memenuhi hukum distributif kanan.

$\therefore$ Terbukti bahwa $\langle M, + \cdot \rangle$ dengan $M = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \middle| a,b \in Z \right\}$ membentuk ring (gelanggang).

1.2 RING KOMUTATIF

Definisi 1.2:

Sebuah ring yang komutatif terhadap operasi $\cdot$ dikatakan **Ring (Gelanggang) Komutatif.** Atau dengan kata lain, jika $\langle R, +, \cdot \rangle$ adalah semigrup komutatif terhadap operasi $\cdot$ maka $\langle R, +, \cdot \rangle$ disebut **Ring (Gelanggang) Komutatif.**

Contoh 1.3:

Buktikan bahwa Z adalah himpunan semua bilangan bulat didefinisikan dengan operasi $+$ dan $\cdot$ berturut-turut operasi penjumlahan dan perkalian, maka $\langle Z, +, \cdot \rangle$ merupakan sebuah Ring.

Penyelesaian:

a. Dapat dengan mudah kita lihat bahwa $\langle Z,+,\cdot\rangle$ merupakan sebuah grup abelian.

b. $\langle Z,\cdot\rangle$ merupakan sebuah semi grup.

c. Serta kita ketahui bahwa operasi $+$ dan $\cdot$ memenuhi hukum distributif kiri dan kanan, terbuktilah bahwa $\langle Z,+,\cdot\rangle$ sebuah Ring (gelanggang), bahkan gelanggangnya komutatif.

Contoh 1.4:

$S=\{1,\ 2,3\ \}$, $P(S)$ adalah himpunan kuasa dari S, didefinisikan operasi biner $P(S)$ sebagai berikut:

$$A+B=(A\cup B)-(A\cap B)$$
$$A\cdot B=A\cap B$$

Tunjukkan bahwa $\langle P\ (S),+,\cdot\rangle$ adalah sebuah ring komutatif.

Penyelesaian:

$$P(S)=\{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$$

Untuk menunjukkan sebuah gelanggang, maka akan kita buat terlebih dahulu tabel Cayley terhadap operasi $+$ dan $\cdot$ sebagai berikut:

TABEL 1.3. Tabel Cayley terhadap Operasi + pada P(S) dengan S = {1, 2, 3}

+	∅	{1}	{2}	{3}	{1,2}	{1,3}	{2,3}	{1,2,3}
∅	∅	{1}	{2}	{3}	{1,2}	{1,3}	{2,3}	{1,2,3}
{1}	{1}	∅	{1,2}	{1,3}	{2}	{3}	{1,2,3}	{2,3}
{2}	{2}	{1,2}	∅	{2,3}	{1}	{1,2,3}	{3}	{1,3}
{3}	{3}	{1,3}	{2,3}	∅	{1,2,3}	{1}	{2}	{1,2}
{1,2}	{1,2}	{2}	{1}	{1,2,3}	∅	{2,3}	{1,3}	{3}
{1,3}	{1,3}	{3}	{1,2,3}	{1}	{2,3}	∅	{1,2}	{2}
{2,3}	{2,3}	{1,2,3}	{3}	{2}	{1,3}	{1,2}	∅	{1}
{1,2,3}	{1,2,3}	{2,3}	{1,3}	{1,2}	{3}	{2}	{1}	∅

a) Jelas dari tabel di atas merupakan sebuah grup abelian, karena memenuhi sifat berikut:

1) Tertutup, karena tidak ada unsur lain selain unsur *P(S)*
2) Asosiatif terhadap operasi biner $+$

Ambil sebarang unsur, misal:

$$a=\{1\},b=\{1,3\},c=\{2,3\};\forall a,b,c\in P(S)$$

$$(a+b)+c = a+(b+c)$$

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

$$\{3\}+\{2,3\}=\{1\}+\{1,2\}$$

$$\{2\}=\{2\}$$

3) Memiliki unsur identitas, yaitu: $i=\varnothing$
   Sebab $\varnothing+\{1,3\}=\{1,3\}$

4) Setiap unsur memiliki invers, yaitu:
   $\varnothing^{-1}=\varnothing$
   $\{1\}^{-1}=\{1\}$
   $\{2\}^{-1}=\{2\}$
   $\{3\}^{-1}=\{3\}$
   $\{1,2\}^{-1}=\{1,2\}$
   $\{1,3\}^{-1}=\{1,3\}$
   $\{2,3\}^{-1}=\{2,3\}$
   $\{1,2,3\}^{-1}=\{1,2,3\}$

5) Grup abelian

$$a+b=b+a$$

$$\{1\}+\{1,3\}=\{1,3\}+\{1\}$$

$$\{3\}=\{3\}$$

b) Untuk membuktikan $\langle P(S),\cdot\rangle$ semigrup, maka perlu kita buat tabel Cayley dengan operasi $\cdot$ sebagai berikut:

Tabel 1.4. Tabel Cayley terhadap Operasi • pada *P(S)* dengan S = {1, 2, 3}

•	∅	{1}	{2}	{3}	{1,2}	{1,3}	{2,3}	{1,2,3}
∅	∅	∅	∅	∅	∅	∅	∅	∅
{1}	∅	{1}	∅	∅	{1}	{1}	∅	{1}
{2}	∅	∅	{2}	∅	{2}	∅	{2}	{2}
{3}	∅	∅	∅	{3}	∅	{3}	{3}	{3}
{1,2}	∅	{1}	{2}	∅	{1,2}	{1}	{2}	{1,2}
{1,3}	∅	{1}	∅	{3}	{1}	{1,3}	{3}	{1,3}
{2,3}	∅	∅	{2}	{3}	{2}	{3}	{2,3}	{2,3}
{1,2,3}	∅	{1}	{2}	{3}	{1,2}	{1,3}	{2,3}	{1,2,3}

Ambil sebarang unsur, misal:

$$a = \{1\}, b = \{1,3\}, c = \{2,3\}; \forall a,b,c \in P(S)$$

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

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

$$\{1\} \cdot \{2,3\} = \{1\} \cdot \{3\}$$

$$\varnothing = \varnothing$$

Terbukti semigrup

c) Apakah berlaku hukum distributif kiri dan kanan?

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$\{1\} \cdot (\{1,3\} + \{2,3\}) = \{1\} \cdot \{1,3\} + \{1\} \cdot \{2,3\}$$

$$\{1\} \cdot \{1,2\} = \{1\} + \varnothing$$

$$\{1\} = \{1\}$$

Terbukti distributif kiri

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

$$(\{1\} + \{1,3\}) \cdot \{2,3\} = \{1\} \cdot \{2,3\} + \{1,3\} \cdot \{2,3\}$$

$$\{3\} \cdot \{2,3\} = \varnothing + \{3\}$$

$$\{3\} = \{3\}$$

Terbukti distributif kanan

d) Apakah $\langle P(S), +, \cdot \rangle$ merupakan Ring (gelanggang) abelian?

$$a \cdot b = b \cdot a$$

$$\{1\} \cdot \{1, 3\} = \{1, 3\} \cdot \{1\}$$

$$\{1\} = \{1\}$$

$\therefore$ Terbukti bahwa $\langle P(S), +, \cdot \rangle$ adalah sebuah ring komutatif.

Contoh 1.5:

Buktikan bahwa $\langle Z_3 \times Z_6 \rangle$ merupakan ring komutatif untuk operasi penjumlahan dan perkalian.

Penyelesaian:

$$Z_3 \times Z_6 = \{0,1,2\} \times \{0,1,2,3,4,5\}$$

$$= \{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (1,0), (1,1), (1,2), (1,3), (1,4), (1,5)\ (2,0), (2,1), (2,2), (2,3), (2,4), (2,5)\}$$

Untuk lebih memudahkan dalam proses pembuktian, maka terlebih dahulu kita buat tabel Cayley untuk operasi penjumlahan dan perkalian sebagai berikut:

Tabel 1.5. Tabel Cayley $Z_3 \times Z_6$ untuk Operasi Penjumlahan

+	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
(0,0)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
(0,1)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,0)
(0,2)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,0)	(1,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,0)	(2,1)
(0,3)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(1,3)	(1,4)	(1,5)	(1,0)	(1,1)	(1,2)	(2,3)	(2,4)	(2,5)	(2,0)	(2,1)	(2,2)
(0,4)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(1,4)	(1,5)	(1,0)	(1,1)	(1,2)	(1,3)	(2,4)	(2,5)	(2,0)	(2,1)	(2,2)	(2,3)
(0,5)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(1,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(2,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)
(1,0)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)
(1,1)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)
(1,2)	(1,2)	(1,3)	(1,4)	(1,5)	(1,0)	(1,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,0)	(2,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)
(1,3)	(1,3)	(1,4)	(1,5)	(1,0)	(1,1)	(1,2)	(2,3)	(2,4)	(2,5)	(2,0)	(2,1)	(2,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)
(1,4)	(1,4)	(1,5)	(1,0)	(1,1)	(1,2)	(1,3)	(2,4)	(2,5)	(2,0)	(2,1)	(2,2)	(2,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)
(1,5)	(1,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(2,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)
(2,0)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)
(2,1)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(2,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,0)
(2,2)	(2,2)	(2,3)	(2,4)	(2,5)	(2,0)	(2,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(1,2)	(1,3)	(1,4)	(1,5)	(1,0)	(1,1)
(2,3)	(2,3)	(2,4)	(2,5)	(2,0)	(2,1)	(2,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(1,3)	(1,4)	(1,5)	(1,0)	(1,1)	(1,2)
(2,4)	(2,4)	(2,5)	(2,0)	(2,1)	(2,2)	(2,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(1,4)	(1,5)	(1,0)	(1,1)	(1,2)	(1,3)
(2,5)	(2,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(1,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)

Tabel 1.6. Tabel Cayley $Z_3 \times Z_6$ untuk Operasi Perkalian

•	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)
(0,2)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)
(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)
(0,4)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)
(0,5)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)
(1,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)
(1,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
(1,2)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(1,0)	(1,2)	(1,4)	(1,0)	(1,2)	(1,4)	(2,0)	(2,2)	(2,4)	(2,0)	(2,2)	(2,4)
(1,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(1,0)	(1,3)	(1,0)	(1,3)	(1,0)	(1,3)	(2,0)	(2,3)	(2,0)	(2,3)	(2,0)	(2,3)
(1,4)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(1,0)	(1,4)	(1,2)	(1,0)	(1,4)	(1,2)	(2,0)	(2,4)	(2,2)	(2,0)	(2,4)	(2,2)
(1,5)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(1,0)	(1,5)	(1,4)	(1,3)	(1,2)	(1,1)	(2,0)	(2,5)	(2,4)	(2,3)	(2,2)	(2,1)
(2,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)
(2,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)
(2,2)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(2,0)	(2,2)	(2,4)	(2,0)	(2,2)	(2,4)	(1,0)	(1,2)	(1,4)	(1,0)	(1,2)	(1,4)
(2,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(2,0)	(2,3)	(2,0)	(2,3)	(2,0)	(2,3)	(1,0)	(1,3)	(1,0)	(1,3)	(1,0)	(1,3)
(2,4)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(2,0)	(2,4)	(2,2)	(2,0)	(2,4)	(2,2)	(1,0)	(1,4)	(1,2)	(1,0)	(1,4)	(1,2)
(2,5)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(2,0)	(2,5)	(2,4)	(2,3)	(2,2)	(2,1)	(1,0)	(1,5)	(1,4)	(1,3)	(1,2)	(1,1)

(a) Dari tabel Cayley $Z_3 \times Z_6$ untuk operasi penjumlahan dikatakan tertutup, karena tidak menghasilkan unsur lain selain unsur $Z_3 \times Z_6$.

(*b*) Akan dibuktikan asosiatif pada operasi penjumlahan
Ambil sembarang unsur, misal: $a = (1,5), b = (2,0), c = (2,5)$;

$$\forall a,b,c \in Z_3 \times Z_6$$
$$(a+b)+c = a+(b+c)$$
$$((1,5)+(2,0))+(2,5) = (1,5)+((2,0)+(2,5))$$
$$(0,5)+(2,5) = (1,5)+(1,5)$$
$$(2,4) = (2,4)$$

Terbukti asosiatif terhadap operasi penjumlahan

(c) Memiliki unsur identitas yaitu: $i = (0, 0)$

(d) Setiap unsur memiliki invers, yaitu:

$(0,0)^{-1} = (0,0)$
$(0,1)^{-1} = (0,5)$
$(0,2)^{-1} = (0,4)$
$(0,3)^{-1} = (0,3)$
$(0,4)^{-1} = (0,2)$
$(0,5)^{-1} = (0,1)$
$(1,0)^{-1} = (2,0)$
$(1,1)^{-1} = (2,5)$
$(1,2)^{-1} = (2,4)$
$(1,3)^{-1} = (2,3)$
$(1,4)^{-1} = (2,2)$
$(1,5)^{-1} = (2,1)$
$(2,0)^{-1} = (1,0)$
$(2,1)^{-1} = (1,5)$
$(2,2)^{-1} = (1,4)$
$(2,3)^{-1} = (1,3)$
$(2,4)^{-1} = (1,2)$
$(2,5)^{-1} = (1,1)$

(e) Akan dibuktikan abelian (komutatif)

$$a + b = b + a$$
$$(1,5) + (2,0) = (2,0) + (1,5)$$
$$(0,5) = (0,5)$$

(f) Asosiatif terhadap operasi perkalian

$$(a \cdot b) \cdot c = a. (b \cdot c)$$
$$((1,5) \cdot (2,0)) \cdot (2,5) = (1,5) \cdot ((2,0) \cdot (2,5))$$
$$(2,0) \cdot (2,5) = (1,5) \cdot (1,0)$$
$$(1,0) = (1,0)$$

(g) Akan dibuktikan distributif kiri dan distributif kanan

$$\mathrm{a} \cdot (b + c) = a \cdot b + a \cdot c$$
$$(1,5) \cdot ((2,0) + (2,5)) = (1,5) \cdot (2,0) + (1,5) \cdot (2,5)$$
$$(1,5) \cdot (1,5) = (2,0) + (2,1)$$
$$(1,1) = (1,1)$$

Terbukti distributif kiri

$$(a + b) \cdot c = a \cdot c + b \cdot c$$
$$((1,5) + (2,0)) \cdot (2,5) = (1,5) \cdot (2,5) + (2,0) \cdot (2,5)$$
$$(0,5) \cdot (2,5) = (2,1) + (1,0)$$

$$(0,1) = (0,1)$$

Terbukti distributif kanan

$\therefore$ Terbukti $Z_3 \times Z_6$ merupakan ring komutatif dengan operasi penjumlahan dan perkalian.

Contoh 1.6:

Misalkan $M_2(Z)$ dinotasikan dengan himpunan semua matriks 2×2 pada ring dari bilangan bulat. Misalkan $+$ dan $\cdot$ notasi yang biasa digunakan untuk penjumlahan dan perkalian. Maka $+$ dan $\cdot$ adalah operasi biner pada $M_2(Z)$. Sangat mudah untuk menunjukkan bahwa $\langle M_2(Z)\rangle, +, \cdot$ adalah sebuah ring. Catat bahwa $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ adalah identitas penjumlahan untuk $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(Z)$,

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

Ambil sembarang unsur, misal $A = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}, B = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}, \forall A, B \in M_2(Z)$, maka:

$$AB = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}\begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix} = \begin{bmatrix} 19 & 22 \\ 43 & 50 \end{bmatrix}$$

$$BA = \begin{bmatrix} 5 & 6 \\ 7 & 8 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix} = \begin{bmatrix} 23 & 34 \\ 31 & 46 \end{bmatrix}$$

Sehingga $AB \neq BA$

Oleh karena itu, $M_2(Z)$ bukan merupakan ring komutatif.

1.3 RING DENGAN UNSUR KESATUAN

Definisi 1.3.

Misalkan R adalah ring, sebuah elemen $e \in R$ disebut **elemen identitas**, jika $ea = a = ae$ untuk semua $a \in R$.

Definisi 1.4.

Sebuah ring R disebut **ring dengan identitas** jika mempunyai sebuah identitas.

Contoh 1.7:

Ring Z dari bilangan bulat adalah ring dengan identitas. Bilangan bulat 1 adalah elemen identitas dari Z.

Contoh 1.8:

Misalkan n adalah bilangan bulat positif. Ring komutatif $\langle Z_n, +, \cdot \rangle$ dengan identitas. Elemen identitas adalah [1].

Contoh 1.9:

Ring $M_2(Z)$ adalah ring dengan identitas. Elemen identitas dari $M_2(Z)$ adalah $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$.

Contoh 1.10:

Misalkan R dinotasikan sebagai himpunan semua fungsi f:R→R. Didefinisikan + dan · pada R untuk semua f,g∈R dan untuk semua a∈R sebagai berikut:

$$(f+g)(a) = f(a) + g(a)$$
$$(f \cdot g)(a) = f(a) \cdot g(a)$$

Dari definisi + dan · dapat ditunjukkan bahwa + dan · adalah operasi biner pada R. Misalkan f, g, $h \in R$. Maka untuk semua $a \in R$, kita menggunakan asosiatif di R, yaitu:

$$((f+g)+h)(a) = (f+g)(a) + h(a) = (f(a) + g(a)) + h(a)$$
$$= f(a) + (g(a) + h(a)) = f(a) + (g(a) + h(a)) = f(a) + (g+h)(a)$$
$$= (f + (g+h))(a).$$

Dengan demikian $(f+g)+h = f+(g+h)$.
Dengan demikian terbukti bahwa + bersifat asosiatif.
Dengan cara yang sama, akan kita tunjukkan bahwa R dengan menggunakan fakta yang ada pada R, maka $\langle R, +, \cdot \rangle$ adalah sebuah ring.
Kita catat bahwa fungsi i_0: $R \to R$, dimana $i_0(a) = 0$ untuk semua $a \in R$ adalah identitas penjumlahan pada R dan elemen $i_1 \in R$ dimana $i_1(a) = 1$ untuk semua $a \in R$ adalah identitas di R. Juga untuk semua $f,g \in R$ dan untuk semua $a \in R$, maka:

$$(f \cdot g)(a) = f(a)g(a) = g(a)f(a) = (g \cdot f)(a)$$

Dengan demikian untuk semua f, $g \in R$, $f \cdot g = g \cdot f$.

Terbukti bahwa $\langle R, +, \cdot \rangle$ adalah ring komutatif dengan identitas.

Definisi 1.5.

Jika $\langle R, \cdot \rangle$ adalah monoid dengan unsur identitas 1, maka ring $\langle R, +, \cdot \rangle$ dikatakan **Ring dengan unsur kesatuan (*ring* dengan *unity*)** yakni jika terdapat satu unsur yang dinotasikan dengan 1 sedemikian sehingga $1 \cdot a = a \cdot 1$ untuk setiap a anggota R, maka kita sebut ring dengan unsur kesatuan, dan **unsur 1 disebut sebagai unsur kesatuan (*unity*)**.

Contoh 1.11:

Ring $\langle Z_6, +, \cdot \rangle$ adalah ring dengan unsur kesatuan 1 (ring dengan *unity*)

Penyelesaian:

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

Tabel 1.7. Tabel Cayley dengan Operasi Biner Perkalian pada Z_6

•	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Dari tabel di atas jelas terlihat bahwa $\langle Z_6, +, \cdot \rangle$ adalah ring dengan unsur kesatuan 1 karena memiliki unsur satuan yaitu 1 dan 5

Teorema 1.1.

Andaikan R adalah suatu ring, maka:

1) $0 \cdot a = a \cdot 0 = 0$ untuk semua $a \in R$
2) $a(-b) = -(ab) = (-a)b$ untuk semua a, $b \in R$
3) $(-a)(-b) = ab$, untuk semua a, $b \in R$
4) $m(ab) = (ma)b = a(mb)$ untuk setiap bilangan bulat m
5) $mn(ab) = (ma)(nb)$ untuk setiap bilangan bulat m dan n

1) Untuk menunjukkan $a \cdot 0 = 0$ cukup dengan menunjukkan:
   $a \cdot 0 + a \cdot 0 = a(0+0) = a \cdot 0 = 0$ atau
   $0 \cdot a + 0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$, karena $\langle R, + \rangle$ sebuah grup maka

$0 \cdot a = 0$ terbukti.

2) Perhatikan $0 = a \cdot 0 = a(b + (-b)) = ab + a(-b)$ tetapi $0 = ab + -(ab)$, sehingga $ab + a(-b)$ karena $\langle R, + \rangle$ grup, maka $a(-b) = -(ab)$
dengan cara yang sama dapat kita perlihatkan bahwa:
$(-a)b \;\; = -(ab)$
$0 = 0\mathrm{b} = (a + (-a))b$
$\quad = ab + (-a)b$
$\quad = ab + -(ab)$
sehingga: $(\text{-}a)b = -(ab)$

3) Akan diperlihatkan $(-a)(-b) = ab$
$(-a)(-b) = -((-a)b) = -(-(-ab))$
Tetapi $-(ab) + (-(-(ab))) = 0$ dan
$-(ab) + ab = 0$, sehingga:
$ab = -(-(ab)) = (-a)(-b)$ terbukti

4) dan 5) sebagai latihan.

Definisi 1.6:

Andaikan R adalah ring dengan unsur kesatuan 1. Satu unsur $\mathrm{a} \neq 0 \in \mathrm{R}$ dikatakan unsur satuan (unit) bila terdapat $\mathrm{b} \neq 0 \in \mathrm{R}$ sehingga $ab = \mathrm{ba} = 1$

Contoh 1.12:

$\langle Z, +, \cdot \rangle$ adalah sebuah ring komutatif dengan unsur kesatuan.

Contoh 1.13:

$\langle 2Z, +, \cdot \rangle$ adalah sebuah ring komutatif tetapi tidak dengan unsur kesatuan.

Contoh 1.14:

Himpunan semua bilangan riel yang disajikan dalam bentuk $a + b\sqrt{2}$, di mana $a, b \in Z$, dengan operasi + dapat disajikan:

$\left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right) = \left(ac\right) + bd\sqrt{2}$ dan operasi $\cdot$ menjadi:

$\left(a + b\sqrt{2}\right) \cdot \left(c + d\sqrt{2}\right) = \left(ac + 2bd\right) + \left(ad + bc\right)\sqrt{2}$ akan membentuk sebuah ring komutatif dengan unsur kesatuan.

Contoh 1.15:

$\langle Z_7, +, \cdot \rangle$ himpunan bilangan bulat modulo n dengan operasi biner penjumlahan dan perkalian akan membentuk sebuah ring dengan unsur kesatuan 1.

Contoh 1.16:

Tentukanlah unsur satuan dari ring $\langle Z_7, +, \cdot \rangle$

Penyelesaian:

Untuk menyelesaikannya lebih mudah dengan membuat tabel Cayley dengan operasi $\cdot$ pada Z_7 seperti pada Tabel 1.8.

Tabel 1.8. Tabel Cayley dengan Operasi Biner Perkalian pada Z_7

•	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Dari tabel di atas, dapat dengan jelas terlihat bahwa selain unsur kesatuan semua elemennya unsur satuan (unit).

Contoh 1.17:

Tentukanlah unsur satuan dari ring $\langle Z_8, +, \cdot \rangle$

Penyelesaian:

Tabel 1.9. Tabel Cayley Operasi Biner Perkalian pada Z_8

•	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Dari tabel di atas dapat kita lihat yang menjadi unsur satuan adalah {1,3,5,7} dengan unsur kesatuan 1.

Sehingga dapat kita simpulkan bahwa unsur satuan dari ring ⟨Z_n, +,·⟩ adalah prima relatif terhadap *n*.

Contoh 1.18:

Tentukan semua unsur satuan dan unsur kesatuan dari ring

Penyelesaian:

$Z_3 \times Z_6 = \{0,1,2\} \times \{0,1,2,3,4,5\}$
$= \{(0,0),\ (0,1),\ (0,2),\ (0,3),\ (0,4),\ (0,5),\ (1,0),\ (1,1),\ (1,2),\ (1,3),\ (1,4),\ (1,5),\ (2,0),\ (2,1),\ (2,2),\ (2,3),\ (2,4),\ (2,5)\}$

Tabel 1.10. Tabel Cayley Operasi Biner Perkalian pada $\langle Z_3 \times Z_6 \rangle$

•	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)
(0,2)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)
(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)
(0,4)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)
(0,5)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)
(1,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)
(1,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
(1,2)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(1,0)	(1,2)	(1,4)	(1,0)	(1,2)	(1,4)	(2,0)	(2,2)	(2,4)	(2,0)	(2,2)	(2,4)
(1,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(1,0)	(1,3)	(1,0)	(1,3)	(1,0)	(1,3)	(2,0)	(2,3)	(2,0)	(2,3)	(2,0)	(2,3)
(1,4)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(1,0)	(1,4)	(1,2)	(1,0)	(1,4)	(1,2)	(2,0)	(2,4)	(2,2)	(2,0)	(2,4)	(2,2)
(1,5)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(1,0)	(1,5)	(1,4)	(1,3)	(1,2)	(1,1)	(2,0)	(2,5)	(2,4)	(2,3)	(2,2)	(2,1)
(2,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)
(2,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)
(2,2)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(2,0)	(2,2)	(2,4)	(2,0)	(2,2)	(2,4)	(1,0)	(1,2)	(1,4)	(1,0)	(1,2)	(1,4)
(2,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(2,0)	(2,3)	(2,0)	(2,3)	(2,0)	(2,3)	(1,0)	(1,3)	(1,0)	(1,3)	(1,0)	(1,3)
(2,4)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(2,0)	(2,4)	(2,2)	(2,0)	(2,4)	(2,2)	(1,0)	(1,4)	(1,2)	(1,0)	(1,4)	(1,2)
(2,5)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(2,0)	(2,5)	(2,4)	(2,3)	(2,2)	(2,1)	(1,0)	(1,5)	(1,4)	(1,3)	(1,2)	(1,1)

Unsur satuannya adalah (1,1), (1,5), (2,1), dan (2,5) dengan unsur kesatuan adalah (1,1).

Teorema 1.2:

Andaikan R ring dengan unsur kesatuan 1, himpunan semua unsur satuan yang berada di ring R membentuk grup dengan operasi perkalian.
Bukti: Andaikan G himpunan semua unsur satuan di R, maka: karena G berada di R maka operasinya jelas biner, sehingga kita tinggal membuktikan apakah unsur satuannya asosiatif:

1) Asosiatif, sebab operasi perkalian asosiatif, dan unsur identitasnya adalah 1 (unsur kesatuan).
2) Untuk setiap $a \in G$, maka $aa^{-1} = a^{-1}\ a = 1$, jadi $a^{-1} \in G$
3) Bila g, $h \in G$, akan diperlihatkan $gh \in G$
   Jika g, $h \in G$, maka g^{-1}, $h^{-1} \in G$
   Perhatikan $h^{-1}\ g^{-1} \in R$, akibatnya $(gh)(h^{-1}\ g^{-1}) = 1$ jadi $gh \in G$
   $g \in G \rightarrow g^{-1} \in G$
   $h \in G \rightarrow h^{-1} \in G$, sehingga
   $gh \in G \rightarrow (gh)^{-1} \in G$
   Karena $gh \in G \rightarrow (gh)\ (h^{-1}\ g^{-1}) = 1$
   $(h^{-1}\ g^{-1})\ (gh) = 1$

RANGKUMAN

1. Ring adalah suatu himpunan tak kosong yang memenuhi dua operasi biner terhadap penjumlahan dan perkalian.
2. Sebuah himpunan R yang tidak kosong dengan operasi biner + dan . dikatakan sebuah Ring (Gelanggang) jika memenuhi aksioma-aksioma berikut:
   a. $\langle R, + \rangle$ merupakan sebuah grup abelian
   b. $\langle R, \cdot \rangle$ merupakan sebuah semigrup (assosiatif terhadap operasi biner $\cdot$)
   c. $\forall\ a, b, c \in R$ berlaku $a \cdot (b+c) = ab + ac$ dan $(a+b) \cdot c = ac + bc$
3. Sebuah ring yang komutatif terhadap operasi $\cdot$ dikatakan ring (Gelanggang) Komutatif. Atau dengan kata lain, jika $\langle R, +, \cdot \rangle$ adalah semigrup komutatif terhadap operasi $\cdot$ maka $\langle R, +, \cdot \rangle$ disebut ring (Gelanggang) Komutatif.
4. Misalkan R adalah ring, sebuah elemen $e \in R$ disebut elemen identitas, jika $ea = a = ae$ untuk semua $a \in R$.

5. Sebuah ring R disebut ring dengan identitas jika mempunyai sebuah identitas.
6. Jika $\langle R,\cdot\rangle$ adalah monoid dengan unsur identitas 1, maka ring $\langle R,+,\cdot\rangle$ dikatakan Ring dengan unsur kesatuan (ring dengan unity) yakni jika terdapat satu unsur yang dinotasikan dengan 1 sedemikian sehingga $1 \cdot a = a \cdot 1$ untuk setiap a anggota R, maka kita sebut ring dengan unsur kesatuan, dan unsur 1 disebut sebagai unsur kesatuan (unity).
7. Andaikan R adalah ring dengan unsur kesatuan 1. Satu unsur $a \neq 0 \in R$ dikatakan unsur satuan (unit) bila terdapat $b \neq 0 \in R$ sehingga $ab = ba = 1$.
8. Andaikan R ring dengan unsur kesatuan 1, himpunan semua unsur satuan yang berada di ring R membentuk grup dengan operasi perkalian.

LATIHAN

1. Misalkan $\langle Z_{10},+,\cdot\rangle$ merupakan himpunan bilangan bulat modulo 10 dengan operasi penjumlahan dan perkalian. Buktikan bahwa $\langle Z_{10},+,\cdot\rangle$ merupakan ring (gelanggang).
2. Misalkan $M = \left\{a + b\sqrt{2} \mid a,b \in Q\right\}$ terhadap operasi penjumlahan dan perkalian biasa, apakah $\langle M,+,\cdot\rangle$ merupakan ring?
3. Diketahui $C = \left\{(a,b) \mid a,b \in Real\right\}$ operasi-operasi penjumlahan dan perkalian pada didefinisikan sebagai berikut:
   $(a,b) + (c,d) = (a+c, b+d)$
   $(a,b) \cdot (c,d) = (ac - bd, ad + bc)$
   a. Apakah C suatu Ring?
   b. Apakah C suatu Ring Komutatif?
4. Apakah $T = \{2y + 3 \mid y \in Z\}$ terhadap operasi penjumlahan dan perkalian merupakan Ring?
5. Jika $S = \{1, 2, 3, 4\}$ dan $P(S)$ adalah himpunan kuasa dari S, maka buktikan bahwa $\langle P(S),+,\cdot\rangle$ merupakan ring (gelanggang) komutatif dengan kriteria:
   $A + B = (A \cup B) - (A \cap B)$
   $A \cdot B = A \cap B$
6. Selidiki apakah $M = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in Z\right\}$ merupakan ring komutatif terhadap operasi penjumlahan dan perkalian matriks.

7. Selidiki apakah $\langle Z_4 \times Z_5 \rangle$ merupakan ring komutatif untuk operasi penjumlahan dan perkalian.
8. Berikan 1 contoh ring komutatif dan 1 contoh bukan ring komutatif.
9. Tentukan unsur satuan dan unsur kesatuan dari ring $\langle Z_{14}, +, \cdot \rangle$
10. Tentukan unsur satuan dan unsur kesatuan dari ring $\langle Z_5 \times Z_3 \rangle$

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$\boxed{\textit{Tingkat penguasaan} = \frac{\textit{Banyak jawaban yang benar}}{\textit{Banyak soal}} \times 100\%}$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai di bawah ini:

Rentang Nilai (%)	Kategori
90 – 100	Sangat Baik
80 – 89	Baik
70 – 79	Sedang
≤ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi $\geq$ 70%, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang $<$ 70%, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

BAB 2

DAERAH INTEGRAL DAN *FIELD*

Tujuan Instruksional Umum:

Setelah mempelajari materi pada bab ini, maka diharapkan mahasiswa dapat mengetahui dan mengaplikasikan definisi dari daerah integral, *field*, dan karakteristik Ring.

Tujuan Instruksional Khusus:

Setelah diberikan penjelasan materi terkait definisi terbentuknya suatu daerah integral, *field*, dan karakteristik ring, maka mahasiswa dapat:

a. Menjelaskan definisi dari unsur pembagi nol (*devisors of zero*).
b. Menjelaskan definisi dari daerah integral (integral domain).
c. Menjelaskan definisi idempoten dan nilpoten.
d. Menjelaskan definisi *field* (lapangan).
e. Menjelaskan definisi karakteristik ring.
f. Mengidentifikasikan suatu ring komutatif yang merupakan daerah integral atau bukan.
g. Mengidentifikasikan suatu ring komutatif yang merupakan *field* atau bukan.
h. Menentukan idempoten dan nilpoten dari ring komutatif.
i. Memberikan contoh dan bukan contoh dari daerah integral dan *field*.

Deskripsi Singkat:

Daerah integral (*integral domain*) adalah suatu ring komutatif dengan unsur kesatuan yang tidak memiliki unsur pembagi nol (*devisors of zero*). Sedangkan *field* adalah ring komutatif dengan unsur kesatuan dan setiap unsur yang tidak nol memiliki invers. Pada bab ini, akan dibahas mengenai sifat-sifat dasar unsur pembagi nol (*devisors of zero*), daerah integral (*integral domain*), idempoten dan nilpoten, *field*, serta karakteristik ring.

2.1 DAERAH INTEGRAL

Definisi 2.1

Suatu unsur $a \neq 0$ pada suatu ring komutatif R, disebut sebagai unsur **pembagi nol** (***devisors of zero***) bilamana terdapat suatu unsur $b \neq 0$ sehingga $ab = 0$

Contoh 2.1:

Ring $\langle Z_{12}, +, \cdot \rangle$ maka unsur-unsur 2, 3, 4, 6 masing-masing adalah unsur pembagi nol. Hal ini disebabkan $(2)(6) = 0$; $(3)(4) = 0$; $(4)(3) = 0$; $(6)(2) = 0$

Definisi 2.2

Suatu ring komutatif D dengan unsur kesatuan yang tidak mempunyai unsur pembagi nol (*devisors of zero*) disebut sebagai **daerah integral (*integral domain*)**.

Contoh 2.2:

$\langle Z_3, +, \cdot \rangle$; $\langle Z_5, +, \cdot \rangle$; $\langle Z_n, +, \cdot \rangle$ dengan n bilangan prima merupakan daerah integral (integral domain).

Contoh 2.3:

Ring dengan bilangan bulat Z adalah suatu integral karena untuk setiap x, $y \in Z$, persamaan $xy = 0$ dipenuhi hanya apabila $x = 0$ atau $y = 0$.

Contoh 2.4:

Ring $Z[i] = \{a + bi \mid a, b \in Z\}$ merupakan daerah integral.

Contoh 2.5:

Ring $Z\left[\sqrt{2}\right] = \left\{a + b\sqrt{2} \mid a, b \in Z\right\}$ merupakan integral domain.

Contoh 2.6:

Ring Z_n dari bilangan bulat modulo n bukan merupakan intehral domain ketika n bukan prima.

Kembali kita ingat bahwa dalam suatu Grup G berlaku hukum kanselasi, tetapi secara umum hukum ini tidak berlaku pada ring, teorema berikut ini akan memperlihatkan bahwa hukum kanselasi juga berlaku pada daerah integral:

Teorema 2.1:

Andaikan D adalah suatu daerah integral dan misalkan $a,b,c \in D$ dengan $a \neq 0$, jika $ab = ac$, maka $b = c$.

Bukti:

$$\begin{aligned} ab-bc &= 0 \\ a(b-c) &= 0 \text{ karena } a \neq 0\text{, maka } (b-c)=0 \text{ (Integral domain)} \\ b-c &= 0 \\ b &= c \quad \text{(terbukti)} \end{aligned}$$

Contoh 2.7:

Buktikan bahwa ring $\langle Z_6, +, \cdot \rangle$ bukan merupakan daerah integral.

Penyelesaian:

$Z_6 = \{0, 1, 2, 3, 4, 5\}$
Z_6 memiliki elemen pembagi nol yaitu:
$\exists 2,3 \in Z_6$, $2 \neq 0$ dan $3 \neq 0$, tetapi $2 \times 3 = 0$.
Sehingga terbukti ring $\langle Z_6, +, \cdot \rangle$ bukan merupakan daerah integral.

2.2 IDEMPOTEN DAN NILPOTEN

Definisi 2.3

Suatu elemen a di ring R disebut **idempoten** jika $a^2 = a$. Suatu elemen $a \in R$ disebut **nilpoten** jika $a^n = 0$ untuk semua bilangan bulat positif n.

Contoh 2.8:

Carilah semua unsur idempoten dan nilpoten dari ring $\langle Z_4, +, \cdot \rangle$

Penyelesaian:

Misalkan diambil $Z_4 = \{0,1,2,3\}$ *mod* 4
$0^2 = 0 \cdot 0 = 0$
$1^2 = 1 \cdot 1 = 1$
$2^2 = 2 \cdot 2 = 0$
$3^2 = 3 \cdot 3 = 1$

Maka unsur idempoten dari ring $\langle Z_4, +, \cdot \rangle$ adalah 0 dan 1. Adapun unsur nilpoten dari ring $\langle Z_4, +, \cdot \rangle$ adalah 0 dan 2.

Contoh 2.9:

Matriks $M_{2\times 2}$ dengan unsur $A = \begin{bmatrix} 1 & 0 \\ 4 & 0 \end{bmatrix}$ adalah idempoten.

Penyelesaian:

Berdasarkan definisi 3, suatu unsur A di $M_{2\times 2}$ disebut idempoten jika $A^2 = A$, yaitu:

$$\begin{bmatrix} 1 & 0 \\ 4 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 4 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 4 & 0 \end{bmatrix}$$

Sedemikian sehingga terbukti bahwa $A^2 = A$.

Contoh 2.10:

$Z_6 = \{0, 1, 2, 3, 4, 5\}$ adalah ring terhadap operasi biner penjumlahan dan perkalian modulo 6. Maka unsur 0, 1, 3, dan 4 adalah unsur idempoten, sebab:

$0^2 = 0$

$1^2 = 1$

$3^2 = 3$

$4^2 = 4$

Contoh 2.11:

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ adalah ring terhadap penjumlahan dan perkalian modulo 8. Maka unsur 0, 2, 4, dan 6 adalah unsur nilpoten, sebab:

$0^2 = 0$

$2^3 = 0$

$4^2 = 0$

$6^3 = 0$

Contoh 2.12:

Tentukan semua unsur pembagi nol, idempoten dan nilpoten dari ring $\langle Z_3 \times Z_6 \rangle$

Penyelesaian:

$Z_3 \times Z_6 = \{0, 1, 2\} \times \{0, 1, 2, 3, 4, 5\}$

= {(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (1,0), (1,1), (1,2), (1,3), (1,4), (1,5)
(2,0), (2,1), (2,2), (2,3), (2,4), (2,5)}

Tabel 2.1. Tabel Cayley dengan Operasi Biner Perkalian pada $Z_3 \times Z_6$

•	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(0,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)
(0,2)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)
(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)
(0,4)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)
(0,5)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)
(1,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)
(1,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)
(1,2)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(1,0)	(1,2)	(1,4)	(1,0)	(1,2)	(1,4)	(2,0)	(2,2)	(2,4)	(2,0)	(2,2)	(2,4)
(1,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(1,0)	(1,3)	(1,0)	(1,3)	(1,0)	(1,3)	(2,0)	(2,3)	(2,0)	(2,3)	(2,0)	(2,3)
(1,4)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(1,0)	(1,4)	(1,2)	(1,0)	(1,4)	(1,2)	(2,0)	(2,4)	(2,2)	(2,0)	(2,4)	(2,2)
(1,5)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(1,0)	(1,5)	(1,4)	(1,3)	(1,2)	(1,1)	(2,0)	(2,5)	(2,4)	(2,3)	(2,2)	(2,1)
(2,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)	(2,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)	(1,0)
(2,1)	(0,0)	(0,1)	(0,2)	(0,3)	(0,4)	(0,5)	(2,0)	(2,1)	(2,2)	(2,3)	(2,4)	(2,5)	(1,0)	(1,1)	(1,2)	(1,3)	(1,4)	(1,5)
(2,2)	(0,0)	(0,2)	(0,4)	(0,0)	(0,2)	(0,4)	(2,0)	(2,2)	(2,4)	(2,0)	(2,2)	(2,4)	(1,0)	(1,2)	(1,4)	(1,0)	(1,2)	(1,4)
(2,3)	(0,0)	(0,3)	(0,0)	(0,3)	(0,0)	(0,3)	(2,0)	(2,3)	(2,0)	(2,3)	(2,0)	(2,3)	(1,0)	(1,3)	(1,0)	(1,3)	(1,0)	(1,3)
(2,4)	(0,0)	(0,4)	(0,2)	(0,0)	(0,4)	(0,2)	(2,0)	(2,4)	(2,2)	(2,0)	(2,4)	(2,2)	(1,0)	(1,4)	(1,2)	(1,0)	(1,4)	(1,2)
(2,5)	(0,0)	(0,5)	(0,4)	(0,3)	(0,2)	(0,1)	(2,0)	(2,5)	(2,4)	(2,3)	(2,2)	(2,1)	(1,0)	(1,5)	(1,4)	(1,3)	(1,2)	(1,1)

a. Unsur pembagi nol (*devisors of zero*) adalah:
(0,1), (0,2), (0,3), (0,4), (0,5), (1,0), (1,2), (1,3), (1,4), (2,0), (2,2), (2,3), (2,4)

b. Unsur idempotennya adalah:
(0,0) karena $(0,0)^2 = (0,0)$
(0,1) karena $(0,1)^2 = (0,1)$
(0,3) karena $(0,3)^2 = (0,3)$
(0,4) karena $(0,4)^2 = (0,4)$
(1,0) karena $(1,0)^2 = (1,0)$
(1,1) karena $(1,1)^2 = (1,1)$

(1,3) karena $(1,3)^2 = (1,3)$
(1,4) karena $(1,4)^2 = (1,4)$

c. Unsur nilpotennya adalah
d. (0,0) karena $(0,0)^2 = (0,0)$

2.3 LAPANGAN (FIELD)

Definisi 2.4:

Suatu ring komutatif F dengan unsur kesatuan dikatakan sebagai lapangan (*field*) jika **setiap unsur tidak 0 (nol) adalah unsur satuan.**

Penjelesan:

1. F dikatakan **lapangan** jika F sebuah **gelanggang dengan unsur kesatuan,** dan **semua unsurnya satuan kecuali nol.**
2. Lapangan (*field*) pasti merupakan daerah integral (integral domain). Akan tetapi, daerah integral belum tentu lapangan (*field*).
3. Daerah integral tidak memiliki unsur pembagi nol (*devisors of zero*) sehingga semua lapangan (*field*) pasti daerah integral.
4. Semua unsur satuan pasti tidak ada pembagi nol. Jika tidak ada pembagi nol, belum tentu semua unsur satuan.

Contoh 2.13:

Buktikan bahwa $\langle Z_5, +, . \rangle$ merupakan sebuah lapangan (*field*)?

Penyelesaian:

Tabel 2.2. Tabel Cayley dengan Operasi Biner Perkalian pada Z_5

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Selain unsur $0 \in Z_5$ semua unsurnya {1, 2, 3, 4} merupakan unsur satuan.
Karena:
$(1)(1) = 1$ sehingga $1^{-1} = 1$

$(2)(3) = 1$ sehingga $2^{-1} = 3$
$(3)(2) = 1$ sehingga $3^{-1} = 2$
$(4)(4) = 1$ sehingga $4^{-1} = 4$

$\therefore$ Dengan demikian, terbukti bahwa $\langle Z_5, +, . \rangle$ merupakan sebuah lapangan (*field*)

Contoh 2.14:

Buktikan Z_p, dimana p = prima, maka $\langle Z_p, +, \cdot \rangle$ merupakan lapangan (*field*).

Penyelesaian:

$Z_p = \{0, a_1, a_2, a_3, \ldots, a_n\}$; $n \in p$
a_1, a_2 tidak mempunyai kelipatan. Akibatnya $a_1 \cdot a_2 \in Z_p \neq 0, 1, 2, 3, \ldots$
Karena $a_1 \cdot a_2 \neq 0$, jika a_1 merupakan invers dari a_2
a_1 merupakan invers satuan
a_2 merupakan invers satuan
$\forall a;\ a \neq 0$ merupakan unsur satuan.
$\therefore$ Z_p merupakan sebuah lapangan (*field*)

Contoh 2.15:

Misalkan $Z_3\,[i] = \{a + bi \mid a, b \in Z_3\}$
$= \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$

Di mana $i^2 = -1$. Ring dari bilangan bulat modulo 3. Semua elemen mengalami penjumlahan dan perkalian pada bilangan kompleks, kecuali koefisien yang tereduksi modulo 3. Misal, $-1 = 2$. Perhatikan Tabel 2.3 berikut:

TABEL 2.3. Tabel Perkalian Elemen Bukan Nol dari Z_3 [i]

•	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
1	1	2	i	$1+i$	$2+i$	$2i$	$1+2i$	$2+2i$
2	2	1	$2i$	$2+2i$	$1+2i$	i	$2+i$	$1+i$
i	i	$2i$	2	$2+i$	$2+2i$	1	$1+i$	$1+2i$
$1+i$	$1+i$	$2+2i$	$2+i$	$2i$	1	$1+2i$	2	i
$2+i$	$2+i$	$1+2i$	$2+2i$	1	i	$1+i$	$2i$	2
$2i$	$2i$	i	1	$1+2i$	$1+i$	2	$2+2i$	$2+i$
$1+2i$	$1+2i$	$2+i$	$1+i$	2	$2i$	$2+2i$	i	1
$2+2i$	$2+2i$	$1+i$	$1+2i$	i	2	$2+i$	1	$2i$

Contoh 2.16:

Bilangan riel merupakan lapangan (*field*)

Penyelesaian:

$a \in R$ dikatakan unsur satuan karena

$a.\frac{1}{a} = 1$, dimana $\frac{1}{a} \in R$

$\therefore$ Bilangan riel merupakan lapangan (*field*)

Contoh 2.17:

Buktikan bahwa bilangan kompleks merupakan lapangan (*field*)!

Penyelesaian:

Bilangan kompleks merupakan unsur satuan.
Ambil sembarang unsur, misal:
$a + bi \in C$; dimana $C =$ bilangan kompleks

$$(a+bi)\left(\frac{1}{a+bi}\right) = 1$$

$$(a+bi)\left(\frac{1}{a+bi} \times \frac{a-bi}{a-bi}\right) = 1$$

$$(a+bi)\left(\frac{a-bi}{a^2+b^2}\right) = 1$$

$$(a+bi)\left(\frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2}\right) = 1$$

$$\text{Karena}\left(\frac{a}{a^2+b^2} - \frac{bi}{a^2+b^2}\right) \in C$$

Maka $a+bi$ merupakan unsur satuan.
Atau ambil sembarang unsur lain, misal: $a+bi \in C$

$$(a+bi)\left(\frac{1}{a+bi}\right) = 1$$

$$\text{karena}\left(\frac{1}{a+bi}\right) \in C$$

maka $a+bi$ merupakan unsur satuan.
$\therefore$ Terbukti bahwa bilangan kompleks merupakan lapangan (*field*)

Contoh 2.18:

Buktikan bahwa bilangan rasional $Q(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in Q\}$ merupakan *field.*

Penyelesaian:

Misalkan diambil sembarang unsur $a + b\sqrt{2} \neq 0$ maka $a - b\sqrt{2} \neq 0$. Sehingga dengan cara merasionalkan penyebut diperoleh:

$$\frac{1}{a+b\sqrt{2}}\left(\frac{a-b\sqrt{2}}{a-b\sqrt{2}}\right) = \frac{a-b\sqrt{2}}{a^2-2b^2}$$

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

di mana $a^2 - 2b^2$ adalah bilangan rasional yang tidak nol, sehingga:

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

Merupakan elemen $Q(\sqrt{2})$. Hal ini menunjukkan setiap elemen $Q(\sqrt{2})$ mempunyai unsur kebalikan (invers) terhadap perkalian $Q(\sqrt{2})$. Sehingga terbukti $Q(\sqrt{2})$ merupakan *field.*

Contoh 2.19:

Rinw Z dengan unsur kesatuan 1 bukanlah sebuah lapangan (*field*) karena tidak mempunyai unsur satuan.

Penyelesaian:

Z = himpunan bilangan bulat

Ambil sembarang unsur, misal: $a \in Z$

$a.\frac{1}{a} = 1$. Akan tetapi $\frac{1}{a} \notin Z$

Maka a bukan unsur satuan.

$\therefore \langle Z, +, \cdot \rangle$ bukan lapangan (*field*)

Teorema 2.2.

Andaikan F adalah suatu lapangan, maka F adalah juga suatu daerah integral.

Bukti:

Kita cukup membuktikan bahwa F tidak mempunyai unsur pembagi nol, yakni untuk sembarang $x, y \in F$ dengan $x \neq 0$ dan $xy = 0$, maka $y = 0$. Sekarang perhatikan sembarang $x, y \in F$ $x \neq 0$ dan $xy = 0$. Karena F adalah suat lapangan, maka setiap unsur tidak nol **mempunyai unsur kebalikan (invers)** yang relatif terhadap operasi perkalian.

Teorema 2.3:

Suatu daerah integral yang berhingga adalah suatu lapangan (*field*).

Bukti:

Andaikan D adalah suatu daerah integral, unsur kesatuan 1, karena D berhingga. Misalkan:

$1, a_1, a_2, a_3, \ldots, a_n$ adalah unsur-unsur dari D, kita tinggal memperlihatkan bahwa setiap unsur tak nol dari D adalah unsur satuan. Untuk itu, misalkan a adalah sembarang unsur tak nol di D, dan perhatikan hasil kali antara a dengan unsur-unsur di D sebagai berikut:

$a, aa_1, aa_2, aa_3, \ldots, aa_n$ dan $(1, a_1, a_2, \ldots, a_n)$ adalah suatu himpunan yang sama. Hal ini berarti bahwa terdapat j dimana $1 \leq j \leq n$, sehingga $aa_j = 1$. Jadi, setiap unsur tak nol di D adalah unsur-unsur satuan, sehingga D adalah suatu lapangan (*field*).

Teorema 2.4:

Untuk setiap bilangan prima P, Z_p adalah suatu lapangan..

2.4 KARAKTERISTIK DARI RING

Definisi 2.5.

Andaikan R adalah suatu ring, karakteristik dari ring R adalah suatu bilangan bulat positif terkecil n sehingga: $nx = x + x + x + x + \ldots + x = 0$ untuk setiap $x \in R$, bila tidak terdapat bilangan n yang demikian, maka R mempunyai karakteristik 0.

Contoh 2.20:

$P(A)$ dimana $A = \{0,1\}$ mempunyai karakteristik 2 karena
$2\varnothing = \varnothing + \varnothing = (\varnothing \cup \varnothing)\text{-}(\varnothing \cap \varnothing)$

Contoh 2.21:

Z_4 = {0, 1, 2, 3} mempunyai karakteristik 4, sebab:
$(4)(0)=0$
$(4)(1)=0$
$(4)(2)=0$
$(4)(3)=0$

Setiap bilangan bulat, karakteristiknya = 0

Contoh 2.22:

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

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

dan operasi perkalian didefinisikan sebagai:

$$X\cdot Y=X\cap Y$$

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.

Teorema 2.5:

Andaikan R adalah suatu ring dengan unsur kesatuan 1, jika order dari unsur 1 adalah tak hingga, maka R mempunyai karakteristik 0, jika unsur 1 mempunyai order n, maka karakteristik dari R adalah n.

Bukti:

Jika unsur kesatuan 1 berorder tak hingga, maka tidak terdapat bilangan bulat n, sehingga $n.\,1=0$, sehingga R mempunyai karakteristik 0.

Sekarang kita misalkan unsur kesatuan 1 beroder n, maka $n.1=0$, hal ini berakibat untuk setiap $x\in R$ diperoleh:

$$\begin{aligned} nx &= n(1x) \\ &= 1x+1x+\ldots+1x \\ &= (1+1+\ldots+1)x \\ &= (n.1)x \\ &= 0x \\ &= 0 \end{aligned}$$

Teorema 2.6.

Bila D adalah suatu daerah integral, maka karakteristik dari D adalah 0 atau suatu bilangan prima.

Bukti:

Untuk membuktikannya kita cukup mencari order dari unsur kesatuan 1, bila unsur kesatuan 1 adalah tidak hingga, maka karakteristik dari D adalah 0, selanjutnya misal order dari unsur 1 adalah bilangan n yang bukan prima, misalkan saja $n = km$ dengan $k<n$ dan $m<n$, maka:

$$\begin{aligned} n.a &= (\mathrm{km}).1 \\ &= (k.1)(m.1) \\ &= 0 \end{aligned}$$

Karena D adalah suatu daerah integral, maka D tidak mempunyai unsur pembagi nol.

Contoh 2.23:

Persamaan $x^2-4\mathrm{x}+3=0$ dalam bilangan bulat. Kita akan mencari semua solusi dengan pemfaktoran sebagai berikut:

$$x^2-4\mathrm{x}+3=(x-3)(x-1)=0$$

dan atur setiap faktor yang sama dengan 0. Akan tetapi perlu dicatat bahwa ketika kita dapat mencari semua solusi dari cara ini, kita menggunakan fakta bahwa hanya cara untuk menghasilkan sama dengan 0 adalah salah satu dari pemfaktoran yang menjadi 0. Kita menggunakan Z sebagai daerah integral. Dalam Z_{12}, ada banyak elemen bukan nol yang menghasilkan 0, yaitu:

$2 \cdot 6 = 0$; $3 \cdot 4 = 0$; $4 \cdot 6=0$; $6 \cdot 8 =0$, dan sebagainya.

Lalu, bagaimana kita mencari semua solusi dari $x^2-4x+3=0$ dalam Z_{12}?

Cara yang mudah dengan mencoba setiap elemen. Kita menemukan ada empat solusi, yaitu: $x=1$, $x=3$, $x=7$, dan $x=9$.

Kemudian, kita akan mencari semua solusi dari $x^2-4x+3=0$ pada Z_{11} atau Z_{13}, katakan dengan mengatur dua faktor $x-3$ dan $x-1$ sama dengan 0. Tentu dengan alasan ini ring tersebut merupakan daerah integral.

Berikut ini akan diberikan Tabel 2.4 yang memberikan rangkuman dari beberapa ring yang telah kita ketahui dan sifat-sifatnya.

Tabel 2.4. Rangkuman Ring dan Sifat-Sifatnya

Ring	Bentuk Elemen	Unsur satuan	Komutatif	Daerah Integral	Field	Karak-teristik
Z	k	1	Ya	Ya	Tidak	0
Z_n, n gabungan	k	1	Ya	Tidak	Tidak	n
Z_p, p prima	k	1	Ya	Ya	Ya	p
$Z[x]$	$a_n x_n + \dots + a_1 x + a_0$	$f(x)=1$	Ya	Ya	Tidak	0
nZ, $n>1$	nk	Kosong	Ya	Tidak	Tidak	0
$M_2(Z)$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	Tidak	Tidak	Tidak	0
$M_2(2Z)$	$\begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$	Kosong	Tidak	Tidak	Tidak	0
$Z[i]$	$a+bi$	1	Ya	Ya	Tidak	0
$Z_3[i]$	$a+bi;\ a, b \in Z_3$	1	Ya	Ya	Ya	3
$Z\left[\sqrt{2}\right]$	$a+b\sqrt{2}; a,b \in Z$	1	Ya	Ya	Tidak	0
$Q\left[\sqrt{2}\right]$	$a+b\sqrt{2}; a,b \in Q$	1	Ya	Ya	Ya	0
$Z \oplus Z$	(a, b)	$(1,1)$	Ya	Tidak	Tidak	0

Bukti:

Diserahkan kepada pembaca sebagai latihan.

RANGKUMAN

1. Suatu unsur $a \neq 0$ pada suatu ring komutatif R, disebut sebagai unsur pembagi nol (*devisors of zero*) jika terdapat suatu unsur $b \neq 0$ sehingga $ab=0$.
2. Suatu ring komutatif D dengan unsur kesatuan yang tidak mempunyai unsur pembagi nol (*devisors of zero*) disebut sebagai daerah integral (*integral domain*).
3. Andaikan D adalah suatu daerah integral dan misalkan a, b, $c \in D$ dengan $a \neq 0$, jika $ab=ac$, maka $b=c$.
4. Suatu elemen a di ring R disebut *idempoten* jika $a^2=a$. Suatu elemen $a \in R$ disebut nilpoten jika $a^n=0$ untuk semua bilangan bulat positif n.

5. Suatu ring komutatif F dengan unsur kesatuan dikatakan sebagai lapangan (*field*) jika setiap unsur tidak 0 (nol) merupakan unsur satuan. Atau dengan kata lain:
   a. F dikatakan lapangan jika F sebuah gelanggang dengan unsur kesatuan, dan semua unsurnya satuan kecuali nol.
   b. Lapangan (*field*) pasti merupakan daerah integral (integral domain). Akan tetapi, daerah integral belum tentu lapangan (*field*).
   c. Daerah integral tidak memiliki unsur pembagi nol (*devisors of zero*) sehingga semua lapangan (*field*) pasti daerah integral.
   d. Semua unsur satuan pasti tidak ada pembagi nol. Jika tidak ada pembagi nol, belum tentu semua unsur satuan.
6. Andaikan F adalah suatu lapangan, maka F adalah jjuga suatu daerah integral.
7. Suatu daerah integral yang berhingga adalah suatu lapangan (*field*)
8. Untuk setiap bilangan prima P, Z_p adalah suatu lapangan.
9. Andaikan R adalah suatu ring dengan unsur kesatuan 1, jika order dari unsur 1 adalah tak hingga, maka R mempunyai karakteristik 0, jika unsur 1 mempunyai order n, maka karakteristik dari R adalah n.
10. Bila D adalah suatu daerah integral, maka karakteristik dari D adalah 0 atau suatu bilangan prima.

LATIHAN

1. Manakah dari ring berikut yang merupakan daerah integral (integral domain). Berikan alasan Anda!
   a. $\langle Z_{11}, +, \cdot \rangle$
   b. $\langle Z_{15}, +, \cdot \rangle$
   c. $\langle Z_{33}, +, \cdot \rangle$
   d. $\langle Z_{19}, +, \cdot \rangle$
2. Tentukan semua unsur pembagi nol (*devisors of zero*), idempoten dan nilpoten dari ring $\langle Z_3 \times Z_3 \rangle$.
3. Tentukan unsur idempoten dan nilpoten pada ring berikut:
   a. $\langle Z_{12}, +, \cdot \rangle$
   b. $\langle Z_{13}, +, \cdot \rangle$
4. Tentukan apakah ring komutatif berikut merupakan lapangan (*field*) atau bukan:
   a. $\langle Z_9, + \cdot \rangle$
   b. $\langle Z_7, + \cdot \rangle$
   c. $\langle U_{10}, + \cdot \rangle$

d. $\langle Z_{11}, +\cdot\rangle$
e. $\langle Z_{15}, +\cdot\rangle$

5. Misalkan $R = \{0, 2, 4, 6, 8\}$ dalam operasi biner penjumlahan dan perkalian modulo 10. Buktikan bahwa adalah R sebuah lapangan (*field*).
6. Diketahui R adalah himpunan semua matriks berbentuk $\begin{bmatrix} x & 0 \\ x & 0 \end{bmatrix}$ dengan x bilangan real. R merupakan ring terhadap operasi biner penjumlahan dan perkalian matriks. Apakah R merupakan lapangan (*field*)?
7. Cari unsur pembagi nol dalam $Z_5[i] = \{a + bi | a, b \in Z_5\}$
8. Cari unsur idempotent dalam $Z_5[i] = \{a + bi | a, b \in Z_5\}$
9. Temukan semua solusi dari $x^2 - x + 2 = 0$ dalam Z_3.
10. Temukan semua solusi dari persamaan $x^2 - 5x + 6 = 0$ dalam Z_{14}.

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$\boxed{\textit{Tingkat penguasaan} = \frac{\textit{Banyak jawaban yang benar}}{\textit{Banyak soal}} \times 100\%}$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai di bawah ini:

Rentang Nilai (%)	Kategori
90 – 100	Sangat Baik
80 – 89	Baik
70 – 79	Sedang
≤ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi $\geq$ 70%, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang $<$ 70%, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

BAB 3

SUBRING

Tujuan Instruksional Umum:

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan dapat mengetahui dan mengaplikasikan teori terkait subring dan sentral suatu gelanggang.

Tujuan Instruksional Khusus:

Setelah diberikan penjelasan terhadap definisi terbentuknya suatu subring dan sentral suatu gelanggang, maka mahasiswa diharapkan dapat:

a. Menjelaskan definisi dari subring dan sentral suatu gelanggang.
b. Mengidentifikasikan sebuah ring yang merupakan subring atau bukan.
c. Mengidentifikasikan sebuah ring yang merupakan sentral suatu gelanggang.
d. Menentukan semua subring dari suatu ring.
e. Memberikan contoh dan bukan contoh dari subring.

Deskripsi Singkat:

Himpunan S dikatakan subring dari R jika S juga merupakan ring pada operasi penjumlahan dan perkalian yang sama dalam ring R, dengan S merupakan himpunan bagian tak kosong dari ring R. Pada bab ini akan dijelaskan terkait persyaratan terbentuknya suatu ring dan sentral suatu gelanggang.

3.1 PENGERTIAN SUBRING

Definisi 3.1

Misal, S merupakan suatu himpunan bagian yang tidak kosong dalam ring $\langle R, +, \cdot \rangle$, maka himpunan S dikatakan **Subring** dari R jika S juga merupakan ring terhadap operasi penjumlahan dan perkalian yang sama pada ring R. Dengan demikian, subring merupakan suatu ring di dalam suatu ring.

Contoh 3.1:

1) Ring $\langle Z,+,\cdot\rangle$ merupakan subring dari $\langle Q,+,\cdot\rangle$, $\langle R,+,\cdot\rangle$ dan $\langle C,+,\cdot\rangle$
2) Ring $\langle Q,+,\cdot\rangle$ subring dari $\langle R,+,\cdot\rangle$ dan $\langle C,+,\cdot\rangle$
3) Ring $\langle R,+,\cdot\rangle$ subring dari $\langle C,+,\cdot\rangle$
4) $2Z$ subring dalam ring $\langle Z,+,\cdot\rangle$
5) Himpunan matriks segitiga atas

$$T_{3\times 3}(R)=\left\{A=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ 0 & a_{22} & a_{23} \\ 0 & 0 & a_{33}\end{pmatrix} \middle| a_{11},a_{12},a_{13},a_{22},a_{23},a_{33}\in R\right\}$$

Merupakan subring dalam $\langle M_{3\times 3}(R),+,\cdot\rangle$

6) Himpunan matriks diagonal

$$D_{3\times 3}(R)=\left\{A=\begin{pmatrix} a_{11} & 0 & 0 \\ 0 & a_{22} & 0 \\ 0 & 0 & a_{33}\end{pmatrix} \middle| a_{11},a_{22},a_{33}\in R\right\}$$

Merupakan subring di $\langle M_{3\times 3}(R),+,\cdot\rangle$

Berdasarkan definisi subring di atas, dapat ditarik kesimpulan bahwa suatu himpunan bagian dari suatu ring $\langle R,+,\cdot\rangle$ dikatakan ring jika dan hanya jika:

1. **Pada operasi penjumlahan $(+)$**

   $\langle S,+\rangle$ juga merupakan grup abelian (komutatif)

2. **Pada operasi perkalian (.)**

   $\langle S,\cdot\rangle$ bersifat asosiatif, yaitu

   $\forall s_1, s_2, s_3 \in S$ berlaku $(s_1 \cdot s_2)\cdot s_3 = s_1\cdot(s_2\cdot s_3)$

3. **Pada operasi keduanya (penjumlahan dan perkalian)**

   $\langle S,+,\cdot\rangle$ bersifat distributif kiri dan distributif kanan, yaitu:

   $\forall s_1, s_2, s_3 \in S$ berlaku distributif kiri $s_1\cdot(s_2+s_3)=(s_1\cdot s_2)+(s_1\cdot s_3)$

   $\forall s_1, s_2, s_3 \in S$ berlaku distributif kanan $(s_1+s_2)\cdot s_3=(s_1\cdot s_3)+(s_2\cdot s_3)$

Hal ini dapat dengan mudah dibuktikan bahwa:

1. Syarat 1, ekuivalen dengan menyatakan bahwa S merupakan subgrup dalam grup $\langle R,+\rangle$, hal ini ekuivalen dengan terpenuhinya:

$$(\forall s_1, s_2 \in S)\rightarrow(s_1 - s_2)\in S$$

2. Syarat 2, asosiatif yang pasti terpenuhi oleh sembarang himpunan

bagian dari R. Terhadap operasi perkalian (.) yang harus diperiksa adalah sifat ketertutupan, yakni:

$$(\forall s_1, s_2 \in S) \rightarrow (s_1 \cdot s_2) \in S$$

3. Syarat 3, distributif yang juga pasti terpenuhi oleh sebarang himpunan bagian dari R.

Untuk membuktikan suatu subhimpunan tak kosong dari suatu ring merupakan subring, kita perlu menyelidiki syarat-syarat supaya subhimpunan tersebut menjadi ring. Jika diperhatikan lebih seksama, syarat berlakunya sifat assositaif, distributif, bisa kita abaikan karena sudah terwarisi dari sifat ringnya. Di samping itu, jika ditinjau dari operasi penjumlahannya, suatu subhimpunan merupakan subring maka terhadap operasi penjumlahan subhimpunan tersebut merupakan subgrup. Dengan adanya fakta ini, diperoleh Teorema berikut ini.

Teorema 3.1

Jika $S \subseteq R$, dan $S \neq \emptyset$, S dikatakan subring dari R jika dan hanya jika:

a) $\forall x, y \in S$ maka $(x - y) \in S$

b) $\forall x, y \in S$, maka $xy \in S$

atau cukup diperlihatkan:

a) $\forall a, b \in S \rightarrow (a+b) \in S$

b) $\forall a \in S \rightarrow -a \in S$

Bukti:

$\forall x, y \in S \rightarrow (x-y) \in S$

Akan dibuktikan

$$\begin{aligned}
(x-y)+(x-y)^{-1} &= 0 \\
(x-y)+(-(-y)-x) &= 0 \\
(x-y)+(y-x) &= 0 \\
x-y+y-x &= 0 \\
x+0-x &= 0 \\
x-x &= 0 \\
0 &= 0 \quad \text{(Terbukti)}
\end{aligned}$$

Invers dari $(x-y)$ adalah $(x-y)^{-1}$

Bukti:

$\forall x, y \in S \rightarrow xy \in S$

Akan dibuktikan

$xy+0=xy$

$xy+(xy-xy) \quad =xy$

$xy+xy=xy+xy$

$xy+xy=x(y+y)$ Distributif

Bukti:

S dikatakan subring dari R, jika:

a) $\forall a,\ b\in S \rightarrow (a+b)\in S$ (tertutup)

b) $\forall a\in S \rightarrow -a\in S$ (invers penjumlahan)

Akan dibuktikan

a) Jelas tertutup

b) $\forall a\in S \rightarrow -a\in S$

Apakah 0 (identitas) termuat dalam S

$\forall a\in S \rightarrow -a\in S$

$\forall a,\ b\in S \rightarrow -(a+b)\in S$ dan $a+b\in S$

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

$$-a-b+a+b=0$$

$$-a+a-b+b=0$$

$$0=0$$

$$0\in S$$

Terbukti bahwa S sebuah subring.

Contoh 3.2:

Buktikan bahwa $K=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}, \forall a,b\in Z$ merupakan subring dari $R=M_{2\times 2}(Z)$

Penyelesaian:

a) Buktikan $\forall A,B\in K \rightarrow (A-B)\in K$

Ambil sembarang unsur, misal $A=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}; B=\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}, \forall a,b,c,d\in Z$

$$A-B=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}-\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}=\begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix}$$

jika $\forall a,\ c\in Z\rightarrow a-c\in Z$

jika $\forall b,\ d\in Z\rightarrow b-d\in Z$

akibatnya $\begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix}\in K$

b) Buktikan $\forall A, B \in K \rightarrow A \cdot B \in K$

Ambil sembarang unsur, misal $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}; B = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}, \forall a,b,c,d \in Z$

$$A \cdot B = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix} = \begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix} \text{karena}$$

$\forall a,\ c \in Z \rightarrow ac \in Z$

$\forall b,\ c \in Z \rightarrow bc \in Z$

Akibatnya $\begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix} \in K$

$\therefore$ Terbukti bahwa K subring R

Contoh 3.3:

Misal $Z_4 = \{0, 1, 2, 3\}$ merupakan suatu ring, buktikan bahwa $S = \{0, 2\}$ adalah subring dari Z_4

Penyelesaian:

Akan dibuktikan $S = \{0, 2\}$ memenuhi syarat dari ring.

1) Buktikan $\forall$a, $b \in S \rightarrow (a–b) \in S$
   Misal, $a = 2$; $b = 0$, $\forall$a, $b \in S$
   Akibatnya $a–b = 2–0 = 2 \in S$
2) Buktikan $\forall$a, $b \in S \rightarrow a \cdot b \in S$
   Misal, $a = 2$; $b = 0$, $\forall$a, $b \in S$
   Akibatnya $a \cdot b = 2 \cdot 0 = 0 \in S$

$\therefore$ Terbukti bahwa S adalah subring dari Z_4

Contoh 3.4:

Buktikan bahwa himpunan $S = \{0, 6\}$ memenuhi sifat tertutup terhadap operasi perkalian tetapi bukan merupakan ring bagian (subring) dari Z_{10}.

Penyelesaian:

$Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

Akan dibuktikan bahwa $S = \{0,6\}$ memenuhi syarat terbentuknya suatu ring.

a) Akan dibuktikan $\forall a,\ b \in S \rightarrow (a–b) \in S$
   Misalkan $a = 0$; $b = 6, \forall a,\ b \in S$
   Akibatnya $a–b = 0–6 = –6 \notin S$

b) Akan dibuktikan $\forall a, b \in S \to a \cdot b \in S$
Misalkan $a = 0$; $b = 6, \forall a, b \in S$
Akibatnya $a \cdot b = 0 \cdot 6 = 0 \in S$

$\therefore$ Terbukti bahwa $S = \{0, 6\}$ adalah bukan subring dari Z_{10}

Contoh 3.5:

Tunjukkan bahwa $Q(\sqrt{3}) = \{a + b\sqrt{3} | a, b \in Q\}$ merupakan subring dari R.

Penyelesaian:

a) Akan dibuktikan $\forall a, b \in Q\sqrt{3} \to (a - b) \in Q\sqrt{3}$
Misalkan $a = a_1 + b_1\sqrt{3}; b = a_2 + b_2\sqrt{3}$ $, \forall a, b \in Q\sqrt{3}$
Akibatnya $a - b = (a_1 + b_1\sqrt{3}) - (a_2 + b_2\sqrt{3})$
$= (a_1 - a_2) + (b_1 - b_2)\sqrt{3} \in Q\sqrt{3}$

b) Akan dibuktikan $\forall a, b \in Q\sqrt{3} \to a \cdot b \in Q\sqrt{3}$
Misalkan $a = a_1 + b_1\sqrt{3}; b = a_2 + b_2\sqrt{3}$ $, \forall a, b \in Q\sqrt{3}$
Akibatnya $a \cdot b = (a_1 + b_1\sqrt{3}) \cdot (a_2 + b_2\sqrt{3})$
$= (a_1a_2) + (a_1b_2)\sqrt{3} + (a_2b_1)\sqrt{3} + 3(b_1b_2)$
$= (a_1a_2 + 3b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{3} \in Q\sqrt{3}$

$\therefore$ Terbukti bahwa $Q(\sqrt{3}) = \{a + b\sqrt{3} | a, b \in Q\}$ merupakan subring dari R.

Contoh 3.6:

Misalkan E adalah himpunan bilangan genap. Buktikan bahwa E membentuk subring dari himpunan bilangan bulat Z.

Penyelesaian:

$E = \{2k | k \in Z\}$ merupakan himpunan yang tak kosong. Sekarang, buktikan bahwa E memenuhi sifat tertutup pada operasi perkalian dan pengurangan.

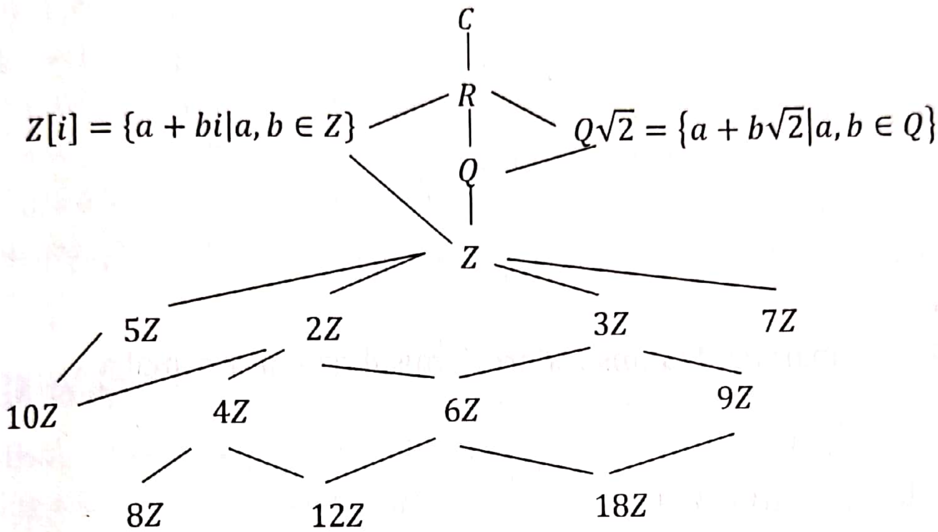
i) Akan dibuktikan tertutup terhadap pengurangan
Karena $(2m) - (2n) = 2(m - n)$ dengan $m - n$ bilangan bulat (Z tertutup terhadap operasi pengurangan), sehingga dalam E.

ii) Akan dibuktikan tertutup terhadap operasi perkalian
Ambil sembarang unsur, misal $a = 2m$, $b = 2n$, $\forall a, b \in E$

Hasil kali (2m)(2n) = 2(m · 2n) dengan m · 2n bilangan bulat sehingga dengan menggunakan hukum asosiatif perkalian, maka hasil perkalian masih dalam E.

∴ Terbukti bahwa himpunan bilangan genap E subring dari Z.

Kita dapat menggambarkan hubungan antara sebuah ring dengan berbagai subringnya melalui diagram lattice subring. Dalam diagram itu, setiap ring adalah subring dari semua ring yang dihubungkan dengan satu atau lebih garis ke atas. Gambar 3.1 menunjukkan hubungan di antara beberapa ring yang telah kita diskusikan.



Gambar 3.1. Diagram Lattice Subring Parsial dari C

Teorema 3.2

Jika S_1 dan S_2 masing-masing subring dari suatu ring R, maka $S_1 \cap S_2$ juga merupakan subring dari R.

Bukti:

$S_1 \cap S_2 \subseteq$ R

Karena S_1 subring dari R, maka $0 \in S_1$.

Karena S_2 subring dari R, maka $0 \in S_2$.

Jadi, $0 \in S_1 \cap S_2$

$S_1 \cap S_2 \neq \emptyset$

Ambil sembarang a, $b \in S_1 \cap S_1$

maka $a - b \in S_1$ *dan* $ab \in S_1$

juga $a - b \in S_2$ *dan* $ab \in S_2$

$a - b \in S_1$ dan $a - b \in S_2 \rightarrow a - b \in S_1 \cap S_2$

$ab \in S_1$ dan $ab \in S_2 \rightarrow ab \in S_1 \cap S_2$
Jadi terbukti bahwa $S_1 \cap S_2$ merupakan subring dari R.

3.2 SENTRAL SUATU GELANGGANG

Definisi 3.2

Misalkan R merupakan suatu ring, suatu himpunan C dikatakan sebagai sentral suatu ring, jika:

$$C = a \in R,\ ax = xa,\ \forall x \in R$$

Bukti:

1) Perhatikan $0 \in C$
   Ambil $0 \in R$
   $0 \cdot x = x \cdot 0$
   $0 = 0$
   $0 \in C$
2) Ambil sembarang dua unsur dari C, misal ax dan bx, maka
   $ax = xa$
   $bx = xb$
   $\forall ax, bx \in C \rightarrow ax - bx \in C$
   $x(a-b) \in C$ distributif kiri
   $ax - bx = (a-b)x$ distributi kanan

$\therefore$ C membentuk sebuah gelanggang

Contoh 3.7:

Buktikan bahwa $R = \langle Z_4, +, \cdot \rangle$ merupakan sentral suatu ring

Penyelesaian:

$Z_4 = \{0, 1, 2, 3\}$
Untuk $a = 1 \rightarrow 1 \cdot R = 1 \cdot \{0, 1, 2, 3\} = \{0, 1, 2, 3\}$ sentral
$a = 2 \rightarrow 2 \cdot R = 2 \cdot \{0, 1, 2, 3\} = \{0, 2\}$ sentral
$a = 3 \rightarrow 3 \cdot R = 3 \cdot \{0, 1, 2, 3\} = \{0, 3, 2, 1\}$ sentral

Contoh 3.8:

Buktikan bahwa $R = \langle Z_3, +, \cdot \rangle$ merupakan sentral suatu ring

Penyelesaian:

$Z_3 = \{0,1,2\}$

Untuk $a=1 \rightarrow 1 \cdot R = 1 \cdot \{0, 1, 2\} = \{0, 1, 2\}$ sentral

$a=2 \rightarrow 2 \cdot R = 2 \cdot \{0, 1, 2\} = \{0, 2\}$ sentral

Contoh 3.9:

Buktikan bahwa $R = \langle Z_5, +, \cdot \rangle$ merupakan sentral suatu ring

Penyelesaian:

$Z_5 = \{0, 1, 2, 3, 4\}$

Untuk $a=1 \rightarrow 1 \cdot R = 1 \cdot \{0,1,2,3,4\} = \{0,1,2,3,4\}$ sentral

$a=2 \rightarrow 2 \cdot R = 2 \cdot \{0,1,2,3,4\} = \{0,2,4,1,3\}$ sentral

$a=3 \rightarrow 3 \cdot R = 3 \cdot \{0,1,2,3,4\} = \{0,3,1,4,2\}$ sentral

$a=4 \rightarrow 4 \cdot R = 4 \cdot \{0,1,2,3,4\} = \{0,4,3,2,1\}$ sentral

Jadi, semua bilangan bulat modulo n adalah sentral.

RANGKUMAN

1. Misal, S merupakan suatu himpunan bagian yang tidak kosong dalam ring $\langle R, +, \cdot \rangle$, maka himpunan S dikatakan **Subring** dari R jika S juga merupakan ring terhadap operasi penjumlahan dan perkalian yang sama pada ring R.
2. Jika $S \subseteq R$, dan $S \neq \emptyset$, S dikatakan subring dari R jika dan hanya jika:
   a) $\forall x, y \in S$, maka $(x-y) \in S$
   b) $\forall x, y \in S$, maka $xy \in S$
3. Jika S_1 dan S_2 masing-masing subring dari suatu ring R, maka $S_1 \cap S_2$ juga merupakan subring dari R.
4. Misalkan R merupakan suatu ring, suatu himpunan C dikatakan sebagai sentral suatu ring, jika:

$$C = a \in R, ax = xa, \forall x \in R$$

LATIHAN

1. Misal Z_5 adalah suatu ring. Tentukan semua subring yang dibangun oleh setiap unsur dari Z_5.
2. Diketahui bahwa himpunan $M_{2\times 2}$ (R) merupakan ring terhadap operasi penjumlahan dan perkalian matriks. Buktikan bahwa himpunan

matriks segitiga atas $TA_{2\times 2}(R)=\left\{\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a,b,c \in R\right\}$ merupakan subring $< M_{2\times 2}(R),+,\cdot >$

3. Diketahui himpunan bilangan prima $< P,+,\cdot >$ dan ring dari himpunan bilangan cacah $< C,+,\cdot >$. Selidiki apakah $< P,+,\cdot >$ merupakan subring dari $< C,+,\cdot >$
4. Manakah dari ring berikut yang merupakan sentral suatu ring (gelanggang):
   a. $< U_9,+,\cdot >$
   b. $< Z_9,+,\cdot >$
5. Misalkan $Q(2)=\left\{a+b\sqrt{2} \middle| a,b \in Q\right\}$ maka buktikan bahwa $Q(2)$ merupakan subring dari R.
6. Buktikan bahwa $Z(5)=\left\{a+b\sqrt{5} \middle| a,b \in Z\right\}$ merupakan subring dari R.
7. Jelaskan mengapa Z_6 bukan subring dari Z_{12}.
8. Misalkan $M_{2\times 2}=\left\{\begin{matrix} a & b \\ c & d \end{matrix} \middle| a,b,c,d \in Z\right\}$ merupakan Ring terhadap operasi penjumlahan dan perkalian matriks. Selanjutnya, misal $S=\left\{\begin{matrix} a & 0 \\ b & 0 \end{matrix} \middle| a,b \in Z\right\}$. Buktikan bahwa S adalah subring dari $M_{2\times 2}$.
9. Buktikan bahwa $Z\left(\sqrt{-1}\right)=Z(i)=\left\{a+bi \middle| a,b \in Z\right\}$ merupakan subring dari C.
10. Berikan masing-masing satu contoh dan bukan contoh dari sentral suatu gelanggang.
11. Misalkan M_2 (Z) adalah ring dari matriks 2×2 dengan entri-entri di dalamnya adalah bilangan bulat, dan misalkan $R=\left\{\begin{bmatrix} a & a+b \\ a+b & b \end{bmatrix} \middle| a,b \in Z\right\}$. Buktikan bahwa R adalah subring di M_2 (Z).
12. Misalkan M_2 (Z) adalah ring dari matriks 2×2 dengan entri-entri di dalamnya adalah bilangan bulat, dan misalkan $R=\left\{\begin{bmatrix} a & a-b \\ a-b & b \end{bmatrix} \middle| a,b \in Z\right\}$. Buktikan bahwa R adalah subring di M_2 (Z).
13. Misalkan M_2 (Z) adalah ring dari matriks dengan entri-entri di dalamnya adalah bilangan bulat, dan misalkan $R=\left\{\begin{bmatrix} a & a \\ b & b \end{bmatrix} \middle| a,b \in Z\right\}$. Buktikan bahwa R adalah subring di M_2 (Z).

14. Tunjukkan bahwa $2Z \cup 3Z$ bukan subring dari Z.
15. Misalkan R adalah ring dengan unsur satuan 1. Tunjukkan bahwa $S = \{n \cdot 1 | n \in Z\}$ adalah subring dari R.
16. Tunjukkan bahwa $T = \left\{ \begin{pmatrix} a & b\sqrt{3} \\ -b\sqrt{3} & a \end{pmatrix} | a, b \in R \right\}$ adalah subring dari M_2 (R).
17. Tunjukkan bahwa $F = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} | a, b \in Z_5 \right\}$ adalah subring dari M_2 (Z_5).
18. Tunjukkan bahwa $T = \left\{ \begin{pmatrix} x+y & y \\ -y & x \end{pmatrix} | x, y \in Z \right\}$ adalah subring dari M_2 (Z).
19. Tunjukkan bahwa $T = \{[0], [5]\}$ adalah subring dari ring Z_{10}.
20. Dalam ring Z bilangan bulat, tentukan yang mana dari himpunan bagian Z berikut yang merupakan subring.
    a) Himpunan bilangan bulat dengan bentuk $4k+2$, $k \in Z$
    b) Himpunan bilangan bulat dengan bentuk $4k+1$, $k \in Z$
    c) Himpunan bilangan bulat dengan bentuk $4k \in Z$

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$\text{Tingkat penguasaan} = \frac{\text{Banyak jawaban yang benar}}{\text{Banyak soal}} \times 100\%$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai di bawah ini:

Rentang Nilai (%)	Kategori
90 – 100	Sangat Baik
80 – 89	Baik
70 – 79	Sedang
≤ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi $\geq 70\%$, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang $< 70\%$, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

BAB 4

IDEAL

Tujuan Instruksional Umum:

Setelah mempelajari materi pada bab ini, mahasiswa diharapkan dapat mengetahui dan menentukan ideal, macam-macam ideal seperti: ideal principal, ideal prima, dan ideal maksimal.

Tujuan Instruksional Khusus:

Setelah diberikan penjelasan mengenai definisi dan syarat terbentuknya ideal, ideal principal, ring principal, ideal prima, dan ideal maksimal, maka diharapkan mahasiswa dapat:

a. Menjelaskan definisi dari ideal kiri, ideal kanan, dan ideal.
b. Menjelaskan definisi dari ring principal.
c. Menjelaskan definisi dari ideal prima.
d. Menjelaskan definisi dari ideal maksimal.
e. Mengidentifikasikan suatu ring yang merupakan ideal kiri atau bukan.
f. Mengidentifikasikan suatu ring yang merupakan ideal kanan atau bukan.
g. Mengidentifikasikan suatu ring yang merupakan ideal atau bukan.
h. Mengidentifikasikan suatu ring yang merupakan ideal principal atau bukan.
i. Mengidentifikasikan suatu ring yang merupakan ideal prima atau bukan.
j. Mengidentifikasikan suatu ring yang merupakan ideal maksimal atau bukan.
k. Memberikan contoh dan bukan contoh dari ideal, ideal principal, ideal prima, dan ideal maksimal.

Deskripsi Singkat:

Ideal pada dasarnya dapat dibagi menjadi dua jenis, yaitu ideal tidak sejati (ideal improper) dan ideal sejati (ideal proper). Sebuah ideal N dari ring R dikatakan ideal tidak sejati jika $N=R$ dan sebaliknya dikatakan ideal sejati jika $N \neq R$. Ideal sejati terbagi menjadi dua jenis, yaitu ideal sejati trivial dan ideal sejati nontrivial. N dikatakan ideal sejati trivial jika $N=\{0\}$ dan sebaliknya dikatakan ideal sejati nontrivial jika $N \neq R$ dan $N \neq \{0\}$. Secara umum, sebarang ring R memiliki minimal dua buah ideal yaitu ideal tidak sejati ($N=R$) dan ideal trivial ($N=\{0\}$). Suatu ring yang hanya tepat memiliki dua buah ideal adalah sebuah *field* (ingat juga bahwa sebuah field hanya memiliki dua buah subfield). Selain itu, ada juga ideal yang memiliki karakteristik khusus, misalnya ada ideal proper yang tidak termuat dalam ideal proper lainnya (disebut ideal maksimal) dan ada ideal yang bersifat bahwa setiap perkalian yang menghasilkan suatu elemen dalam ideal maka salah satu faktornya pasti merupakan elemen dalam ideal tersebut (disebut ideal prima). Pada bab ini, akan dibahas tentang ideal kiri, ideal kanan, syarat terbentuknya ideal, ideal principal (ideal utama), ideal prima, dan ideal maksimal.

4.1 IDEAL

Definisi 4.1.

Misalkan $\langle R,+,\cdot\rangle$ adalah suatu Ring dan $\langle S,+,\cdot\rangle$ adalah Subring dari R disebut **Ideal Kiri** jika $\forall a\in S$ dan $\forall r\in R$ berlaku $ra\in S$. Atau dengan kata lain, misalkan $\langle R,+,\cdot\rangle$ adalah suatu Ring dan $S\neq\emptyset$ merupakan himpunan bagian dari R atau $S\subseteq R$ disebut Ideal Kiri, jika $\forall a,\ b\in S$ dan $\forall r\in R$, berlaku:

i) $a-b\in S$
ii) $a\cdot b\in S$
iii) $ra\in S$

Contoh 4.1:

$R=M_2\,(Z)$ matriks 2×2 dengan unsur-unsur matriks bilangan bulat. $K\subset R$ dimana $K=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\forall a,b\in Z$. Selidiki apakah K merupakan ideal kiri dari R.

Penyelesaian:

i) Akan dibuktikan $\forall A,\ B\in K\rightarrow A-B\in K$

Ambil sembarang unsur misal $A=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix};B=\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix},\forall a,b,c,d\in Z$

$$A-B=\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}-\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$$

$$=\begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix}$$

jika $\forall a,\ c\in Z\rightarrow a-c\in Z$ dan
jika $\forall b,\ d\in Z\rightarrow b-d\in Z$

akibatnya $\begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in K$

ii) Akan dibuktikan $\forall A, B \in K \rightarrow A \cdot B \in K$

Ambil sembarang unsur (seperti di atas), maka:

$$A \cdot B = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$$

$= \begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix}$ karena

$\forall a, c \in Z \rightarrow ac \in Z$

$\forall b, c \in Z \rightarrow bc \in Z$

akibatnya $\begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix} \in K$

iii) Akan dibuktikan K ideal kiri dari $R = M_2\ (Z)$

$\forall R \in M_2\ (Z)$ dan $\forall A \in K$, maka $RA \in K$

Ambil sembarang unsur $R = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix}$ dan $A = \begin{bmatrix} a_1 & 0 \\ a_2 & 0 \end{bmatrix} \in K$

Akan dibuktikan $Ra \in K$

$$RA = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ a_2 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 r_1 + a_2 r_3 & 0 \\ a_1 r_2 + a_2 r_4 & 0 \end{bmatrix} \in K$$

Karena $a_1\ r_1 + a_2\ r_3 \in Z$ dan $a_1\ r_2 + a_2\ r_4 \in Z$ maka $Ra \in K$

$\therefore$ Terbukti K ideal kiri dari $R = M_2\ (Z)$

Definisi 4.2.

Misalkan $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $\langle S, +, \cdot \rangle$ adalah Subring dari R disebut **Ideal Kanan** jika $\forall a \in S$ dan $\forall r \in R$ berlaku $ar \in S$. Atau dengan kata lain, misalkan $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $S \neq \varnothing$ merupakan himpunan bagian dari R atau $S \subseteq R$ disebut Ideal Kanan, jika $\forall a,\ b \in S$ dan $\forall r \in R$, berlaku:

i) $a - b \in S$

ii) $a \cdot b \in S$

iii) $ar \in S$

Contoh 4.2:

$R = M_2(Z)$ matriks 2×2 dengan unsur-unsur matriks bilangan bulat. $K \subset R$ di mana $K = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \forall a, b \in Z$. Buktikan bahwa K ideal kanan dari R.

Penyelesaian:

i) Akan dibuktikan $\forall A, B \in K \rightarrow A - B \in K$

Ambil sembarang unsur misal $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}; B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}, \forall a,b,c,d \in Z$

$$A - B = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix}$$

jika $\forall a, c \in Z \rightarrow a - c \in Z$ dan

jika $\forall b, d \in Z \rightarrow b - d \in Z$

akibatnya $\begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in K$

ii) Akan dibuktikan $\forall A, B \in K \rightarrow A \cdot B \in K$

Ambil sembarang unsur (seperti di atas), maka:

$$A \cdot B = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix} karena$$

$\forall a,c \in Z \rightarrow ac \in Z$

$\forall a,d \in Z \rightarrow ad \in Z$

akibatnya $\begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix} \in K$

iii) Akan dibuktikan K ideal kanan dari $R = M_2(Z)$

$\forall R \in M_2(Z)$ dan $\forall A \in K$, maka $AR \in K$

Ambil sembarang unsur $R = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix}$ dan $A = \begin{bmatrix} a_1 & a_2 \\ 0 & 0 \end{bmatrix} \in K$

Akan dibuktikan AR$\in$K

$$AR = \begin{bmatrix} a_1 & a_2 \\ 0 & 0 \end{bmatrix}\begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix}$$

$$= \begin{bmatrix} a_1r_1 + a_2r_2 & a_1r_3 + a_2r_4 \\ 0 & 0 \end{bmatrix} \in K$$

Karena $a_1r_1 + a_2r_2 \in Z$ dan $a_1r_3 + a_2r_4 \in Z$, maka $AR \in K$

$\therefore$ Terbukti K ideal kanan dari $R = M_2\,(Z)$

Definisi 4.3

Misalkan $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $\langle S, +, \cdot \rangle$ adalah Subring dari R disebut **Ideal** jika merupakan ideal kiri dan ideal kanan, yaitu $\forall a \in S$ dan $\forall r \in R$ berlaku $ra \in S$ dan $ar \in S$. Atau dengan kata lain, misalkan $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $S \neq \varnothing$ merupakan himpunan bagian dari R atau $S \subseteq R$ disebut Ideal, jika $\forall a,\, b \in S$ dan $\forall r \in R$, berlaku:

i) $a - b \in S$

ii) $a \cdot b \in S$

iii) $ra \in S$ dan $ar \in S$

Contoh 4.3:

Buktikan bahwa $K = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in M_2(2Z) \right\}$ merupakan ideal dari $R = M_2\,(Z)$

Penyelesaian:

a) Akan dibuktikan $A - B \in K$, $\forall A, B \in K$

Ambil sebarang unsur, misal $A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$ dan $B = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$, $\forall A, B \in K$

$$A - B = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} - \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 - b_1 & a_2 - b_2 \\ a_3 - b_3 & a_4 - b_4 \end{bmatrix}$$

Karena $a_1 - b_1, a_2 - b_2, a_3 - b_3, a_4 - b_4 \in 2Z$

Terbukti $A - B \in K$

b) Akan dibuktikan $A \cdot B \in K$, $\forall A, B \in K$

Ambil sebarang unsur, misal $A = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix}$ dan $B = \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$, $\forall A, B \in K$

$$A \cdot B = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \cdot \begin{bmatrix} b_1 & b_2 \\ b_3 & b_4 \end{bmatrix}$$
$$= \begin{bmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{bmatrix}$$

Karena $a_1b_1 + a_2b_3, a_1b_2 + a_2b_4, a_3b_1 + a_4b_3, a_3b_2 + a_4b_4 \in 2Z$

Terbukti $A \cdot B \in K$

c) Akan dibuktikan K ideal kiri dari R atau $RK \in M_2\ (2Z)$

Ambil sembarang unsur, misal $R = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ dan $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ maka

$$RK = \begin{bmatrix} p & q \\ r & s \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$
$$= \begin{bmatrix} ap + cq & bp + dq \\ ar + cs & br + ds \end{bmatrix}$$

karena $ap + cq, bp + dq, ar + cs, br + ds \in 2Z$

terbukti K ideal kiri dari R

d) Akan dibuktikan K ideal kanan dari R atau $KR \in M_2\ (2Z)$

Ambil sembarang unsur, misal $R = \begin{bmatrix} p & q \\ r & s \end{bmatrix}$ dan $K = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, maka

$$KR = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} p & q \\ r & s \end{bmatrix} = \begin{bmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{bmatrix}$$

karena $ap + br, aq + bs, cp + dr, cq + ds \in 2Z$

terbukti K ideal kanan dari R

$\therefore$ Terbukti bahwa $K = M_2\ (2Z)$ ideal dari $R = M_2\ (Z)$

Contoh 4.4:

Buktikan bahwa N ideal dari R jika $R = \langle Z_8, +, \cdot \rangle$ dan $N = \langle 0, 2, 4, 6 \rangle$

Penyelesaian:

i) Bukti N merupakan subring dari R (diserahkan kepada pembaca)

ii) Akan dibuktikan N ideal kiri dari R atau $rn \in N$

$1 \cdot N = N$

$2 \cdot N = N$

$3 \cdot N = N$

$4 \cdot N = N$

$5 \cdot N = N$

$6 \cdot N = N$
$7 \cdot N = N$
Terbukti N ideal kiri dari R atau $rn \in N$

iii) Akan dibuktikan N ideal kanan dari R atau $nr \in N$
$N \cdot 1 = N$
$N \cdot 2 = N$
$N \cdot 3 = N$
$N \cdot 4 = N$
$N \cdot 5 = N$
$N \cdot 6 = N$
$N \cdot 7 = N$
Terbukti N ideal kanan dari R atau $nr \in N$

$\therefore$ Terbukti N ideal dari R.

Contoh 4.5:

Misalkan $\langle Z, +, \cdot \rangle$ adalah suatu Ring, maka himpunan bagian dari $\langle Z, +, \cdot \rangle$ yaitu $\langle 2Z, +, \cdot \rangle$, $\langle 3Z, +, \cdot \rangle$, $\langle 4Z, +, \cdot \rangle$ dan seterusnya merupakan ideal dari $\langle Z, +, \cdot \rangle$.

Contoh 4.6:

Misalkan $\langle Q, +, \cdot \rangle$ adalah suatu Ring, maka himpunan bagian dari $\langle Q, +, \cdot \rangle$ yaitu $\langle Z, +, \cdot \rangle$ merupakan ideal dari $\langle Q, +, \cdot \rangle$.

Contoh 4.7:

$R = M_2\,(Z)$ matriks 2×2 dengan unsur-unsur matriks bilangan bulat. $K \subset R$ dimana $K = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \forall a, b \in Z$. Selidiki apakah K ideal dari R.

Penyelesaian:

i) Akan dibuktikan $\forall A, B \in K \rightarrow A - B \in K$

Ambil sembarang unsur misal $A = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}; B = \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}, \forall a, b, c, d \in Z$

$$A - B = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} - \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$$
$$= \begin{bmatrix} a - c & 0 \\ b - d & 0 \end{bmatrix}$$

jika $\forall a,c \in Z \rightarrow a-c \in Z$ dan
jika $\forall b,d \in Z \rightarrow b-d \in Z$
akibatnya $\begin{bmatrix} a-c & 0 \\ b-d & 0 \end{bmatrix} \in K$

ii) Akan dibuktikan $\forall A, B \in K \rightarrow A \cdot B \in K$
Ambil sembarang unsur (seperti di atas), maka:

$$A \cdot B = \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \cdot \begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}$$

$$= \begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix} \text{karena}$$

$\forall a,c \in Z \rightarrow ac \in Z$
$\forall b,c \in Z \rightarrow bc \in Z$
akibatnya $\begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix} \in K$

iii) Akan dibuktikan K ideal kiri dari $R = M_2\ (Z)$
$\forall R \in M_2\ (Z)$ dan $\forall A \in K$, maka $RA \in K$
Ambil sembarang unsur $R = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix}$ dan $A = \begin{bmatrix} a_1 & 0 \\ a_2 & 0 \end{bmatrix} \in K$
Akan dibuktikan $RA \in K$

$$RA = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix} \begin{bmatrix} a_1 & 0 \\ a_2 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a_1r_1 + a_2r_3 & 0 \\ a_1r_2 + a_2r_4 & 0 \end{bmatrix} \in K$$

Karena $a_1r_1 + a_2r_3 \in Z$ dan $a_1r_2 + a_2r_4 \in Z$ maka $Ra \in K$ sehingga terbukti K ideal kiri dari $R = M_2\ (Z)$

iv) Akan dibuktikan K ideal kanan dari $R = M_2\ (Z)$
$\forall R \in M_2\ (Z)$ dan $\forall A \in K$, maka $Ar \in K$
Ambil sembarang unsur $R = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix}$ dan $A = \begin{bmatrix} a_1 & 0 \\ a_2 & 0 \end{bmatrix} \in K$
Akan dibuktikan $Ar \in K$

$$AR = \begin{bmatrix} a_1 & 0 \\ a_2 & 0 \end{bmatrix} \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix}$$

$$= \begin{bmatrix} a_1r_1 & a_1r_3 \\ a_2r_1 & a_2r_3 \end{bmatrix} \notin K$$

Sehingga K bukan ideal kanan dari $R = M_2(Z)$

$\therefore$ **K bukan ideal dari** R

Contoh 4.8:

$R = M_2(Z)$ matriks 2×2 dengan unsur-unsur matriks bilangan bulat. $K \subset R$ dimana $K = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \forall a, b \in Z$. Selidiki apakah K ideal dari R.

Penyelesaian:

i) Akan dibuktikan $\forall$A, $B \in K \to A - B \in K$

Ambil sembarang unsur misal $A = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}; B = \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}, \forall a, b, c, d \in Z$

$$A - B = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} - \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix}$$

jika $\forall a, c \in Z \to a - c \in Z$ dan
jika $\forall b, d \in Z \to b - d \in Z$

akibatnya $\begin{bmatrix} a-c & b-d \\ 0 & 0 \end{bmatrix} \in K$

ii) Akan dibuktikan $\forall A, B \in K \to A \cdot B \in K$

Ambil sembarang unsur (seperti di atas), maka:

$$A \cdot B = \begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} c & d \\ 0 & 0 \end{bmatrix}$$
$$= \begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix} \text{karena}$$

$\forall a, c \in Z \to ac \in Z$
$\forall a, d \in Z \to ad \in Z$

akibatnya $\begin{bmatrix} ac & ad \\ 0 & 0 \end{bmatrix} \in K$

iii) Akan dibuktikan K ideal kiri dari $R = M_2(Z)$

$\forall R \in M_2(Z)$ dan $\forall A \in K$, maka $RA \in K$

Ambil sembarang unsur $R = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix}$ dan $A = \begin{bmatrix} a_1 & a_2 \\ 0 & 0 \end{bmatrix} \in K$

Akan dibuktikan $RA \in K$

$$RA = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix} \begin{bmatrix} a_1 & a_2 \\ 0 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 r_1 & a_2 r_1 \\ a_1 r_2 & a_2 r_2 \end{bmatrix} \notin K$$

sehingga terbukti K bukan ideal kiri dari $R = M_2\ (Z)$

iv) Akan dibuktikan K ideal kanan dari $R = M_2\ (Z)$

$\forall R \in M_2\ (Z)$ dan $\forall A \in K$, maka $Ar \in K$

Ambil sembarang unsur $R = \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix}$ dan $A = \begin{bmatrix} a_1 & a_2 \\ 0 & 0 \end{bmatrix} \in K$

Akan dibuktikan $AR \in K$

$$AR = \begin{bmatrix} a_1 & a_2 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} r_1 & r_3 \\ r_2 & r_4 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 r_1 + a_2 r_2 & a_1 r_3 + a_2 r_4 \\ 0 & 0 \end{bmatrix} \in K$$

Karena $a_1 r_1 + a_2 r_2 \in Z$ dan $a_1 r_3 + a_2 r_4 \in Z$, maka $AR \in K$

Sehingga K ideal kanan dari $R = M_2\ (Z)$

$\therefore$ **K bukan** ideal dari R

Teorema 4.1

Misalkan R suatu gelanggang, $N \neq \varnothing, N \subset R$, N adalah ideal dari R jika dan hanya jika:

(1) $\forall a, a \in N$, maka $(a-b) \in N$

(2) $\forall a \in N, \forall r \in R$, maka $ar \in N$ dan $ra \in N$

Bukti:

Misalkan N adalah suatu ideal R, maka menurut definisi maka N adalah subring R yang tentu saja memenuhi $\forall a, a \in N$ maka $(a-b) \in N$ dan $\forall a \in N, \forall r \in R$ berlaku $ar \in N$ dan $ra \in N$. Sebaliknya, apabila $a, a \in N$ maka menurut ketentuan yang berlaku juga berada dalam N sehingga N adalah sebuah subring dari R, selanjutnya karena $\forall a \in N, \forall r \in R$ berlaku $ar \in N$ dan $ra \in N$. Terbukti bahwa N sebuah ideal dari R.

Contoh 4.9:

Misalkan R adalah ring dari semua matriks ordo 2×2 dengan semua elemennya bilangan bulat. Didefinisikan $N=\left\{\begin{bmatrix}0 & a\\0 & b\end{bmatrix} \middle| a,b\in Z\right\}$. Selidikilah apakah N ideal dari R.

Penyelesaian:

Akan dibuktikan $N=\left\{\begin{bmatrix}0 & a\\0 & b\end{bmatrix} \middle| a,b\in Z\right\}$ merupakan ideal dari R.

Ambil sebarang unsur $A=\begin{bmatrix}0 & c\\0 & d\end{bmatrix}$ dan $B=\begin{bmatrix}0 & e\\0 & f\end{bmatrix}$

i) $\forall$A, $A\in N$, maka $(A-B)\in$N

$$A-B=\begin{bmatrix}0 & c\\0 & d\end{bmatrix}-\begin{bmatrix}0 & e\\0 & f\end{bmatrix}$$
$$=\begin{bmatrix}0 & c-e\\0 & d-f\end{bmatrix}$$

Misalkan $c-e=m$ dan $d-f=n$, maka:

$$\begin{bmatrix}0 & c-e\\0 & d-f\end{bmatrix}=\begin{bmatrix}0 & m\\0 & n\end{bmatrix}\in N$$

ii) Akan dibuktikan $N=\left\{\begin{bmatrix}0 & a\\0 & b\end{bmatrix} \middle| a,b\in Z\right\}$ merupakan ideal kiri dari R.

$(\forall A\in N) dan (\forall T\in R)\rightarrow TA\in N$

Ambil sebarang unsur $T=\begin{bmatrix}m & n\\o & p\end{bmatrix}$

$$TA=\begin{bmatrix}m & n\\o & p\end{bmatrix}\begin{bmatrix}0 & c\\0 & d\end{bmatrix}$$
$$=\begin{bmatrix}0 & cm+dn\\0 & co+dp\end{bmatrix}$$

Misalkan $cm+dn=s$ dan $co+dp=t$, maka:

$$\begin{bmatrix}0 & cm+dn\\0 & co+dp\end{bmatrix}=\begin{bmatrix}0 & s\\0 & t\end{bmatrix}\in N$$

Terbukti N ideal kiri dari R

iii) Akan dibuktikan $N=\left\{\begin{bmatrix}0 & a\\0 & b\end{bmatrix} \middle| a,b\in Z\right\}$ merupakan ideal kanan dari R.

$(\forall A \in N) dan (\forall T \in R) \rightarrow AT \in N$

Ambil sebarang unsur $T = \begin{bmatrix} m & n \\ o & p \end{bmatrix}$

$$AT = \begin{bmatrix} 0 & c \\ 0 & d \end{bmatrix} \begin{bmatrix} m & n \\ o & p \end{bmatrix}$$

$$= \begin{bmatrix} co & cp \\ do & dp \end{bmatrix} \notin N$$

N bukan ideal kanan dari R

$\therefore$ Terbukti N bukan ideal dari R

4.2 IDEAL PRINCIPAL

Definisi 4.4

Andaikan R adalah ring komutatif $a \in R$, $Na = \{ra | r \in R\}$, Na adalah ideal dari R, maka ideal yang demikian disebut sebagai ideal ***principal*** **(ideal utama)** dengan unsur pembangun (generator) a.

i) $r_1 a, r_2 a \in Na, (r_1 a - r_2 a) \in Na$

ii) $\forall x \in R$ dan $\forall ra \in Na, x(ra) \in Na$

Contoh 4.10:

Setiap ideal di Z berbentuk $nZ = \langle n \rangle$ merupakan ideal utama yang dibangun oleh n.

Contoh 4.11:

Tentukan semua ideal principal yang dibentuk dari $\langle Z_{12}, +, \cdot \rangle$

Penyelesaian:

$Z^{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$N_1 = 1 \cdot \{0, 1, 2, \ldots, 11\} = Z_{12}$

yaitu *ideal principal* yang dibangun oleh unsur 1

$N_2 = 2 \cdot \{0, 1, 2, \ldots, 11\} = \{0, 2, 4, 6, 8, 10\}$

yaitu *ideal principal* yang dibangun oleh unsur 2

$N_3 = 3 \cdot \{0, 1, 2, \ldots, 11\} = \{0, 3, 6, 9\}$

yaitu *ideal principal* yang dibangun oleh unsur 3

$N_4 = 4 \cdot \{0, 1, 2, \ldots, 11\} = \{0, 4, 8\}$

yaitu ideal principal yang dibangun oleh unsur 4

$N_6 = 6 \cdot \{0, 1, 2, \ldots, 11\} = \{0,6\}$
yaitu *ideal principal* yang dibangun oleh unsur 6

4.3 RING PRINCIPAL

Definisi 4.5.

Suatu ring komutatif yang semua idealnya adalah ideal principal disebut **ring principal.**

Contoh 4.12:

Buktikan bahwa Ring $\langle P(A), +, \cdot\rangle$ adalah ring principal dengan $A = \{1,2\}$ dan himpunan kuasa $P(A) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

Penyelesaian:

Ideal dari himpunan kuasa $P(A)$ adalah $N_0 = \{\emptyset\}, N_1 = \{\emptyset, \{1\}\}$, $N_2 = \{\emptyset, \{2\}\}$, dan $N_3 = \{\emptyset, \{1,2\}\}$ karena $A \cdot B = A \cap B$ maka:

$N_0 = \{\emptyset\} \cap \{\emptyset, \{1\}, \{2\}, \{1,2\}\} = \{\emptyset\} \quad \in P(A)$
$N_1 = \{1\} \cap \{\emptyset, \{1\}, \{2\}, \{1,2\}\} = \{\emptyset, \{1\}\} \in P(A)$
$N_2 = \{2\} \cap \{\emptyset, \{1\}, \{2\}, \{1,2\}\} = \{\emptyset, \{2\}\} \in P(A)$
$N_3 = \{1,2\} \cap \{\emptyset, \{1\}, \{2\}, \{1,2\}\} = \{\emptyset, \{1,2\}\} \quad \in P(A)$

$\therefore$ Terbukti Ring $\langle P(A), +, \cdot\rangle$ adalah ring *principal*

4.4 IDEAL PRIMA

Definisi 4.6.

Suatu ideal sejati N dari ring R dikatakan **ideal prima** jika $\forall x, y \in R$ dengan $xy \in N$, maka $x \in N$ atau $y \in N$.

Contoh 4.13:

Buktikan bahwa $N = \{0,2,4,6,8,10\}$ merupakan ideal prima dari Ring $\langle Z_{12}, +, \cdot\rangle$

Penyelesaian:

$Z_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

$N = \{0, 2, 4, 6, 8, 10\}$

Untuk $N = 2 \rightarrow 2 \times 1$ dimana $2 \in N$ atau $1 \notin N$, maka ideal prima

Untuk $N = 4 \rightarrow 2 \times 2$ dimana $2 \in N$, maka ideal prima

Untuk $N = 6 \rightarrow 2 \times 3$ dimana $2 \in N$ atau $3 \notin N$, maka ideal prima

Untuk $N = 8 \rightarrow 2 \times 4$ dimana $2 \in N$ atau $4 \in N$, maka ideal prima

Untuk $N = 10 \rightarrow 2 \times 5$ dimana $2 \in N$ atau $5 \notin N$, maka ideal prima

$\therefore$ Terbukti bahwa $N = \{0,2,4,6,8,10\}$ merupakan ideal prima dari Ring $\langle Z_{12}, +, \cdot \rangle$

Contoh 4.14:

4Z bukan merupakan ideal prima

Penyelesaian:

$4 \in 4Z$ tetapi $4 = 2 \times 2$ dengan $2 \notin 4Z$

$12 \in 4Z$ tetapi $12 = 2 \times 6$ dengan $2 \notin 4Z$ dan $6 \notin 4Z$

$\therefore$ Terbukti bahwa $4Z$ bukan merupakan ideal prima (salah satu unsur merupakan anggota dari suatu himpunan N, maka dikatakan ideal prima).

4.5 IDEAL MAKSIMAL

Definisi 4.7

Suatu ideal sejati N dari R dikatakan **ideal maksimal** dari ring R, bila untuk setiap ideal M di R berlaku hubungan $M \subseteq N \subseteq R$ atau dengan kata lain semua subring harus merupakan ideal prima.

Contoh 4.15:

Buktikan bahwa $\langle Z_6, +, \cdot \rangle$ merupakan ideal maksimal.

Penyelesaian:

$Z_6 = \{0, 1, 2, 3, 4, 5\}$

Subring dari Z_6 adalah:

$S_1 = \{0,2,4\}$

$S_2 = \{0,3\}$

$a, b \in S_1$, $a \in Z_6 \cup b \in Z_6$

Akan dibuktikan: Ideal Prima dari S_1

$a \in S_1 \cup b \in S_1$

Pilih $2 \in S_1 \rightarrow 2 \times 1 \rightarrow 2 \in S_1 \quad \cup 1 \notin S_1 \rightarrow$ Ideal prima dari Z_6

Pilih $4 \in S_1 \rightarrow 2 \times 2 \rightarrow 2 \in S_1 \quad \rightarrow$ Ideal prima dari Z_6

Akan dibuktikan: Ideal Prima dari S_2

$a \in S_2 \cup b \in S_2$

Pilih $3 \in S_2 \rightarrow 3 \times 1 \rightarrow 3 \in S_2 \quad \cup 1 \notin S_2 \rightarrow$ Ideal prima dari Z_6

$\therefore$ **Terbukti bahwa $\langle Z_6, +, \cdot \rangle$ merupakan ideal maksimal.**

$$\begin{tikzcd}
 & Z_6 \arrow[dl] \arrow[dr] & \\
\{0,2,4\} \arrow[dr] & & \{0,3\} \arrow[dl] \\
 & \{0\} &
\end{tikzcd}$$

Contoh 4.16:

Tentukan semua ideal maksimal dari Z_{12}

$$\begin{tikzcd}
 & Z_{12} \arrow[dl] \arrow[dr] & \\
\langle 2 \rangle = \{0,2,4,6,8,10\} \arrow[d] \arrow[dr] & & \langle 3 \rangle = \{0,3,6,9\} \arrow[dl] \\
\langle 4 \rangle = \{0,4,8\} & \langle 6 \rangle = \{0,6\} \arrow[d] & \\
 & \{0\} &
\end{tikzcd}$$

Berdasarkan gambar diagram lattice di atas, ideal proper dari Z_{12} adalah $\langle 0 \rangle, \langle 6 \rangle, \langle 4 \rangle, \langle 3 \rangle$, dan $\langle 2 \rangle$. Ideal $\langle 0 \rangle, \langle 6 \rangle$, dan $\langle 4 \rangle$ jelas bukan ideal maksimal dari Z_{12} karena ideal-ideal tersebut termuat dalam $\langle 2 \rangle$. Sehingga, dapat kita pastikan bahwa ideal maksimal dari Z_{12} adalah $\langle 2 \rangle$ dan $\langle 3 \rangle$.

Contoh 4.17:

Buktikan bahwa $4Z$ adalah ideal maksimal dari $2Z$.

Bukti:

$4Z = \{\ldots, -16, -12, -8, -4, 0, 4, 8, 12, 16, \ldots\}$

$2Z = \{\ldots, -10, -8, -6, -4, -2, 0, 2, 4, 6, 8, 10, \ldots\}$

Misalkan U ideal dari 2Z, $4Z \subseteq U \subseteq R$, maka:
akan ditunjukkan $U = 4Z \cup U = 2Z$
misalkan $U \neq 4Z$ $\exists a \in U$ tetapi $a \notin 4Z$
katakan $a = 4k + 2$ dengan $k \in Z$, $a \in U, 4k \in U$
$\rightarrow a - 4k = 4k + 2 - 4k$
$= 2 \in U$
Karena $2 \in U$ maka $u = 2Z$

$\therefore$ **Terbukti 4Z ideal maksimal dari 2Z**

Teorema 4.2

Andaikan R adalah suatu ring dengan unsur kesatuan 1, jika N adalah suatu ideal dari R yang mengandung unsur satuan maka $N = R$.

Bukti:

Misalkan $a \in N$ adalah unsur satuan, maka $a^{-1} \in R$, karena N adalah suatu ideal, maka $a^{-1}\ a = 1 \in R$, hal ini berakibat bahwa untuk setiap $r \in R$, maka $r = r \cdot 1 \in N$, jadi $N = R$, akibatnya: jika F adalah suatu lapangan, maka F tidak mempunyai ideal sejati.

Bukti:

Andaikan N adalah sebarang ideal dari lapangan F, jika $N = (0)$, maka N adalah ideal tak sejati dari F. Selanjutnya kita misalkan $N \neq \{0\}$, karena F adalah suatu lapangan, setiap $n \in N$ dengan $n \neq 0$ adalah suatu unsur satuan. Berdasarkan teorema di atas, maka $N = F$ sehingga F tidak mempunyai ideal sejati.

Contoh 4.18:

Z_5 adalah sebuah *field*, dan tidak mempunyai sub ideal sejati karena Z_5 tidak mempunyai sub ring.

RANGKUMAN

1. Misalkan $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $\langle S, +, \cdot \rangle$ adalah Subring dari R disebut Ideal Kiri jika $\forall a \in S$ dan $\forall r \in R$ berlaku $ra \in S$. Atau dengan kata lain, misalkan $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $S \neq \varnothing$ merupakan himpunan bagian dari R atau $S \subseteq R$ disebut Ideal Kiri, jika $\forall a, b \in S$ dan $\forall r \in R$, berlaku:

i) $a - b \in S$
ii) $a \cdot b \in S$
iii) $ra \in S$

2. Misalkan $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $\langle S, +, \cdot \rangle$ adalah Subring dari R disebut Ideal Kanan jika $\forall a \in S$ dan $\forall r \in R$ berlaku $ar \in S$. Atau dengan kata lain, misalkan $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $S \neq \emptyset$ merupakan himpunan bagian dari R atau $S \subseteq R$ disebut Ideal Kanan, jika $\forall a, b \in S$ dan $\forall r \in R$, berlaku:
   i) $a - b \in S$
   ii) $a \cdot b \in S$
   iii) $ar \in S$
3. Misalkan $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $\langle S, +, \cdot \rangle$ adalah Subring dari R disebut Ideal jika merupakan ideal kiri dan ideal kanan, yaitu $\forall a \in S$ dan $\forall r \in R$ berlaku $ra \in S$ dan $ar \in S$. Atau dengan kata lain, *misalkan* $\langle R, +, \cdot \rangle$ adalah suatu Ring dan $S \neq \emptyset$ merupakan himpunan bagian dari R atau $S \subseteq R$ disebut Ideal, jika $\forall a, b \in S$ dan $\forall r \in R$, berlaku:
   i) $a - b \in S$
   ii) $a \cdot b \in S$
   iii) $ra \in S$ dan $ar \in S$
4. Misalkan R suatu gelanggang, $N \neq \emptyset$, $N \subset R$, N adalah ideal dari R jika dan hanya jika:
   i) $\forall a, a \in N$, maka $(a - b) \in N$
   ii) $\forall a \in N$, $\forall r \in R$, maka $ar \in N$ dan $ra \in N$
5. Andaikan R adalah ring komutatif $a \in R$, $Na = \{ra \mid r \in R\}$, Na adalah ideal dari R, maka ideal yang demikian disebut sebagai ideal principal (ideal utama) dengan unsur pembangun (generator) a.
   i) $r_1 a, r_2 a \in Na, (r_1 a - r_2 a) \in Na$
   ii) $\forall x \in R$ dan $\forall ra \in Na, x(ra) \in Na$
6. Suatu ring komutatif yang semua idealnya adalah ideal principal disebut ring principal.
7. Suatu ideal sejati N dari ring R dikatakan ideal prima jika $\forall x, y \in R$ dengan $xy \in N$, maka $x \in N$ atau $y \in N$.
8. Suatu ideal sejati N dari R dikatakan ideal maksimal dari ring R, bila untuk setiap ideal M di R berlaku hubungan $M \subseteq N \subseteq R$ atau dengan kata lain semua subring harus merupakan ideal prima.
9. Andaikan R adalah suatu ring dengan unsur kesatuan 1, jika N adalah suatu ideal dari R yang mengandung unsur satuan maka $N = R$.

LATIHAN

1. Diketahui Ring R dari matriks-matriks persegi berordo 3 dengan operasi penjumlahan dan perkalian matriks, selidiki apakah $N = \left\{ \begin{bmatrix} a & b & c \\ 0 & 0 & 0 \\ d & e & f \end{bmatrix} \middle| a,b,c,d,e,f \in Z \right\}$ adalah ideal dari R.

2. Diketahui $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a,b,c \in Z \right\}$ suatu ring terhadap operasi penjumlahan dan perkalian matriks. Buktikan bahwa $N = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} \middle| b \in Z \right\}$ ideal dalam R.

3. Jika R adalah Ring himpunan bilangan bulat, r suatu bilangan bulat dan $N = \{ra \mid a \in Z\}$ tunjukkan bahwa N adalah ideal dari R.
4. Misalkan $Q(\sqrt{2}),+,\cdot$ adalah subring dari Q. Tunjukkan bahwa $Q(\sqrt{2})$ adalah suatu ideal dari Q, didefinisikan $Q(\sqrt{2}) = \{a + b(\sqrt{2}) | a,b \in Q\}$
5. Misalkan M dan N adalah ideal di ring R, buktikan bahwa $M \cap N$ adalah ideal di R.
6. Tentukan semua ideal principal yang dibentuk dari $\langle Z_{18}, +, \cdot \rangle$
7. Buktikan bahwa Ring $\langle P(A), +, \cdot \rangle$ adalah ring principal dengan $A = \{1,2,3\}$, dan himpunan kuasa dari A atau $P(A) = \{\varnothing,\{1\},\{2\},\{3\},\{1,2\},\{1,3\},\{2,3\},\{1,2,3\}\}$
8. Buktikan bahwa $N = \{0,3,6,9\}$ merupakan ideal prima dari Ring $\langle Z_{12}, +, \cdot \rangle$
9. Tentukan semua ideal maksimal dari Z_{24} dan Z_{30}
10. Tentukan semua ideal dari masing-masing ring berikut. Tentukan jenis dari ideal yang diberikan, apakah termasuk ideal maksimal atau ideal prima.
    a. Z_{18}
    b. Z_{25}
    c. $M_2(R)$, matriks 2×2 dengan entri-entri bilangan real R.
    d. $M_2(Z)$, matriks 2×2 dengan entri-entri bilangan bulat Z.
    e. Q

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$Tingkat\ penguasaan = \frac{Banyak\ jawaban\ yang\ benar}{Banyak\ soal} \times 100\%$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai di bawah ini:

Rentang Nilai (%)	Kategori
90 – 100	Sangat Baik
80 – 89	Baik
70 – 79	Sedang
≤ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi ≥ 70%, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang < 70%, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

BAB 5

RING FAKTOR

Tujuan Instruksional Umum:

Setelah mempelajari materi pada bab ini, maka diharapkan mahasiswa mampu mengetahui dan mengaplikasikan syarat-syarat terpenuhinya ring faktor (*quotient ring*).

Tujuan Instruksional Khusus:

Setelah diberikan penjelasan terkait definisi terbentuknya suatu ring faktor (*quotient ring*), maka mahasiswa diharapkan dapat:

a. Menjelaskan definisi dari ring faktor (*quotient ring*) dan gelanggang residu.
b. Menentukan koset-koset dari ideal dalam ring.
c. Menentukan ring faktor (*quotient ring*) dari sebuah ring.
d. Mengidentifikasikan suatu ring yang merupakan ring faktor (*quotient ring*) atau bukan.
e. Mengidentifikasikan suatu ring ring faktor (*quotient ring*) yang merupakan daerah integral atau bukan.
f. Mengidentifikasikan suatu ring ring faktor (*quotient ring*) yang merupakan *field* atau bukan.

Deskripsi Singkat:

Jika sebuah grup mempunyai subgrup normal, maka himpunan semua koset-koset kanan/kiri dari subgrup normal tersebut akan membentuk sebuah grup yang dikatakan grup faktor. Begitu juga pada ring R, himpunan semua koset dari ideal dalam ring R akan membentuk sebuah gelanggang kembali yang dikatakan Ring Faktor.

5.1 RING FAKTOR

Definisi 5.1

Ring faktor (*quotient ring*) secara formal dapat didefinisikan berikut ini:

Diketahui R ring dan N sembarang ideal dalam R, maka sistem aljabar R/N dinyatakan sebagai berikut:

a) $R/N = \{a + N | a \in N\}$

b) R/N pada operasi penjumlahan dapat didefinisikan dengan:

$(a + N) + (b + N) = (a + b) + N$

sedangkan R/N pada operasi perkalian didefinisikan dengan:

$(a + N)(b + N) = ab + N$

Struktur aljabar R/N ini merupakan suatu Ring dan R/N dikatakan **Ring Faktor** (*quotient ring*).

Teorema 5.1

Jika R adalah gelanggang dan N adalah ideal dari R, maka himpunan R/N dari koset-koset dengan operasi penjumlahan $(N, +)$ adalah sebuah ring dengan operasi:

$(N + a) + (N + b) = N + (a + b)$

$(N + a)(N + b) = N + ab$

Bukti:

Kita telah mengetahui bahwa R/N adalah sebuah grup dengan operasi penjumlahan dan grup ini adalah grup dengan operasi penjumlahan dan grup ini adalah grup abelian. Telah kita ketahui sebelumnya bahwa operasi perkalian juga merupakan operasi biner pada R/N, sekarang kita tinggal membuktikan apakah asosiatif terhadap operasi perkalian dan juga berlaku hukum distributif.

Perhatikan sembarang tiga unsur $(N + a), (N + b), (N + c) \in R/N$, maka:

$$((N + a)(N + b))(N + c) = (N + a)((N + b)(N + c))$$
$$(N + ab)(N + c) = (N + a)(N + bc)$$
$$N + (ab)c = N + a(bc)$$

Karena sifat asosiatif pada operasi perkalian pada R, maka berlaku juga sifat distributif pada R/N.

$$(N + a)((N + b) + (N + c)) = (N + a)(N + (b + c))$$

$$= N + (ab + ac)$$
$$= (N + ab) + (N + ac)$$
$$= (N + a)(N + b) + (N + a)(N + c)$$

Teorema 5.2

Misalkan R merupakan suatu ring dan N merupakan ideal dari R. Jika himpunan R/N $\{r + N;\ r \in R\}$ didefinisikan dengan operasi $(r_1 + N) + (r_2 + N) = (r_1 + r_2) + N$ dan $(r_1 + N)(r_2 + N) = r_1 r_2 + N$. Untuk setiap $(r_1 + N)$, $(r_2 + N) \in R/N$, maka $\langle R/N, +, \cdot\rangle$ merupakan suatu ring.

Bukti:

Karena $\langle R, +\rangle$ merupakan suatu grup abelian, maka $\langle R/N, +, \cdot\rangle$ adalah suatu grup komutatif (abelian), sekarang akan dibuktikan bahwa operasi perkalian memnuhi sifat asosiatif dan distributif terhadap operasi penjumlahan.

Misalkan $(r_1 + N)$, $(r_2 + N)$, $(r_3 + N) \in R/N$, maka:

$$\begin{aligned}((r_1 + N)(r_2 + N))(r_3 + N) &= (r_1 r_2 + N)(r_3 + N)\\ &= (r_1 r_2) r_3 + N\\ &= r_1 (r_2 r_3) + N\\ &= (r_1 + N)(r_2 r_3 + N)\\ &= (r_1 + N)((r_2 + N)(r_3 + N))\end{aligned}$$

Sehingga operasi perkalian adalah asosiatif, selanjutnya untuk sembarang $(r_1 + N)$, $(r_2 + N)$, $(r_3 + N) \in R/N$, berlaku:

$$\begin{aligned}(r_1 + N)((r_2 + N) + (r_3 + N)) &= (r_1 + N)((r_2 + r_3) + N)\\ &= (r_1 r_2 + r_1 r_3) + N\\ &= (r_1 r_2 + N) + (r_1 r_3 + N)\\ &= (r_1 + N)(r_2 + N) + (r_1 + N)(r_3 + N)\end{aligned}$$

Dengan cara yang sama akan diperlihatkan bahwa:

$(r_1 + N)((r_2 + N) + (r_3 + N)) = (r_1 + N)(r_3 + N) + (r_2 + N)(r_3 + N)$ sedemikian hingga $\langle R/N, +, \cdot\rangle$ adalah sebuah ring.

Ring R/N pada teorema di atas dikatakan ring faktor (*quotient ring*) dari R modulo N. Berikut ini akan kita diskusikan sifat-sifat dari ring faktor R/N.

Contoh 5.1:

Z adalah sebuah himpunan bilangan bulat dan M adalah himpunan semua bilangan bulat kelipatan 5. Tunjukkanlah bahwa M adalah ideal dari Z, serta tunjukkanlah bahwa koset-koset dalam Z membentuk sebuah gelanggang.

Penyelesaian:

Koset-koset dari M dalam Z adalah:

$M+1=\{\ldots, -9, -4, 1, 6, 11, \ldots\}=M+6=M-4= \ldots$

$M+2=\{\ldots, -8, -3, 2, 7, 12, \ldots\}=M+7=M-3=\ldots$

$M+3=\{\ldots, -7, -2, 3, 8, 13, \ldots\}=M+8=M-2=\ldots$

$M+4=\{\ldots, -6, -1, 4, 9, 14, \ldots\}=M+9=M-1=\ldots$

$M+0=\{\ldots, -10, -5, 0, 5, 10, \ldots\}=M+5=M+10=\ldots$

Sehingga diperoleh:

$Z/M = \{M, M+1, M+2, M+3, M+4\}$

Untuk membuktikan himpunan Z/M membentuk suatu ring (gelanggang) atau tidak, selidiki tabel berikut:

Tabel 5.1. Tabel Cayley untuk Himpunan Z/M pada Operasi +

$+$	M	$M+1$	$M+2$	$M+3$	$M+4$
M	M	$M+1$	$M+2$	$M+3$	$M+4$
$M+1$	$M+1$	$M+2$	$M+3$	$M+4$	M
$M+2$	$M+2$	$M+3$	$M+4$	M	$M+1$
$M+3$	$M+3$	$M+4$	M	$M+1$	$M+2$
$M+4$	$M+4$	M	$M+1$	$M+2$	$M+3$

Tabel 5.2. Tabel Cayley untuk Himpunan Z/M pada Operasi ·

$\bullet$	M	$M+1$	$M+2$	$M+3$	$M+4$
M	M	M	M	M	M
$M+1$	M	$M+1$	$M+2$	$M+3$	$M+4$
$M+2$	M	$M+2$	$M+4$	$M+1$	$M+3$
$M+3$	M	$M+3$	$M+1$	$M+4$	$M+2$
$M+4$	M	$M+4$	$M+3$	$M+2$	$M+1$

Dengan memperhatikan tabel cayley untuk Z/M maka dapat dengan mudah kita selidiki bahwa membentuk sebuah Ring yang dikenal dengan nama **Ring Faktor**.

(Catatan: Buktikan bahwa sebuah grup abelian, asosiatif terhadap operasi perkalian, memenuhi hukum distributif kiri dan kanan).

Contoh 5.2:

Bila $K = \{0,2,4\}$ merupakan ideal yang dibangun oleh unsur 2 dalam Z_6. Tunjukkan bahwa Z_6/K adalah ring faktor (*quotient ring*).

Penyelesaian:

Terdapat dua koset/ideal dari ring Z_6, yaitu:
$K = \{0,2,4\}$
$K + 1 = \{1,3,5\}$

Sehingga $Z_6/K = \{K, K+1\}$

Tabel 5.3. Tabel Cayley $\langle Z_6/K,+\rangle$ dengan Operasi Biner Penjumlahan

$+$	K	$K+1$
K	K	$K+1$
$K+1$	$K+1$	K

Tabel 5.4. Tabel Cayley $\langle Z_6/K,\cdot\rangle$ dengan Operasi Biner Perkalian

$\bullet$	K	$K+1$
K	K	K
$K+1$	K	$K+1$

Dari tabel tersebut menunjukkan penjumlahan dan perkalian unsur-unsur dari Z_6/K. Akan dibuktikan bahwa Z_6/K memenuhi syarat-syarat terbentuknya suatu ring yang merupakan Ring Faktor dari Z_6/K. Kemudian, syarat-syarat terbentuknya ring akan dijelaskan sebagai berikut:

1. Tertutup terhadap operasi penjumlahan $(+)$ di Z_6/K
   $\forall K,\ K+1 \in Z_6/K$
   Berlaku $K + (K+1) = K + (0+1) = K+1$
   Sehingga $K+1 \in Z_6/K$
2. Asosiatif terhadap penjumlahan $(+)$ di Z_6/K
   $\forall K, K+1 \in Z_6/K$
   $$\big(K + (K+1)\big) + (K+1) = K + \big((K+1) + (K+1)\big)$$
   $$\big(K + (0+1)\big) + (K+1) = K + \big(K + (1+1)\big)$$
   $$(K+1) + (K+1) = K + (K+0)$$
   $$K = K$$
   Sehingga $\big(K + (K+1)\big) + (K+1) = K + \big((K+1) + (K+1)\big) = K$

3. Terdapat unsur satuan identitas pada operasi penjumlahan (+) di Z_6/K

$\forall K+1 \in Z_6/K$

$(K+0)+(K+1)=K+(0+1)=K+1$

$(K+1)+(K+0)=K+(1+0)=K+1$

Sehingga $(K+0)+(K+1)=(K+1)+(K+0)=K+1$

4. Terdapat unsur invers terhadap operasi penjumlahan (+) di Z_6/K

$\forall K+1 \in Z_6/K$

$(K+1)+(K+(-1))=K+(1+(-1))=K+0=K$

$(K+(-1))+(K+1)=K+((-1)+1)=K+0=K$

Sehingga $(K+1)+(K+(-1))=(K+(-1))+(K+1)=K+0=K$

5. Berlaku komutatif terhadapoperasi penjumlahan (+) di Z_6/K

$\forall K+1 \in Z_6/K$

$K+(K+1)=(K+1)+K$

$K+(0+1)=K+(1+0)$

$K+1=K+1$

Sehingga $K+(K+1)=(K+1)+K=K+1$

6. Asosiatif terhadap perkalian $(\cdot)$ di Z_6/K

$\forall K,K+1 \in Z_6/K$

$(K\cdot(K+1))\cdot(K+1)=K\cdot((K+1)\cdot(K+1))$

$(K+(0\cdot1))\cdot(K+1)=K\cdot(K+(1\cdot1))$

$(K+0)\cdot(K+1)=K\cdot(K+1)$

$K+(0\cdot1)=K+(0\cdot1)$

$K=K$

Sehingga $(K\cdot(K+1))\cdot(K+1)=K\cdot((K+1)\cdot(K+1))=K$

7. Distributif Kiri terhadap operasi penjumlahan (+) dan perkalian $(\cdot)$ di Z_6/K

$\forall K,\ K+1 \in Z_6/K$

Misalkan $a=K$, $b=K+1$, dan $c=K+1$

$$a \cdot (b+c) = (a \cdot b) + (a \cdot c)$$
$$K \cdot ((K+1)+(K+1)) = (K \cdot (K+1)) + (K \cdot (K+1))$$
$$K \cdot (K+(1+1)) = (K+(0 \cdot 1)) + (K+(0 \cdot 1))$$

$$K \cdot (K+(1+1)) = (K+(0 \cdot 1)) + (K+(0 \cdot 1))$$
$$K \cdot (K+0) = K + ((0 \cdot 1)+(0 \cdot 1))$$
$$K \cdot (K) = K + (0+0)$$
$$K = K$$

Sehingga berlaku hukum distributif kiri yaitu:

$$K \cdot ((K+1)+(K+1)) = (K \cdot (K+1)) + (K \cdot (K+1)) = K$$

8. Distributif Kanan terhadap operasi penjumlahan $(+)$ dan perkalian $(\cdot)$ di Z_6/K

$\forall K, K+1 \in Z_6 / K$

Misalkan $a = K, b = K+1, \text{dan}\, c = K+1$

$$(a+b) \cdot c = (a \cdot c) + (b \cdot c)$$
$$(K+(K+1)) \cdot (K+1) = (K \cdot (K+1)) + ((K+1) \cdot (K+1))$$
$$(K+1) \cdot (K+1) = K + (K+1)$$
$$K+1 = K+1$$

Sehingga berlaku hukum distributif kanan yaitu:

$$(K+(K+1)) \cdot (K+1) = (K \cdot (K+1)) + ((K+1) \cdot (K+1))$$
$$= K+1$$

Jadi, $Z_6/K = \{K, K+1\}$ terbukti merupakan suatu Ring Faktor.

Teorema 5.3:

Apabila R sebuah ring dan N suatu ideal dari R maka R/N adalah suatu Ring.

Bukti:

Ambil $(N+a)$, $(N+b) \in R/N$, maka $(N+a)+(N+b) = N+(a+b) \in R/N$ dan $(N+a)(N+b) = N+ab \in R/N$

Jika $(N+a)$, $(N+b)$, $(N+c) \in R/N$

$((N+a)+(N+b))+(N+c) = (N+(a+b))+(N+c)$

$$
\begin{aligned}
&= (N + ((a + b) + c)) \\
&= (N + (a + (b + c))) \\
&= (N + a) + (N + (b + c)) \\
&= (N + a) + ((N + b) + (N + c))
\end{aligned}
$$

R/N mempunyai elemen 0 (nol) yaitu $N + 0 = N$, sebab jika $N + a \in R/N$, maka:

$(N + a) + (N + 0) = N + (a + 0) = N + a$ dan

$(N + 0) + (N + a) = N + (0 + a) = N + a$

di mana, $\forall \in R/N$ memiliki invers pada operasi penjumlahan, yaitu:

Jika $(N + a) \in R/N$, maka $(N - a) \in R/N$ merupakan invers dari $(N + a) \in R/N$

Sedemikian sehingga:

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

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

Kemudian akan dibuktikan berlaku juga hukum distributif sebagai berikut:

Jika $(N + a)$, $(N + b)$, $(N + c) \in R/N$, maka:

$$
\begin{aligned}
(N + a)\ ((N + b) + (N + c)) &= (N + a)\ (N + (b + c)) \\
&= N + a\ (b + c) \\
&= N + (ab + ac) \\
&= (N + ab) + (N + ac) \\
&= (N + a)\ (N + b) + (N + a)\ (N + c)
\end{aligned}
$$

Dengan cara yang sama akan dibuktikan bahwa:

$((N + a) + (N + b))\ (N + c) = (N + a)\ (N + c) + (N + b)\ (N + c)$

Maka terbuktilah R/N adalah suatu Ring.

5.2 GELANGGANG RESIDU

Definisi 5.2

Jika R suatu Ring dan N suatu ideal dari R, maka R/N dikatakan gelanggang hasil bagi gelanggang faktor dari R oleh S atau **Gelanggang Residu** dari R oleh S.

Lemma 5.1

Misalkan R merupakan ring komutatif dengan unsur kesatuan 1. Jika N merupakan suatu ideal dari R, maka R/N merupakan suatu ring komutatif dengan unsur kesatuan.

Bukti:

Berdasarkan teorema sebelumnya, R/N adalah suatu ring selanjutnya untuk setiap $r_1 + N$, $r_2 + N \in R/N$, maka:

$$(r_1 + N)(r_2 + N) = (r_1 r_2 + N)$$
$$= (r_2 + N)(r_1 + N)$$

Sehingga R/N adalah ring komutatif, karena:

$(1 + N)(r + N) = (r + N)(1 + N) = r + N$

$\forall (r + N) \in R/N$, $(1 + N)$ merupakan unsur kesatuan dari R/N.

Teorema 5.4

Misalkan R merupakan suatu ring komutatif dengan unsur kesatuan 1, dan misalkan N merupakan suatu ideal dari N, maka R/N adalah suatu lapangan (*field*) jika dan hanya jika N merupakan ideal maksimal.

Bukti:

Misalkan R/N adalah suatu lapangan, kita akan perlihatkan bahwa N adalah ideal maksimal. Misalkan M adalah ideal maksimal dari R sehingga $N \subset M$. Kita akan perlihatkan bahwa $M = R$, menurut teori sebelumnya cukup dengan kita perlihatkan bahwa $1 \in M$, misalkan $m \in M$ sehingga $m \notin N$, karenanya $m + N \in R/N$. Karena R/N merupakan *field*, maka $k + N \in R/N$ sehingga $(m + N)(k + N) = 1 + N$. Perhatikan bahwa $(m + N)(k + N) = m\text{-}k + N = 1 + N$. Akibatnya $1 - mk \in N \subset M$. Kemudian, karena M adalah suatu ideal dan $m \in M$, maka $mk \in M$. Dengan demikian, mengakibatkan $1 = (1 - mk) + mk \in M$. Jadi, $M = R$, sehingga N adalah ideal maksimal.

Sebaliknya misalkan N adalah ideal maksimal dari R/N. Kita perlihatkan R/N adalah suatu lapangan, kita cukup memperlihatkan bahwa setiap $(r + N) \in R/N$ adalah unsur satuan. Perhatikan himpunan:

$$S = \{sr + n,\ r \in R \text{ dan } n \in N\}$$

Jelaslah bahwa $N \subset S$, kita perlihatkan bahwa S adalah suatu ideal dari R. Untuk sebarang $sr_1 + N_1$, $sr_2 + n_2 \in S$, maka:

$$(sr_1 + N_1) - (sr_2 + N_2) = sr_1 - sr_2 + N_1 - N_2$$
$$= s(r_1 - r_2) + (N_1 - N_2)$$

Karena $(r_1 - r_2) \in R$ dan $(N_1 - N_2) \in N$, maka $(sr_1 + N_1) - (sr_2 + N_2) \in S$. Selanjutnya, ambil sembarang unsur $r' \in R$ dan $sr + n \in S$, maka $r'(sr + N) = r' sr + r' n = sr' r + r'n$. Jelaslah bahwa $r'r \in R$, kemudian karena N adalah suatu ideal maka $r'n \in N$. Jadi $r'(sr + n) \in S$. Dengan cara yang sama, kita dapat memperlihatkan bahwa $(sr+n)r' \in S$. Jadi, S adalah ideal dari R. Karena N adalah ideal maksimal dari R dan $N \subset S$, maka $S=R$ sehingga unsur kesatuan $1 \in S$. Misalkan $1 = sr + n'$ dengan $n \in N$, maka:

$$(1+N) = sr + n' + N = sr + N = (s+N)(r+N)$$

Hal ini berakibat bahwa setiap unsur tak nol dari R/N adalah unsur satuan. Sehingga R/N adalah suatu lapangan.

Teorema 5.5

Andaikan R merupakan suatu ring komutatif dengan unsur kesatuan 1 dan misalkan N adalah ideal dari R, maka R/N merupakan suatu daerah integral (integral domain) jika dan hanya jika N adalah suatu ideal prima.

Bukti:

Karena R merupakan suatu ring komutatif dengan unsur kesatuan 1, maka R/N adalah suatu ring komutatif dengan unsur kesatuan $(1+N)$. Misalkan N adalah suatu ideal prima, untuk memperlihatkan R/N adalah suatu daerah integral (*integral domain*), akan ditunjukkan bahwa R/N tidak mempunyai unsur pembagi nol. Yakni bila $(r_1+N)\ (r_2+N)=N$, maka harus diperlihatkan $(r_1+N)=N$ atau $(r_2+N)=N$. Misalkan $(r_1+N)\ (r_2+N)=N$, maka $r_1\ r_2+N=N$, hal ini berarti $r_1\ r_2 \in N$. Karena N adalah suatu ideal prima, maka $r_1 \in N$ atau $r_2 \in N$. Sehingga $(r_1+N)=N$ atau $(r_2+N)=N$. Jadi, R/N adalah suatu *integral domain*, sekarang kita akan ditunjukkan bahwa N adalah ideal prima. Yaitu jika $r_1\ r_2 \in N$, maka $r_1 \in N$ atau $r_1 \in N$ untuk semua $r_1\ r_2 \in R$. Perhatikan sembarang dua unsur r_1+N dan r_2+N di R/N. Bila $r_1\ r_2 \in N$, maka $(r_1+N)(r_2+N) = r_1\ r_2+N=N$. Karena R/N adalah suatu daerah integral, $(r_1+N)(r_2+N)=N$ akan selalu berakibat $r_1+N=N$ atau $r_2+N=N$, hal ini berarti $r_1 \in N$ atau $r_2 \in N$. Sehingga N adalah suatu ideal prima.

Contoh 5.3:

Perhatikan ring Z_{12} dengan ideal maksimal $N=\{0, 3, 6, 9\}$. Maka $R/N=\{N, 1+N, 2+N\}$ adalah suatu ring dengan tabel Cayley sebagai berikut:

Tabel 5.5. Tabel Cayley Ring Faktor R/N pada Operasi Penjumlahan

$+$	N	$1+N$	$2+N$
N	N	$1+N$	$2+N$
$1+N$	$1+N$	$2+N$	N
$2+N$	$2+N$	N	$1+N$

Tabel 5.6. Tabel Cayley Ring Faktor R/N pada Operasi Perkalian

$\times$	N	$1+N$	$2+N$
N	N	N	N
$1+N$	N	$1+N$	$2+N$
$2+N$	N	$2+N$	$1+N$

Dari tabel di atas, kita ketahui bahwa R/N adalah suatu lapangan dan juga R/N adalah suatu daerah integral.

Teorema 5.6

Semua ideal maksimal dari ring komutatif R dengan unsur kesatuan merupakan ideal prima.

Bukti:

Jika N merupakan ideal maksimal dari ring komutatif R dengan unsur kesatuan, maka berdasarkan teorema sebelumnya mengakibatkan R/N adalah suatu *field*. Sehingga R/N juga merupakan suatu integral domain, yang pada akhirnya menjamin terbentuknya suatu ideal prima.

Contoh 5.4:

Himpunan $Z_{10}=\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ adalah Ring terhadap operasi-operasi penjumlahan dan perkalian. Tentukan Ring faktor (*quotient ring*) yang terbentuk dari masing-masing ideal maksimal.

Penyelesaian:

Ideal-ideal dalam Z_{10} adalah:

$\langle 0\rangle=\{0\}$

$\langle 1\rangle=\langle 3\rangle=\langle 7\rangle=\langle 9\rangle=\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$\langle 5\rangle=\{0,5\}$

$\langle 2\rangle=\langle 4\rangle=\langle 6\rangle=\langle 8\rangle=\{0, 2, 4, 6, 8\}$

Ideal $N_1 = \langle 2 \rangle$ adalah ideal maksimal dalam Z_{10}. Sehingga ring faktor (*quotient ring*) yang terbentuk adalah:

$Z_{10}/N_1 = \{N_1, N_1 + 1\}$

Jika diambil ideal $N_2 = \langle 5 \rangle$, maka ring faktor (*quotient ring*) yang terbentuk adalah:

$Z_{10}/N_2 = \{N_2, N_2 + 1, N_2 + 2, N_2 + 3, N_2 + 4\}$

Contoh 5.5:

Misalkan $Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$ merupakan suatu ring pada operasi penjumlahan dan perkalian. Tentukan ring faktor yang terbentuk dari ideal maksimal dalam Z_8. Apakah Z_8 merupakan daerah integral?

Penyelesaian:

Ideal-ideal dalam Z_8 yang dihasilkan oleh unsur-unsur Z_8, yaitu:

$\langle 0 \rangle = \{0\}$

$\langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle = Z_8$

$\langle 2 \rangle = \langle 6 \rangle = \{0, 2, 4, 6\}$

$\langle 4 \rangle = \{0,4\}$

Ideal $N_1 = \langle 2 \rangle$ adalah ideal maksimal dalam Z_8. Sehingga ring faktor (*quotient ring*) yang terbentuk adalah:

$Z_8/N_1 = \{N_1, N_1 + 1\}$

Dengan demikian berarti Z_8/N_1 merupakan lapangan (*field*) yang hanya berisi 2 unsur.

Selanjutnya jika kita ambil ideal maksimal $N_2 = \langle 4 \rangle$, maka ring faktor yang terbentuk adalah:

$Z_8/N_2 = \{N_2, N_2 + 1, N_2 + 2, N_2 + 3\}$

Lebih lanjut, Z_8/N_2 mempunya unsur netral (identitas) yaitu $N_2 + 1$. Dalam hal ini, Z_8/N_2 mempunyai unsur pembagi nol sejati yaitu $N_2 + 2$ dan $(N_2 + 2)\,(N_2 + 2) = N_2$. Sehingga Z_8 bukan merupakan daerah integral.

RANGKUMAN

1. Ring faktor (*quotient ring*) secara formal dapat didefinisikan berikut ini: Diketahui R ring dan N sembarang ideal dalam R, maka sistem aljabar R/N dinyatakan sebagai berikut:
   a) $R/N = \{a + N \mid a \in N\}$
   b) R/N pada operasi penjumlahan dapat didefinisikan dengan:

$(a+N)+(b+N)=(a+b)+N$

sedangkan R/N pada operasi perkalian didefinisikan dengan:

$(a+N)(b+N)=ab+N$

Struktur aljabar R/N ini merupakan suatu Ring dan R/N dikatakan ring faktor (*quotient ring*).

2. Jika R adalah gelanggang dan N adalah ideal dari R, maka himpunan R/N dari koset-koset dengan operasi penjumlahan $(N,+)$ adalah sebuah ring dengan operasi:
   $(N+a)+(N+b)=N+(a+b)$
   $(N+a)(N+b)=N+ab$
3. Misalkan R merupakan suatu ring dan N merupakan ideal dari R. Jika himpunan R/N $\{r+N;\ r\in R\}$ didefinisikan dengan operasi $(r_1+N)+(r_2+N)=(r_1+r_2)+N$ dan $(r_1+N)\ (r_2+N)=r_1\ r_2+N$. Untuk setiap (r_1+N), $(r_2+N)\in R/N$, maka $\langle R/N,+,\cdot\rangle$ merupakan suatu ring.
4. Apabila R sebuah ring dan N suatu ideal dari R maka R/N adalah suatu Ring.
5. Jika R suatu Ring dan N suatu ideal dari R, maka R/N disebut gelanggang hasil bagi/ gelanggang faktor dari R oleh S atau Gelanggang Residu dari R oleh S.
6. Misalkan R merupakan ring komutatif dengan unsur kesatuan 1. Jika N merupakan suatu ideal dari R, maka R/N merupakan suatu ring komutatif dengan unsur kesatuan.
7. Misalkan R merupakan suatu ring komutatif dengan unsur kesatuan 1, dan misalkan N merupakan suatu ideal dari N, maka R/N adalah suatu lapangan (*field*) jika dan hanya jika N merupakan ideal maksimal.
8. Andaikan R merupakan suatu ring komutatif dengan unsur kesatuan 1 dan misalkan N adalah ideal dari R, maka R/N merupakan suatu daerah integral (integral domain) jika dan hanya jika N adalah suatu ideal prima.
9. Semua ideal maksimal dari ring komutatif R dengan unsur kesatuan merupakan ideal prima.

LATIHAN

1. Andaikan K merupakan ideal-ideal yang dibangun oleh Z_4. Temukan ideal-ideal yang dibangun tersebut dan buktikan bahwa Z_4/K merupakan ring faktor (*quotient ring*).
2. Temukan K yang merupakan suatu ideal yang dibangun oleh 2 dalam Z_8. Tunjukkan Z_8/K merupakan Ring Faktor.

3. Jika diketahui $B/12$ adalah ring dari semua kelas-kelas bilangan bulat modulo 12. Tentukan elemen-elemen pembagi nol dari $B/12$, kemudian tentukanlah ideal dari $B/12$ yang tidak memuat elemen pembagi nol, dan tentukan ideal maksimal, misalnya N dari ring $B/12$, dan tunjukkan ring faktor dari $B/12$ oleh N adalah suatu *field*.
4. Misalkan Z_{15} merupakan ring terhadap operasi $+$ dan $\cdot$ pada bilangan bulat modulo 15. Tentukan semua ideal dalam Z_{15}, kemudian pilih ideal maksimal N dan temukan Z_{15}/N.
5. Misalkan Z_{18} merupakan ring terhadap operasi $+$ dan $\cdot$ bilangan bulat pada modulo 18. Tentukan semua ideal dalam Z_{18} kemudian pilih ideal maksimal N dan temukan Z_{18}/N. Apakah Z_{18} merupakan daerah integral?

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$\text{Tingkat penguasaan} = \frac{\text{Banyak jawaban yang benar}}{\text{Banyak soal}} \times 100\%$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai di bawah ini:

Rentang Nilai (%)	Kategori
90 – 100	Sangat Baik
80 – 89	Baik
70 – 79	Sedang
$\leq$ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi $\geq$ 70%, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang $<$ 70%, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

BAB 6

HOMOMORFISMA RING

Tujuan Instruksional Umum:

Setelah mempelajari materi pada bab ini, maka diharapkan mahasiswa dapat memahami dan mengidentifikasikan suatu ring yang termasuk homomorfisma ring, kernel dan *image* dari homomorfisma, monomorfisma ring, epimorfisma ring, dan isomorfisma ring.

Tujuan Instruksional Khusus:

Setelah diberikan penjelasan terkait definisi dan syarat terbentuknya homomorfisma ring, kernel dan *image* dari homomorfisma, monomorfisma ring, epimorfisma ring, dan isomorfisma ring, maka mahasiswa dapat:

a. Menjelaskan definisi dari homomorfisma ring, kernel dan *image* dari homomorfisma, monomorfisma ring, epimorfisma ring, dan isomorfisma ring.
b. Mengidentifikasikan suatu ring yang merupakan homomorfisma ring atau bukan.
c. Menentukan kernel dan *image* dari homomorfisma.
d. Mengidentifikasikan suatu ring yang merupakan monomorfisma ring atau bukan.
e. Mengidentifikasikan suatu ring yang merupakan epimorfisma ring atau bukan.
f. Mengidentifikasikan suatu ring yang merupakan isomorfisma ring atau bukan.

Deskripsi Singkat:

Secara umum, definisi homomorfisma ring tidak jauh berbeda dengan definisi homomorfisma grup. Perbedaannya hanya terletak pada banyaknya operasi yang dilibatkan. Homomorfisma grup hanya melibatkan satu operasi biner, sedangkan homomorfisma ring melibatkan dua operasi biner yaitu penjumlahan dan perkalian.

6.1 PENGERTIAN HOMOMORFISMA RING

Definisi 6.1

Sebuah pemetaan f yang membawa dari ring R ke ring R' yang disajikan dalam bentuk $f : R \to R'$, dikatakan sebuah homomorfisma sebuah ring, jika $\forall a, b \in R$, berlaku:

i) $f(a+b) = f(a) + f(b)$

ii) $f(ab) = f(a) \cdot f(b)$

Contoh 6.1:

Ring bilangan bulat Z dengan operasi penjumlahan dan perkalian biasa dengan ring $M_2(Z) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in Z \right\}$, dengan operasi penjumlahan dan perkalian matriks, didefinisikan pemetaan $f(Z) \to M_2\ (Z)$ dengan $f : x \to \begin{bmatrix} x & x \\ x & x \end{bmatrix}$ apakah f sebuah homomorfisma?

Penyelesaian:

Ambil sembarang $x, y \in R$, maka:

$$x + y = \begin{bmatrix} x+y & x+y \\ x+y & x+y \end{bmatrix} = \begin{bmatrix} x & x \\ x & x \end{bmatrix} + \begin{bmatrix} y & y \\ y & y \end{bmatrix}$$

$$x \cdot y = \begin{bmatrix} xy & xy \\ xy & xy \end{bmatrix} \neq \begin{bmatrix} x & x \\ x & x \end{bmatrix} \begin{bmatrix} y & y \\ y & y \end{bmatrix}$$

Dengan demikian pemetaan $f(Z) \to M_2\ (Z)$ dengan $f : x \to \begin{bmatrix} x & x \\ x & x \end{bmatrix}$ bukan sebuah ring homomorfisma.

Contoh 6.2:

Didefinisikan pemetaan $f : R \to M_2\ (Z)$ dengan $f(x) = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix}$. Jika diambil sebarang $x, y \in R$, maka berlaku sifat:

$$f(x+y) = \begin{bmatrix} x+y & 0 \\ 0 & x+y \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} + \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} = f(x) + f(y)$$

$$f(xy) = \begin{bmatrix} xy & 0 \\ 0 & xy \end{bmatrix} = \begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \cdot \begin{bmatrix} y & 0 \\ 0 & y \end{bmatrix} = f(x) \cdot f(y)$$

Hal itu berarti f homomorfisma

Contoh 6.3:

Andaikan $\propto$ merupakan pemetaan dari $Z_2 \to Z_2$ dan untuk sembarang $x \in Z_2$, $\propto(x) = x^2$. Buktikan bahwa $\propto$ merupakan suatu homomorfisma ring.

Penyelesaian:

Untuk membuktikan bahwa $\propto$ adalah suatu homomorfisma ring, maka akan ditunjukkan bahwa untuk sembarang $a, b \in Z_2$ memenuhi dua syarat yang tertuang pada Definisi 6.1. Misalkan ambil sembarang $a,b \in Z_2$, maka:

$\propto(a+b) = (a+b)^2 = a^2 + 2ab + b^2 = \propto(a) + \propto(b)$ (*i*)

Sebagai catatan $ab = $ ba karena Z_2 adalah ring komutatif dan $2ab = 0$ dalam Z_2. Kemudian, berdasarkan sifat komutatif atas perkalian, maka diperoleh:

$\propto(ab) = (ab)^2 = a^2\, b^2 = \propto(a) \propto (b)$ (ii)

Berdasarkan (*i*) dan (ii) maka terbukti bahwa $\propto$ merupakan suatu homomorfisma ring.

Contoh 6.4:

Misalkan β adalah pemetaan dari $Z \to Z$ dengan syarat untuk sembarang $x \in Z$, $\beta(x) = 3x$. Buktikan bahwa β bukan merupakan suatu homomorfisma ring.

Penyelesaian:

Perhatikan bahwa, untuk sebarang $a, b \in Z$

$\beta(a+b) = 3(a+b) = 3a + 3b = \beta(a) + \beta(b)$

Terbukti bahwa β merupakan homomorfisma terhadap penjumlahan. Namun, tidak untuk perkalian. Misalkan, ambil sembarang unsur $a = 1$, $b = 3$, $\forall a, b \in Z$

$\beta(1 \cdot 3) = 3(3) = 9$ sedangkan $\beta(1)\, \beta(3) = (3 \cdot 1)\, (3 \cdot 3) = 27$

Jelas bahwa $\beta(1 \cdot 3) \neq \beta(1)\, \beta(3)$, jadi β beta bukan merupakan ring homomorfisma.

Contoh 6.5:

Tunjukkan bahwa pemetaan $\gamma : C \to M_2\,(R)$ dengan syarat untuk setiap $a + bi \in C, \gamma\left(a + bi\right) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ merupakan homomorfisma ring!

Penyelesaian:

Ambil sebarang $x, y \in C$, maka x dan y dapat dinyatakan dalam bentuk $x = a_1 + b_1 i$ dan $y = a_2 + b_2 i$. Sehingga,

$$\begin{aligned}
\gamma(x+y) &= \gamma\left[(a_1 + b_1 i) + (a_2 + b_2 i)\right] \\
&= \gamma\left[(a_1 + a_2) + (b_1 + b_2) i\right] \\
&= \begin{bmatrix} (a_1 + a_2) & (b_1 + b_2) \\ -(b_1 + b_2) & (a_1 + a_2) \end{bmatrix} \\
&= \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} \\
&= \gamma(a_1 + b_1 i) + \gamma(a_2 + b_2 i) \\
&= \gamma(x) + \gamma(y) \qquad (i)
\end{aligned}$$

dan

$$\begin{aligned}
\gamma(x+y) &= \gamma\left[(a_1 + b_1 i) \cdot (a_2 + b_2 i)\right] \\
&= \gamma\left[(a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1) i\right] \\
&= \begin{bmatrix} (a_1 a_2 - b_1 b_2) & (a_1 b_2 + a_2 b_1) \\ -(a_1 b_2 + a_2 b_1) & (a_1 a_2 - b_1 b_2) \end{bmatrix} \\
&= \begin{bmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{bmatrix} \\
&= \gamma(a_1 + b_1 i)\gamma(a_2 + b_2 i) \\
&= \gamma(x)\ \gamma(y) \qquad (ii)
\end{aligned}$$

Berdasarkan (i) dan (ii) maka dapat disimpulkan bahwa γ merupakan suatu homomorfisma ring.

Contoh 6.6:

Misal Φ: $Z_9 \to Z_2$ dengan aturan: untuk setiap $x \in Z_9, \Phi(x) = r$ di mana r adalah sisa jika x dibagi 2. Tentukan apakah Φ merupakan homomorfisma ring atau bukan.

Penyelesaian:

Misalkan ambil sebarang unsur, $5, 7 \in Z_9$, maka $\Phi(5) = 1$ dan $\Phi(7) = 1$. Sehingga $\Phi(5) + \Phi(7) = 1 + 1 = 0$ dalam Z_2. Di lain pihak, $\Phi(5+7) = \Phi(12)$ $= \Phi(3) = 1$

Karena $\Phi(5) + \Phi(7) \neq \Phi(5+7)$ maka jelas bahwa Φ bukan merupakan homomorfisma ring.

Contoh 6.7:

Sebuah pemetaan f yang membawa dari Ring $R = \langle Z_8, +, \cdot \rangle$ ke ring $S = \langle Z_4, +, \cdot \rangle$ dimana $f(x) =$ sisa pembagian dari 4 (mod 4) apakah f suatu homomorfisma?

Penyelesaian:

$2+3 = f(2+3) = f(2) + f(3) = 1$

$5 \cdot 6 = f(5 \cdot 6) = f(5) \cdot f(6) = 2$

$f(30) = 2 \; Mod \; 4$

$f(5) = 1 \; Mod \; 4$

$f(6) = 2 \; Mod \; 4$

$f(30) = f(5) \cdot f(6)$

$2 = 1 \cdot 2$

Terbukti homomorfisma.

Contoh 6.8:

Pemetaan $f : \langle Z, +, \cdot \rangle \to \langle Z, +, \cdot \rangle$ didefinisikan dengan $f(x) = 2x$ dan ini adalah Ring Homomorfisma dengan operasi penjumlahan, tetapi bukan merupakan sebuah ring homomorfisma sebab tidak memenuhi:

$f(x \cdot y) = 2(xy) \neq 2x \cdot 2y = 4xy$

Contoh 6.9:

Sebuah Ring R dari semua bilangan riel yang membentuk $a + b\sqrt{2}$, dimana a, b∈Z. Pemetaan $f : R \to R$, dimana $f\left(a + b\sqrt{2}\right) = a - b\sqrt{2}$, dengan operasi penjumlahan dan perkalian apakah f sebuah homomorfisma?

Penyelesaian:

i) $\left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right) = f\left(\left(a + b\sqrt{2}\right) + \left(c + d\sqrt{2}\right)\right)$

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

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

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

ii) $$\begin{aligned}(a+b\sqrt{2})\cdot(c+d\sqrt{2}) &= f\left((a+b\sqrt{2})\cdot(c+d\sqrt{2})\right)\\ &= f\left((ac+2bd)+(bc\sqrt{2}+ad\sqrt{2})\right)\\ &= (ac+2bd)-(bc\sqrt{2}+ad\sqrt{2})\\ &= (a-b\sqrt{2})(c-d\sqrt{2})\\ &= f(a+b\sqrt{2})\cdot f(c+d\sqrt{2})\end{aligned}$$

Terbukti Ring Homomorfisma

Lemma 6.1.

Jika R, S, dan T adalah ring dan $\alpha : R \to S$ serta $\beta : S \to T$ adalah ring homomorfisma maka komposisi fungsi $\beta \circ \alpha : R \to T$ juga merupakan homomorfisma ring.

Bukti:

Ambil sebarang $x, y \in R$, maka:

$$\begin{aligned}(\beta\circ\alpha)(x+y) &= \beta[\alpha(x+y)]\\ &= \beta[\alpha(x)+\alpha(y)] \text{(karena } \propto \text{ homomorfisma ring)}\\ &= \beta[\alpha(x)]+\beta[\alpha(y)] \text{(karena } \beta \text{ homomorfisma ring)}\\ &= (\beta\circ\alpha)(x)+(\beta\circ\alpha)(y)\end{aligned}$$

dan

$$\begin{aligned}(\beta\circ\alpha)(xy) &= \beta[\alpha(xy)]\\ &= \beta[\alpha(x)\alpha(y)] \text{(karena } \propto \text{ homomorfisma ring)}\\ &= \beta[\alpha(x)]\beta[\alpha(y)] \text{(karena } \beta \text{ homomorfisma ring)}\\ &= (\beta\circ\alpha)(x)(\beta\circ\alpha)(y)\end{aligned}$$

Dengan demikian dapat disimpulkan bahwa $\beta\circ\alpha$ merupakan homomorfisma ring.

Definisi 6.2

Endomorfisma merupakan suatu homomorfisma dari suatu ring ke dalam dirinya sendiri. Sedangkan **Automorfisma** merupakan suatu endomorfisma yang bijektif dinamakan Automorfisma.

Contoh 6.10.

Buktikan bahwa $f: Q(\sqrt{2}) \to Q(\sqrt{2})$ dengan $f(a+b\sqrt{2}) = a - b\sqrt{2}$ merupakan automorfisma dari $Q(\sqrt{2})$.

Penyelesaian:

Misalkan $a+b\sqrt{2}, c+d\sqrt{2}$ dalam $Q(\sqrt{2})$. Akibatnya:

$$\begin{aligned} f\left(\left(a+b\sqrt{2}\right)+\left(c+d\sqrt{2}\right)\right) &= f\left((a+c)+(b+d)\sqrt{2}\right) \\ &= (a+c)-(b+d)\sqrt{2} \\ &= \left(a-b\sqrt{2}\right)+\left(c-d\sqrt{2}\right) \\ &= f\left(a+b\sqrt{2}\right)+f(c+d)\sqrt{2} \end{aligned}$$

Selanjutnya

$$\begin{aligned} f\left(\left(a+b\sqrt{2}\right)\left(c+d\sqrt{2}\right)\right) &= f\left((ac+2bd)+(ad+bc)\sqrt{2}\right) \\ &= (ac+2bd)-(ad+bc)\sqrt{2} \\ &= \left(a-b\sqrt{2}\right)\left(c-d\sqrt{2}\right) \\ &= f\left(a+b\sqrt{2}\right)f(c+d)\sqrt{2} \end{aligned}$$

Hal itu berarti f homomorfisma ring.

Karena $\mathrm{Ker}(f) \neq Q(\sqrt{2})$ maka f bukan homomorfisma trivial dan $Q(\sqrt{2})$ *field* maka f isomorfisma dari $Q(\sqrt{2})$ ke $f(Q(\sqrt{2}))$. Dengan demikian, terbukti bahwa $f(Q(\sqrt{2})) = Q(\sqrt{2})$.

$\therefore$ **Terbukti bahwa f automorfisma.**

Teorema 6.1

Diketahui $f: A \to B$ homomorfisma ring dengan peta $f(A)$.

(i) $f(A)$ komutatif, jika A komutatif.

(ii) 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 trivial.

(iii) $f(A)$ tidak perlu daerah integral, jika A daerah integral.

(iv) $f(A)$ merupakan *field*, jika A *field* dan $f(1) \neq 0$.

Bukti:

(i) Jika A komutatif, maka untuk sembarang $f(x)$, $f(y)$ dalam $f(A)$ berlaku:

$$f(x)f(y)=f(xy)=f(yx)=f(y)f(x)$$

Sehingga $f(A)$ komutatif.

(ii) Jika $f(1)=0$, maka untuk sembarang $f(x)$, $f(y)$ dalam $f(A)$ berlaku:

$$f(x)=f(x\cdot 1)=f(x)f(1)=f(x)\cdot 0=0$$

Dengan demikian, $f(A)=\{0\}$ dan mengakibatkan $f(A)$ tidak mempunyai elemen satuan. Jika $f(1)\neq 0$, maka $f(1)\ f(x)=f(1\ \cdot x)=f(x)$ dan $f(x)=f(1)=f(x\cdot 1)=f(x)$, sehingga $f(1)$ merupakan elemen satuan dalam $f(A)$.

(iii) Jika didefinisikan pemetaan $f: Z\rightarrow Z_6$ dengan n dalam Z dipetakan ke sisa pembagian dari n dengan modulo 6, maka f merupakan homomorfisma yang surjektif sehingga $f(Z)=Z_6$. Dalam hal ini, Z_6 bukan daerah integral (integral domain), karena $2\cdot 3=0$ dengan $2, 3\in Z_6$ sedangkan Z merupakan integral domain.

(iv) Jika A merupakan *field* dan $f(1)\neq 0$, maka $f(A)$ mempunyai elemen satuan $f(1)$. Ambil sembarang $f(x)\neq 0$, karena f homomorfisma grup terhadap penjumlahan, maka $f(0)=0$. Karena A *field*, maka untuk x dalam A dan $x\neq 0$, maka terdapat x^{-1} sehingga $f(x^{-1}))$ merupakan invers terhadap perkalian dari $f(x)$ dan berlaku:

$$f(x)f\left(x^{-1}\right)=f\left(xx^{-1}\right)=f(1)$$

Hal ini berarti, $f\left(x^{-1}\right)=\left(f(x)\right)^{-1}$

dengan cara yang sama diperoleh: $f\left(x^{-1}\right)f(x)=f(1)$

Dengan demikian, $f\left(x^{-1}\right)=\left(f(x)\right)^{-1}$.

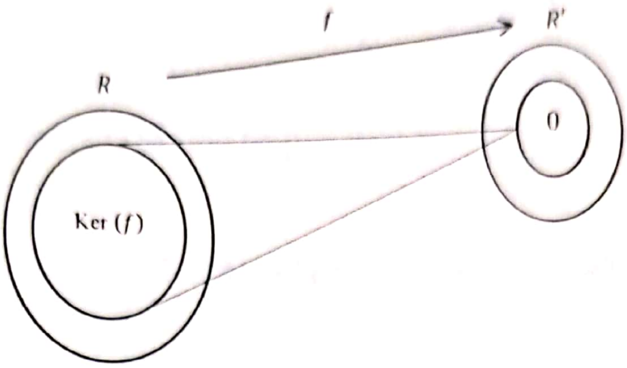
6.2 KERNEL DAN IMAGE DARI HOMOMORFISMA

Definisi 6.3

Misal f: $R\rightarrow R'$ adalah suatu homomorfisma ring, kernel (inti) dari f, ditulis dengan:

$$\operatorname{Ker}(f)=K=\{x\in R | f(x)=0\}$$

Hubungan antara homomorfisma ring dengan Ker f, digambarkan sebagai berikut:



GAMBAR 6.1. Hubungan antara Homomorfisma Ring dengan Ker (f)

Teorema 6.2

Jika adalah suatu homomorfisma ring, maka $Ker\ (f) = K$ adalah ideal dari R.

Bukti:

Karena $f(0) = 0$, mengakibatkan 0 dalam K. Dengan demikian K tidak kosong.

Ambil sembarang unsur, $x, y \in K$ dan sembarang $a \in R$.

$f(x\text{-}y) \quad = f(x) - f(y) = 0 - 0 = 0$

$f(ax) \quad = f(a)\, f(x) = f(a) \cdot 0 = 0$

$f(xa) \quad = f(x)\, f(a) = 0 \cdot f(a) = 0$

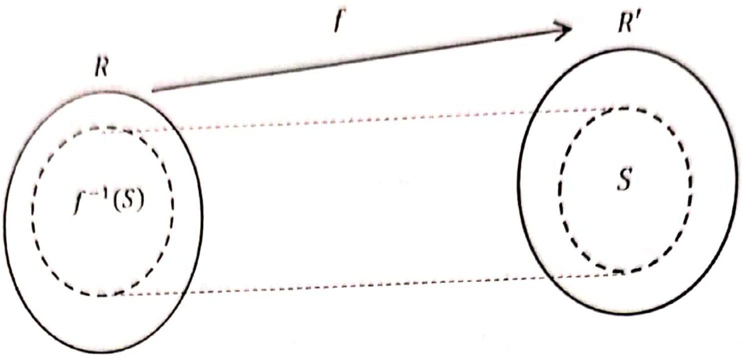
Hal itu berarti $x-y$, ax dan xa dalam K sehingga berdasarkan definisi di atas, K adalah ideal.

Definisi 6.4

Diketahui $f : \mathrm{R} \rightarrow \mathrm{R}'$ sembarang fungsi dan S sembarang himpunan bagian dari R'. Himpunan f^{-1} (S) didefinisikan sebagai semua elemen R yang dibawa f ke elemen S. Ditulis dengan:

$$f^{-1}(S) = \{x \in A | f(x) \in S\}$$

Himpunan $f^{-1}(S)$ dinamakan **prapeta** (*invers image*) dari S di bawah f. Gambar hubungan antara fungsi $f: R \to R'$ dan $f^{-1}(S)$ sebagai berikut:



Gambar 6.2. Hubungan antara fungsi f: R→R' dan f^{-1} (S)

Teorema 6.3

Diketahui $f: R \to R'$ homomorfisma ring.

(i) Jika S ideal dalam $f(R)$, maka $f^{-1}(S)$ ideal dalam R.

(ii) Jika S ring bagian dari R', maka $f^{-1}(S)$ ring bagian dari R.

Bukti:

(i) Jika diambil sembarang 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 ideal dalam $f(R)$.

Berarti $x - y$ dalam $f^{-1}(S)$.

Jika diambil sembarang $r \in R$, maka:

$$f(rx) = f(r)f(x) = f(r) \cdot s'$$

dan

$$f(xr) = f(x)f(r) = s' \cdot f(r)$$

Dalam S karena $f(r)$ dalam $f(R)$ dan S ideal dalam $f(R)$.

Berarti rx dan xr dalam $f^{-1}(S)$.

Terbukti bahwa $f^{-1}(S)$ ideal dalam R.

(ii) Jika diambil sembarang 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 R') dan di samping itu:

$$f(xy)=f(x)f(y)=s'\cdot s''\in S$$

dan

$$f(yx)=f(y)f(x)=s''\cdot s'\in S$$

Berarti $x-y$, xy dan yx dalam $f^{-1}(S)$.
Terbukti bahwa $f^{-1}(S)$ ring bagian dari R.

Contoh 6.11:

Pemetaan $f: Q(\sqrt{2}) \to Q(\sqrt{2})$ dengan $f(a+b\sqrt{2})=a-b\sqrt{2}$ merupakan automorfisma dari $Q(\sqrt{2})$. Himpunan bilangan rasional Q adalah subring dalam $Q(\sqrt{2})$ sehingga $f^{-1}(Q)=Q$ yang adalah subring dari dalam *domain* (daerah asal).

Contoh 6.12:

Misal F adalah *field* dimana setiap elemen x memenuhi:

$$2\cdot x=x+x=0$$

Himpunan Z_2 merupakan salah satu contoh dari *field* yang mempunyai sifat tersebut dan demikian juga *field* didefinisikan f : F→F dengan $f(x)=x^2$.
Akan dibuktikan bahwa f automorfisma.
Ambil sembarang 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:

$$\begin{aligned} f(x+y) &= x^2+2xy+y^2 \\ &= x^2+0+y^2 \\ &= f(x)+f(y) \end{aligned}$$

dan karena F *field*, maka

$$\begin{aligned} f(xy) &= (xy)^2 \\ &= x^2y^2 \\ &= f(x)f(y) \end{aligned}$$

dalam $Z_2(\propto)=\{a+b\propto \mid a, b\in Z_2\}$ juga berlaku sifat:

$$2\cdot x=x+x=0$$

berarti

$f(\alpha)=\propto_2 \quad =\propto+1$

dan

$$\begin{aligned} f(\alpha+1) &= (\alpha+1)^2 \\ &= \alpha^2+2\alpha+1 \\ &= \alpha+1+0+1 \\ &= \alpha \end{aligned}$$

6.3 MONOMORFISMA RING

Definisi 6.5

Misal $f: R \to R'$ adalah sebuah homomorfisma maka f dinamakan monomorfisma jika f injektif.

Contoh 6.13:

Fungsi f yang memetakan $\varphi: R \to R'$ dengan definisi $\varphi = x^2$. Selidiki apakah φ suatu monomorfisme atau bukan.

Penyelesaian:

Ambil sembarang $a, b \in R$, maka
Karena $\exists a \neq b$, tetapi $\varphi(a) = \varphi(b)$
Yaitu $\varphi(2) = 4$ dan $\varphi(-2) = 4$

$\therefore$ **Terbukti φ bukan monomorfisma.**

Contoh 6.14:

Suatu fungsi f yang memetakan $Z_4 \to R$ dimana $R = \langle i \rangle$. Fungsi f tersebut didefinisikan dengan: $f: Z_4 \to R$, dengan $f(x) = i^x$, $x \in Z_4$. Buktikan bahwa fungsi f merupakan suatu monomorfisma.

Penyelesaian:

a. f suatu homomorfisma

$$\begin{aligned} f(xy) &= f(x)\,f(y) \\ &= i^{xy} \\ &= i^x\, i^y \\ &= f(x)\,f(y) \end{aligned}$$

b. f suatu pemetaan yang injektif
Jika $f(x) = f(y)$, maka $x = y$
Dapat kita tunjukkan sebagai berikut:
$Z_4 = \{0, 1, 2, 3\}$
$f(0) = i^0 = 1$

$f(1) = i^0 = i$
$f(2) = i^2 = -1$
$f(3) = i^3 = -i$

$\therefore$ **Terbukti bahwa *f* merupakan suatu monomorfisma.**

Contoh 6.15:

Diketahui dua himpunan bilangan Real R, yaitu: $R^* = \{x \in R | x \neq 0\}$ dan himpunan $R^+ = \{x \in R | x > 0\}$. Diberikan suatu pemetaan f yang memetakan R^* ke R^+ yang didefinisikan sebagai berikut:
$f: R^* \to R^+$ dengan $f(x) = |x|$, $\forall x \in R^*$
Selidiki apakah pemetaan tersebut merupakan monomorfisma atau bukan.

Penyelesaian:

a. f suatu homomorfisma

$$\begin{aligned} f(x \cdot y) &= f(x) \cdot f(y) \\ &= |xy| \\ &= |x| \cdot |y| \\ &= f(x) \cdot f(y) \end{aligned}$$

b. f suatu pemetaan yang injektif

Jika $f(x) = f(y)$, maka $|x| = |y|$
Ambil sembarang unsur, misal: $x = 4$, $y = -4 \to \forall x, y \in R$
$x = 4 \to |x| = 2$
$y = -4 \to |y| = 4$
$\exists x \neq y$ tetapi $f(x) = f(y)$

$\therefore$ **Terbukti bahwa *f* bukan suatu monomorfisma.**

6.4 EPIMORFISMA RING

Definisi 6.6.

Misal $f: R \to R'$ adalah sebuah homomorfisme, maka f dinamakan epimorfisma jika f surjektif.

Contoh 6.16:

Suatu fungsi f yang memetakan $Z_4 \to R$ dimana $R = \langle i \rangle$. Fungsi f didefinisikan dengan:

$f: Z_4 \to R$, dengan $f(x) = i^x$, $x \in Z_4$
Tunjukkan bahwa f merupakan pemetaan yang surjektif.

Penyelesaian:

Ambil sembarang elemen di R, misal $y \in R$, maka:
$y = i^x$, sehingga $x = \log_{iy}$
sehingga jelas bahwa $R = \langle i \rangle = \{1, i, -1, -i\}$
$\therefore$ **Terbukti bahwa f merupakan pemetaan yang surjektif.**

Contoh 6.17:

Didefinisikan sebuah fungsi f yang memetakan dua buah ring $\langle R, +, \cdot \rangle$ dengan $\langle R^+, +, \cdot \rangle$. Fungsi f didefinisikan sebagai berikut:
$f: R \to R^+$, dengan $f(a) = e^a$
Buktikan bahwa f merupakan suatu epimorfisma.

Penyelesaian:

a. f suatu homomorfisma

$$\begin{aligned} f(a_1 + a_2) &= f(a_1)\, f(a_2) \\ &= e^{(a_1 + a_2)} \\ &= e^{a_1} e^{a_2} \\ &= f(a_1)\, f(a_2) \end{aligned}$$

b. f suatu pemetaan yang surjektif
Ambil sembarang unsur di R^+, misal $b \in R^+$, maka:
$b = e^a$ diperoleh $a = \ln b$
Sehingga $f(a) = e^a = e^{(\ln b)} = b$

$\therefore$ **Terbukti bahwa f merupakan suatu epimorfisma.**

Contoh 6.18:

Diketahui himpunan matriks $M = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \middle| a, b, c \in Z \right\}$ adalah Ring terhadap operasi penjumlahan dan perkalian matriks. Tunjukkan bahwa pemetaan $\varphi : M \to Z$, yang didefiniskan oleh $\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} \right) = a$ adalah suatu Epimorfisma.

Penyelesaian:

a) Akan dibuktikan bahwa φ suatu homomorfisma

$$\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}+\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}\right)=\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\right)+\varphi\left(\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}\right)$$

$$\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}+\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}\right)=a+c$$

$$=\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\right)+\varphi\left(\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}\right)$$

Selanjutnya:

$$\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\cdot\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}\right)=\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\right)\cdot\varphi\left(\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}\right)$$

$$\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\cdot\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}\right)=\varphi\begin{bmatrix} ac & 0 \\ bc & 0 \end{bmatrix}=ac$$

$$\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\right)\cdot\varphi\left(\begin{bmatrix} c & 0 \\ d & 0 \end{bmatrix}\right)=ac$$

Terbukti bahwa φ merupakan homomorfisme.

b) Akan ditunjukkan bahwa suatu pemetaan yang surjektif

$$\forall a \in Z, \exists \begin{bmatrix} a & 0 \\ x & 0 \end{bmatrix} \in M$$

Sehingga terbukti bahwa φ pemetaan yang surjektif.

∴ Terbukti bahwa pemetaan φ : $M \rightarrow Z$, yang didefiniskan oleh: $\varphi\left(\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}\right)=a$ adalah suatu Epimorfisma

6.5 ISOMORFISMA RING

Misal terdapat dua Ring, yaitu R dan R'. Ring R dan R' dikatakan Isomorfik jika terdapat suatu Isomorfisma dari R ke R' atau sebaliknya terdapat suatu Isomorfisma dari R ke R'.

Terdapat tiga teorema dasar terkait Isomorfisma Ring. Teorema berikut disebut teorema pertama untuk Isomorfisma Ring.

Definisi 6.7

Suatu homomorfisma μ dari ring R ke R' disebut **isomorfisma** jika μ merupakan pemetaan satu-satu (bijektif) dan onto.

Definisi 6.8

Dua buah ring R dan R' disebut **isomorfik** ($R \approx R'$), jika ada suatu isomorfisma dari ring R ke ring R'.

Teorema 6.4

Misalkan R dan R' adalah suatu Ring. Jika μ adalah suatu Homomorfisma dari R pada R' dengan kernel K, maka $R' \cong R/K$.

Bukti:

Misal $\tau : R/K \rightarrow R$, maka $\tau(K+a) = \mu(a)$

a. Akan ditunjukkan bahwa τ merupakan suatu pemetaan

Misalkan $K+a=K+b$, dimana $K+a, K+b | R/K$

Maka $\tau(K+a)=\mu(a)$ dan $\tau(K+b)=\mu(b)$

Jika μ adalah Homomorfisma maka $\mu(a\text{-}b)=\mu(a)-\mu(b)$

$K+a=K+b$, berarti juga $a-b \in K$

Sehingga:

$\mu(a\text{-}b) = 0'$

$\mu(a)\text{-}\mu(b) = 0'$

$\mu(a) = \mu(b)$

$\tau(K+a) = \tau(K+b)$

Jadi, τ merupakan suatu pemetaan.

b. Akan ditunjukkan bahwa merupakan suatu Homomorfisma

$$\begin{aligned}\tau[(K+a)+(K+b)] &= \tau(K+(a+b)) \\ &= \mu(a+b) \\ &= \mu(a)+\mu(b) \\ &= \tau(K+a)+\tau(K+b)\end{aligned}$$

dan

$$\begin{aligned}\tau[(K+a)\cdot(K+b)] &= \tau(K+(a\cdot b)) \\ &= \mu(a\cdot b) \\ &= \mu(a)\cdot\mu(b) \\ &= \tau(K+a)\cdot\tau(K+b)\end{aligned}$$

Jadi, τ merupakan suatu Homomorfisma.

c. Akan ditunjukkan bahwa τ bersifat injektif $(1-1)$

Misalkan $\mu(a) = \mu(b) \rightarrow K+a=K+b$

$\mu(a) = \mu(b)$

$\mu(a)+\mu(b) = 0'$

Scanned with CamScanner

$\mu(a+b \quad = 0'$

Itu berarti $a - b \in K$, sehingga $K+a=K+b$

Jadi, τ bersifat injektif (1 – 1)

d. Akan ditunjukkan bahwa τ bersifat surjektif (pada)

Misalkan $b \in R'$, berarti $b=\mu(a)$ untuk suatu $a \in R$

Diketahui $a \in R$ dan f: $R \to R/K$, berarti a dipetakan ke $K+a \in R/K$

Kita pilih $c=K+a \in R/K$, sehingga

$\tau(c)=\tau(K+a)=\mu(a)=b \in R'$

Jadi, τ bersifat surjektif (pada)

Terbukti terdapat Isomorfisma dari R/K ke R'

$R' \cong R/K$ atau $R/K \cong R'$

Teorema berikut ini disebut sebagai teorema kedua dari Isomorfisma Ring.

Teorema 6.5

Misalkan R dan R' adalah suatu Ring dan μ adalah Homomorfisma dari R pada R' dengan kernel K. Bila S' adalah suatu Ideal dari R' dan S adalah suatu Ideal dari R, maka $S/K \cong S'$ untuk $S=\{a \in R \mid \mu(a) \in S'\}$.

Bukti:

Untuk membuktikan teorema ini, maka terlebih dahulu perlu kita buktikan bahwa S merupakan Ideal dari R.

Dari definisi Ideal, diperoleh:

a. $S \neq \emptyset$, maka terdapat $0 \in R$, sehingga $\mu(0)=0'$ dan $0' \in S'$

b. S merupakan himpunan bagian dari R, sehingga $S \subseteq R$

c. Misalkan a, $b \in S$

Sehingga diperoleh $a \in R$, $\mu(a) \in S'$ dan $b \in R$, $\mu(b) \in S'$

Jika $a+b \in R$, maka $\mu(a+b)=\mu(a)+\mu(b) \in S'$

d. Misalkan $a \in S$ dan $r \in R$

(*i*) Untuk Ideal Kiri

Misalkan $a \in R$ dan $r \in R$

$\mu(ra)=\mu(r) \cdot \mu(a)$

Sehingga $\mu(a) \in S'$ dan $\mu(r) \in R'$

Karena S' merupakan Ideal R', maka diperoleh:

$\mu(ra)=\mu(r) \cdot \mu(a)$

Jadi, $ra \in S$, sehingga S merupakan Ideal Kiri di R.

(ii) Misalkan $a \in R$ dan $r \in R$

$\mu(ar)=\mu(a) \cdot \mu(r)$

Sehingga $\mu(a) \in S'$ dan $\mu(r) \in R'$

Karena S' merupakan Ideal R', maka diperoleh:

$\mu(ar) = \mu(a) \cdot \mu(r)$

Jadi, $ar \in S$, sehingga S merupakan Ideal Kanan di R.

Maka, dapat disimpulkan bahwa S adalah Ideal di R.

Berikutnya akan ditunjukkan bahwa

Berikutnya akan ditunjukkan bahwa $K \subseteq S$

Misalkan $k \in K$ dan $\mu(k) = 0' \in S'$

Sehingga $k \in S$, yang berarti $\forall k \in K$, $k \in K \rightarrow k \in S$

Dapat disimpulkan $K \subseteq S$

Jadi, pemetaan μ yang dibatasi pada S mendefinisikan suatu Homomorfisma dari S ke S' dengan **Kernel** K. Sehingga berdasarkan teorema pertama Isomorfisma, terbukti bahwa terdapat Isomorfisma dari S/K ke S'.

$$\mathbf{S' \cong S/K \text{ atau } S/K \cong S'}$$

Teorema berikut ini disebut teorema ketiga dari Ismorfisma Ring.

Teorema 6.6.

Misalkan R dan R' merupakan suatu Ring dan μ merupakan Homomorfisma dari R pada R' dengan kernel K. Jika S' adalah suatu Ideal dari R' dan S merupakan suatu Ideal dari R, maka $R/S \cong R'/S'$ untuk $S = \{a \in R | \mu(a) \in S'\}$.

Secara ekuivalen, bila K suatu Ideal dari R dan $K \subseteq S$ merupakan suatu Ideal dari R, maka $R / S \cong \left(\frac{R}{K}\right) / \left(\frac{S}{K}\right)$.

Bukti:

Misalkan $\tau : a \rightarrow \mu(a) + S'$ atau $\tau(a) \in R'/S'$, mendefinisikan pemetaan $\tau : R \rightarrow R'/S'$

a. Akan ditunjukkan bahwa τ merupakan suatu Homomorfisma

Misalkan $a, b \in R$

Sehingga diperoleh $\tau(a) = \mu(a) + S'$ dan $\tau(b) = \mu(b) + S'$

$$\begin{aligned}\tau(a+b) &= \mu(a+b) + S' \\ &= (\mu(a) + \mu(b)) + S' \\ &= (\mu(a) + S') + (\mu(b) + S') \\ &= \tau(a) + \tau(b)\end{aligned}$$

dan

$$\begin{aligned}\tau(a \cdot b) &= \mu(a \cdot b) + S' \\ &= (\mu(a) \cdot \mu(b)) + S' \\ &= (\mu(a) + S') \cdot (\mu(b) + S')\end{aligned}$$

$= \tau(a) \cdot \tau(b)$

Jadi, $\forall a, b \in R$ berlaku $\tau(a+b) = \tau(a) + \tau(b)$ dan $\tau(a \cdot b) = \tau(a) \cdot \tau(b)$, yang berarti τ merupakan suatu Homomorfisma.

b. Akan ditunjukkan bahwa τ bersifat surjektif (pada)
   Ambil $x \in R'/S'$
   Misalkan $x = a' + S'$, $a' \in R'$
   Jika μ pemetaan pada, berarti $\exists a \in R$ sehingga $\mu(a) = a$
   Maka diperoleh $x = \mu(a) + S'$
   Pilih $a \in R$ sehingga $\tau(a) = \mu(a) + S^{\wedge\prime} = x$
   Jadi, $\forall x \in R'/S'$, $\exists a \in R$ sehingga $\tau(a) = x$
   Dengan kata lain, τ bersifat surjektif (pada)

c. Akan ditunjukkan bahwa $S = K$
   Ambil $a \in Ker(\tau) \subseteq R$
   diperoleh $\tau(a) = S'$, padahal $\tau(a) = \mu(a) + S'$
   jadi $\mu(a) + S' = S'$
   karena S' Grup bagian aditif dari R' diperoleh $\mu(a) \in S'$
   berdasarkan definisi Ideal, diperoleh $a \in S$
   jadi, $\forall a \in Ker(\tau) \to a \in S$
   dengan kata lain, $Ker(\tau) \subseteq S$
   ambil $a \in S$, berarti $a \in R$ dan $\mu(a) \in S'$
   diperoleh $\tau(a) = \mu(a) + S' = S'$, sebab $\mu(a) \in S'$
   sehingga $a \in K$, yang berarti $S \subseteq K$
   dari $S \subseteq K$, dapat disimpulkan bahwa $S = K$

Diperoleh $\tau : R \to R'/S'$ Homomorfisma surjektif (pada) dengan kernel $K = S$. Berdasarkan teorema kedua Isomorfisma, diperoleh $R/S \cong R'/S'$. Padalah $R' \cong R/K$ dan $S' \cong S/K$ sehingga terbukti terdapat Isomorfisma dari R'/S' ke R/S.

$$\boldsymbol{R'/S' \cong R/S \cong \left(\frac{R}{K}\right) / \left(\frac{S}{K}\right)}$$

Contoh 6.19:

Suatu pemetaan $f: R \to R'$, dimana $R = Z$ dan $R' = 2Z$, maka pemetaan f merupakan suatu pemetaan yang isomorfisma.

Penyelesaian:

Akan dibuktikan:

f merupakan fungsi injektif dan surjektif
Injektif: ambil sembarang $a,\ b \in R$, dengan $f(a) = f(b) \rightarrow a = b$

$f(a) = f(b)$

$2a = 2b$

$a = b$ (injektif)

Surjektif: $\forall y \in R'\ \exists a \in R$ sedemikian hingga $f(a) = y$

$\exists \frac{y}{2} \in R$ sedemikian hingga $2a = y$

$2(y/2) = y$

$y = y$ (surjektif)

Terbukti f merupakan isomorfik dari R ke R' atau $(R \approx R')$.

Contoh 6.20:

Diberikan D suatu gelanggang, dimana D adalah matriks 2×2 dalam bentuk $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$. Tunjukkan bahwa D isomorfisma dibilangan kompleks C. Dimana D adalah lapangan.

Penyelesaian:

Diberikan $f : C \rightarrow D$ didefinisikan $f(a + ib) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ jelas f satu-satu dan pada.

Misalkan $Z_1 = a + ib$ dan $Z_2 = c + id$, sehingga:

$Z_1 + Z_2 = (a + c) + (b + d)i$ dan $Z_1\ Z_2 = (ac - bd) + (ad + bc)i$

Jadi,

$$f(Z_1) + f(Z_2) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a + c & -(b + d) \\ b + d & a + c \end{bmatrix} = f(Z_1 + Z_2)$$

$$f(Z_1) f(Z_2) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac - bd & -(ad + bc) \\ ad + bc & ac - bd \end{bmatrix} = f(Z_1 Z_2)$$

Terakhir, $f(I) = f(1 + 0i) = I$, identitas matriks.

Jadi, terbukti f adalah Isomorfisma.

Contoh 6.21:

Diketahui Ring $\langle R, +, \cdot \rangle$ isomorfis dengan Ring $\langle R^+, +, \cdot \rangle$ apabila didefinisikan suatu pemetaan dari R ke R^+, didefinisikan sebagai berikut:

$$\varphi : R \rightarrow R^+, \text{dengan}\ \varphi(a) = e^a, \forall a \in R$$

Untuk membuktikan bahwa φ suatu isomorfisma, maka φ harus bijektif dan φ suatu homomorfisma.

Penyelesaian:

a) Akan dibuktikan bahwa φ suatu pemetaan yang bijektif
Misal diberikan sembarang $b \in R^+$, dan $a \in R$, maka $b = e^a$, sehingga $a = \ln b$, diperoleh:

$$\varphi(a) = e^a = e^{(\ln b)} = b$$

Sehingga φ suatu pemetaan yang surjektif, selanjutnya untuk membuktikan φ adalah pemetaan yang injektif.
Misalkan $\varphi(a_1) = \varphi(a_2)$, maka:

$e^{a1} \quad = e^{a2}$

$e^{a1-a2} = 1$

$a_1 - a_2 = 0$

$\quad a_1 = a_2$

Karena $\varphi(a_1) = \varphi(a_2) \rightarrow a^1 = a^2$
Maka φ adalah fungsi yang injektif (satu-satu).
Terbukti φ fungsi bijektif.

b) Akan dibuktikan bahwa φ suatu homomorfisma

$\varphi(a+b) = \varphi(a) \cdot \varphi(b)$

$\qquad = e^{(a+b)}$

$\qquad = e^a \cdot e^b$

$\qquad = \varphi(a) \cdot \varphi(b)$

Terbukti φ adalah suatu homomorfisma.

∴ **Terbukti Ring ⟨R, +, ·⟩ isomorfis dengan ring ⟨R⁺, +, ·⟩**

RANGKUMAN

1. Sebuah pemetaan f yang membawa dari ring R ke ring R' yang disajikan dalam bentuk $f : R \rightarrow R'$, dikatakan sebuah homomorfisma sebuah ring, jika $\forall a, b \in R$, berlaku:
   i) $f(a+b) = f(a) + f(b)$
   ii) $f(ab) = f(a) \cdot f(b)$
2. Jika R, S, dan T adalah ring dan $\alpha : R \rightarrow S$ serta $\beta : S \rightarrow T$ adalah ring homomorfisma maka komposisi fungsi $\beta \circ \alpha : R \rightarrow T$ juga merupakan homomorfisma ring.
3. Diketahui $f : A \rightarrow B$ homomorfisma ring dengan peta $f(A)$.

i) $f(A)$ komutatif, jika A komutatif.

ii) 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 trivial.

iii) $f(A)$ tidak perlu daerah integral, jika A daerah integral.

iv) $f(A)$ merupakan *field*, jika A *field* dan $f(1) \neq 0$.

4. Misal $f : R \rightarrow R'$ adalah suatu homomorfisma ring, kernel (inti) dari f, ditulis dengan:

$$Ker\ (f) = K = \{x \in R \mid f(x) = 0\}$$

5. Jika $f: R \rightarrow R'$ adalah suatu homomorfisma ring, maka Ker$(f) = K$ adalah ideal dari R.

6. Diketahui $f : R \rightarrow R'$ sembarang fungsi dan S sembarang himpunan bagian dari R'. Himpunan $f^{-1}\ (S)$ didefinisikan sebagai semua elemen R yang dibawa f ke elemen S. Ditulis dengan:

$$f^{-1}\ (S) = \{x \in A \mid f(x) \in S\}$$

Himpunan $f^{-1}\ (S)$ dinamakan prapeta (*invers image*) dari S di bawah f.

7. Diketahui $f: R \rightarrow R'$ homomorfisma ring.

i) Jika S ideal dalam $f(R)$, maka $f^{-1}\ (S)$ ideal dalam R.

ii) Jika S ring bagian dari R', maka $f^{-1}\ (S)$ ring bagian dari R.

8. Misal $f : R \rightarrow R'$ adalah sebuah homomorfisma maka f dinamakan monomorfisma jika f injektif.

9. Misal $f : R \rightarrow R'$ adalah sebuah homomorfisme, maka f dinamakan epimorfisma jika f surjektif.

10. Suatu homomorfisma μ dari ring R ke R' disebut isomorfisma jika μ merupakan pemetaan satu-satu (bijektif) dan onto.

11. Dua buah ring R dan R' disebut isomorfik ($R \approx R'$), jika ada suatu isomorfisma dari ring R ke ring R'.

12. Misalkan R dan R' adalah suatu Ring. Bila μ adalah suatu Homomorfisma dari R pada R' dengan kernel K, maka $R' \cong R/K$.

13. Misalkan R dan R' adalah suatu Ring dan μ adalah Homomorfisma dari R pada R' dengan kernel K. Bila S' adalah suatu Ideal dari R' dan S adalah suatu Ideal dari R, maka $S/K \cong S'$ untuk $S = \{a \in R \mid \mu(a) \in S'\}$.

14. Misalkan R dan R' merupakan suatu Ring dan μ merupakan Homomorfisma dari R pada R' dengan kernel K. Jika S' adalah suatu Ideal dari R' dan S merupakan suatu Ideal dari R, maka $R/S \cong R'/S'$ untuk $S = \{a \in R \mid \mu(a) \in S'\}$. Secara ekuivalen, bila K suatu Ideal dari R dan $K \subseteq S$ merupakan suatu Ideal dari R, maka $R\ /\ S \cong \left(\dfrac{R}{K}\right) / \left(\dfrac{S}{K}\right)$.

LATIHAN

1. Tentukan apakah merupakan homomorfisma ring atau bukan.
   a. $f : Z \to Z$ dengan $f(x) = 4x$
   b. $f : Z_6 \to Z_5$ dengan $f(x) = 3x$
   c. $f : R \to R$ dengan $f(x) = x^2$
   d. $f: R \to R$ dengan $f(x) = e^x$
   e. $f : Z \to R$ dengan $f(x) = 2^x$
   f. $f : Z_6 \to Z_3$ dengan $f(x) = a + 1$
   g. $f : Z \to Z$ dengan $f(x) = x^3$
2. Dari soal nomor 1, selidiki manakah yang termasuk monomorfisma, epimorfisma, atau isomorfisma?
3. Tunjukkan bila R, R',dan R'' merupakan suatu ring-ring dan bila g: $R \to R'$ dan $f : R' \to R''$ merupakan suatu homomorfisma-homomorfisma, maka pemetaan komposisi $f \circ g : R \to R''$ adalah juga merupakan Homomorfisma.
4. Buktikan bahwa $\varphi : C \to M_{2\times2}(R)$ yang didefinisikan dengan:

$$\varphi(a + bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

   adalah sebuah isomorfisma dari C ke $M_{2\times2}(R)$.
5. Pemetaan dari C ke C, yang didefinisikan oleh:

$$\varphi : C \to C, \text{dengan } \varphi(a + bi) = a - bi$$

   Selidiki apakah φ merupakan suatu homomorfisma
6. Tunjukkan apakah $Z_2 \times Z_3$ merupakan Isomorfisma terhadap Z_6, sehingga $Z_2 \times Z_3 \cong Z_6$
7. Diketahui pemetaan $f : Z \to R$ yang didefinisikan oleh $f(x) = x$. Buktikan bahwa f adalah suatu homomorfisma yang injektif. Apakah f surjektif?
8. Misalkan F adalah *field* dimana setiap elemen x memenuhi:

$$3 \cdot x = x + x = 0$$

   Himpunan Z_3 merupakan salah satu contoh dari *field* yang memiliki sifat tersebut. Didefinisikan $f : F \to F$ dengan $f(x) = x^3$. Buktikan bahwa f automorfisma.

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$\textit{Tingkat penguasaan} = \frac{\textit{Banyak jawaban yang benar}}{\textit{Banyak soal}} \times 100\%$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai di bawah ini:

Rentang Nilai (%)	Kategori
90 – 100	Sangat Baik
80 – 89	Baik
70 – 79	Sedang
≤ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi ≥ 70%, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang < 70%, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

BAB 7

RING POLINOMIAL

Tujuan Instruksional Umum:

Setelah mempelajari materi pada bab ini, maka mahasiswa diharapkan dapat mengetahui dan menggunakan konsep dasar dari ring polinomial, menentukan teorema sisa dan teorema faktor dalam ring polinomial, serta menentukan polinomial yang *irreducible* dan *reducible*.

Tujuan Instruksional Khusus:

Setelah diberikan penjelasan bentuk umum ring polinomial dan syarat terbentuknya ring polinomial, teorema sisa dan teorema faktor, serta polinomial *irreducible* dan *reducible*, maka mahasiswa dapat:

a. Menjelaskan definisi dari ring polinomial, polinomial yang *irreducible* dan *reducible*
b. Mengaplikasikan teorema sisa dan teorema faktor.
c. Mengaplikasikan definisi algoritma pembagian polinom.
d. Menentukan hasil bagi dan sisa dari suatu algoritma pembagian polinom.
e. Mengidentifikasikan polinomial yang *irreducible* dan *reducible*.

Deskripsi Singkat:

Pada bab 7 ini, membahas tentang ring polinomial, algoritma pembagian polinom, teorema sisa dan teorema faktor dalam ring polinomial, serta menentukan polinomial yang *irreducible* dan *reducible*.

7.1 KONSEP DASAR RING POLINOMIAL

Definisi 7.1.

Bentuk umum dari suatu polinomial adalah:

$$p(x) = a_0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n = \sum_{i=0}^{n} a_i x_i$$

Dimana a_i adalah koefisien dari $p(x)$. Bila $x^n \neq 0$ maka derajat $p(x)$ adalah n dan bila $n = 0$ maka derajat $p(x)$ adalah nol.

Contoh 7.1:

a) $p(x) = 2x^4 + 3x^3 - 2x + 5$, adalah polinom yang mempunyai derajat 4.
b) $p(x) = x^7 + x^3 + 2x^2 - 1$, adalah polinom yang mempunyai derajat 7.
c) $p(x) = 5$, adalah polinom yang mempunyai derajat 0.

Polinomial nol dan polinomial yang berderajat nol, disebut **polinomial konstan.**

Definisi 7.2

Misalkan dua buah polinom $p(x) = a_0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n$ dan $q(x) = b_0 + b_1x^1 + b_2x^2 + \ldots + b_mx^m$ dikatakan sama $p(x) = q(x)$ jika dan hanya jika $a_i = b_i$ untuk semua $i \geq 0$.

Contoh 7.2:

$$2x^4 + 3x^3 - 2x + 5 \neq 2x^4 + 5x^3 - 2x + 5$$

Dua buah polinom di atas dikatakan tidak sama karena memiliki koefisien yang berbeda, di mana koefisien x^3 di ruas kiri bernilai 3, sedangkan koefisien x^3 di ruas kanan bernilai 5.

Contoh 7.3:

$$2x^4 + 5x^3 - 2x + 5 = 2x^4 + 5x^3 - 2x + 5$$

Dua buah polinom di atas dikatakan sama karena memiliki koefisien yang sama pada setiap suku yang bersesuaian.

Definisi 7.3

Misalkan dua buah polonomia $p(x) = a_0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n$ dan $q(x) = b_0 + b_1x^1 + b_2x^2 + \ldots + b_mx^m$, maka hasil penjumlahan dua polinomial yaitu: $p(x) + q(x) = c_0 + c_1x^1 + c_2x^2 + \ldots + c_kx^k$ di mana $k = \text{maks}\{n, m\}$ untuk setiap i, $c_i = a_i + b_i$, untuk $0 \leq i \leq k$.

Contoh 7.4:

Misal $p(x) = 2x^4 + 3x^3 - 2x + 5$ dan $q(x) = 5x^4 + 3x^3 + 3x^2 - 5x + 1$, maka:

$$\begin{aligned} p(x) + q(x) &= \left(2x^4 + 3x^3 - 2x + 5\right) + \left(5x^4 + 3x^3 + 3x^2 - 5x + 1\right) \\ &= (2+5)x^4 + (3+3)x^3 + (0+3)x^2 + (-2-5)x + (5+1) \\ &= 7x^4 + 6x^3 + 3x^2 - 7x + 6 \end{aligned}$$

Definisi 7.4

Misalkan dua buah polinomial $p(x) = a_0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n$ dan $q(x) = b_0 + b_1x^1 + b_2x^2 + \ldots + b_mx^m$, maka hasil perkalian dua buah polinomial yaitu: $p(x) \cdot q(x) = c_0 + c_1x^1 + c_2x^2 + \ldots + c_kx^k$ di mana $k = n + m$ untuk setiap $i, c_i = a_ib_0 + a_{i-1}b_1 + \ldots + a_1b_{i-1} + a_0b_i$.

Contoh 7.5:

Misalkan $p(x) = 3x^2 + x + 2$ dan $q(x) = x + 2$, maka:

$$\begin{aligned} p(x) \cdot q(x) &= (3x^2 + x + 2) \cdot (x + 2) \\ &= 3x^3 + 6x^2 + x^2 + 2x + 2x + 4 \\ &= 3x^3 + 7x^2 + 4x + 4 \end{aligned}$$

Definisi 7.5

Misal R adalah suatu Ring Komutatif. $R[x]$ disebut sebagai Ring Polinomial atas R dengan $R[x] = \{p(x), q(x), r(x), \ldots\}$ untuk $p(x) = \sum_{i=0}^{n} a_ix_i$ dan $q(x) = \sum_{i=0}^{n} bx_i$ dan $a_i \in R$.

Contoh 7.6:

Misal $p(x)$ dan $q(x)$ adalah polinom-polinom pada Z_2 $[x]$ dengan $p(x) = 2x^4 + 3x^3 + 2x + 5$ dan $q(x) = 5x^4 + 3x^3 + 3x^2 + 5x + 1$, maka:

$$\begin{aligned}
p(x)+q(x) &= \left(2x^4+3x^3-2x+5\right)+\left(5x^4+3x^3+3x^2-5x+1\right)\\
&= (2+5)x^4+(3+3)x^3+(0+3)x^2+(2+5)x+(5+1)\\
&= 7x^4+6x^3+3x^2+7x+6 \text{ karena modulo 2, maka}\\
&= 1x^0+0x^1+1x^0+1x+0\\
&= 1+1+x\\
&= x+2
\end{aligned}$$

Contoh 7.7:

Misal $p(x)$ dan $q(x)$ adalah polinom-polinom pada $Z_4\ [x]$, dengan $p(x)=3x^2+x+2$ dan $q(x)=x+2$, maka:

$$\begin{aligned}
p(x)\cdot q(x) &= (3x^2+x+2\ )\cdot(x+2\ )\\
&= (3\cdot 1)x^{(2+1)}+(3\cdot 2)\ x^2+x^{(1+1)}+2x+2x+4\\
&= 3x^3+7x^2+4x+4\\
&= 3x^3+3x^2+0x+0\\
&= 3x^3+3x^2
\end{aligned}$$

Contoh 7.8:

Diketahui dua buah polinomial, yaitu:

$p(x)=2x^3+2x^2+1$ dan $q(x)=3x^2+4x+1$ dalam ring $Z_5\ [x]$.

a) $p(x)+q(x)$

b) $p(x)\cdot q(x)$

Penyelesaian:

$p(x)$ dan $q(x)\in Z_5\ (x)$, maka:

a) $p(x)+q(x)=(2x^3+2x^2+1)+(3x^2+4x+1)$
$\qquad\qquad\qquad = 2x^3+4x+2$

b) $p(x)\cdot q(x)\ =(2x^3+2x^2+1)\cdot(3x^2+4x+1)$
$\qquad\qquad\qquad = x^5+\ 4x^4+4x+1$

Berdasarkan beberapa contoh di atas, dapat ditarik kesimpulan bahwa jika tidak terdapat penjelasan terkait koefisien, maka polinom dianggap sebagai bilangan real. Namun, jika terdapat penjelasan lebih lanjut, maka koefisien berdasarkan Ring yang dimaksud.

Contoh 7.9:

Dalam $Z_2\ [x]$ yaitu ring polinomial dengan koefisien bilangan bulat modulo 2. Misal $p(x) = x + 1$. Hitunglah:

a) $p(x) \cdot p(x)$ dalam $Z_2\,[x]$

b) $p(x) + p(x)$ dalam $Z_2\,[x]$

penyelesaian:

a) $$\begin{aligned} p(x) \cdot p(x) &= (x+1) \cdot (x+1) \\ &= x^2 + 2x + 1 \\ &= x^2 + 1 \end{aligned}$$

b) $$\begin{aligned} p(x) + p(x) &= (x+1) + (x+1) \\ &= 2x + 2 \\ &= 0 \end{aligned}$$

Teorema 7.1

Misalkan R adalah ring komutatif dengan unsur identitas. Maka $R[x]$ adalah ring komutatif dengan unsur identitas.

Bukti:

Akan ditunjukkan bahwa $R[x]$ adalah grup abelian di bawah polinomial penjumlahan. Polinomial nol, $f(X) = 0$, identitas penjumlahan. Diberikan sebuah polinomial $p(x) = \sum_{i=0}^{n} a_i x^i$, invers dari $p(x)$ dengan mudah dapat diverifikasi menjadi $-p(x) = \sum_{i=0}^{n} (-a_i) x^i = \sum_{i=0}^{n} a_i x^i$.

Sifat komutatif dan asosiatif ditunjukkan dari definisi penjumlahan polinomial dan dari fakta penjumlahan di R adalah keduanya komutatif dan asosiatif.

Akan ditunjukkan perkalian polinomial bersifat asosiatif, misalkan:

$$p(x) = \sum_{i=0}^{m} a_i x^i,$$

$$q(x) = \sum_{i=0}^{n} b_i x^i,$$

$$r(x) = \sum_{i=0}^{p} c_i x^i.$$

Maka

$$[p(x)q(x)]r(x) = \left[\left(\sum_{i=0}^{m} a_i x^i\right)\left(\sum_{i=0}^{n} b_i x^i\right)\right]\left(\sum_{i=0}^{p} c_i x^i\right)$$

$$= \left[\sum_{i=0}^{m+n}\left(\sum_{j=0}^{i} a_j b_{i-j}\right)x^i\right]\left(\sum_{i=0}^{p} c_i x^i\right)$$

$$= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i}\left(\sum_{k=0}^{j} a_k b_{j-k}\right)c_j\right]x^i$$

$$= \sum_{i=0}^{m+n+p}\left(\sum_{j+k+l=i} a_j b_k c_r\right)x^i$$

$$= \sum_{i=0}^{m+n+p}\left[\sum_{j=0}^{i} a_j\left(\sum_{k=0}^{i-j} b_k c_{i-j-k}\right)\right]x^i$$

$$= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\sum_{i=0}^{n+p}\left(\sum_{j=0}^{i} b_j c_{i-j}\right)x^i\right]$$

$$= \left(\sum_{i=0}^{m} a_i x^i\right)\left[\left(\sum_{i=0}^{n} b_i x^i\right)\left(\sum_{i=0}^{p} c_i x^i\right)\right]$$

$$= p(x)\left[q(x)r(x)\right]$$

Sifat komutatif dan distributif dari perkalian polinomial dapat dibuktikan dengan cara yang sama. Pembuktian kedua sifat tersebut kita tinggalkan sebagai latihan oleh pembaca.

Proposisi 7.1:

Jika R suatu daerah integral, dan $p(x)$, $q(x) \in \mathrm{R}[x]$ dengan masing-masing $p(x)$ dan $q(x)$ bukan polinomial nol, maka:

$$\deg(p(x) \cdot q(x)) = \deg p(x) + \deg q(x)$$

Jika polinomial $R[x]$ bukan daerah integral, derajat dari hasil suatu perkalian polinomial bisa lebih kecil dari derajat hasil penjumlahan polinomial tersebut.

Contoh 7.10:

Misal $p(x)$ dan $q(x)$ dalam $Z_6\,[x]$ dimana $p(x) = 2x^3 + x$ dan $q(x) = 3x$, maka hitunglah $p(x) \cdot q(x)$ dalam $Z_6\,[x]$.

Penyelesaian:

$$p(x) \cdot q(x) = (2x^3 + x) \cdot 3x$$
$$= 6x^4 + 3x^2$$
$$= 3x^2$$

7.2 ALGORITMA PEMBAGIAN POLINOM

Teorema 7.2

Misalkan $f(x)$ dan $g(x)$ adalah dua buah polinom, dengan $f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ dan $g(x) = b_0 + b_1 x^1 + b_2 x^2 + \ldots + b_m x^m$ di mana $f(x)$, $g(x) \in R[x]$ dan $g(x) \neq 0$, maka terdapat polinom-polinom yang unik $q(x)$, $r(x) \in R[x]$ sedemikian sehingga:

$$f(x) = q(x) \cdot g(x) + r(x)$$

dengan $r(x) = 0$ atau derajat $r(x) <$ derajat $g(x)$.

Polinom-polinom $q(x)$ dan $r(x)$ ditentukan secara tunggal oleh $f(x)$ dan $g(x)$ yang diperlukan. Selanjutnya $f(x)$ disebut polinom yang dibagi, $g(x)$ disebut polinom pembagi, $q(x)$ disebut hasil bagi (*quotient*) polinom, dan $r(x)$ disebut sisa hasil bagi (*reminder*) polinom.

Contoh 7.11:

Tentukan hasil bagi dari polinom-polinom dari $f(x) = x^3 + 4x^2 + 5x + 7$ dan $g(x) = x + 1$.

Penyelesaian:

Diperoleh:

$$\begin{array}{r l}
 & x^2 + 3x + 2 \\
(x+1) \; / & x^3 + 4x^2 + 5x + 7 \\
 & x^3 + x^2 \qquad\qquad - \\
\hline
 & 3x^2 + 5x \\
 & 3x^2 + 3x \qquad - \\
\hline
 & 2x + 7 \\
 & 2x + 2 \quad - \\
\hline
 & 5
\end{array}$$

Jadi, $f(x) = q(x) \cdot g(x) + r(x)$ dengan mengambil $q(x) = x^2 + 3x + 2$ dan $r(x) = 5$.

Contoh 7.12:

Tentukan hasil bagi dan sisa dari polinom-polinom berikut terhadap Z_4 $[x]$, dimana $p(x) = 3x^3 + 3x^2 + 2x + 1$ dan $q(x) = x^2 + 2$, $p(x)$ adalah polinom yang dibagi dan $g(x)$ polinom pembagi.

Penyelesaian:

$p(x) = 3x^3 + 3x^2 + 2x + 1$ adalah polinom yang dibagi dalam Z_4 $[x]$
$q(x) = x^2 + 2$ adalah polinom pembagi dalam Z_4 $[x]$
Hal ini berarti bahwa koefisien-koefisien dari polinom-polinom tersebut hanya bernilai 0, 1, 2, dan 3 saja.

$$\frac{p(x)}{g(x)} = \frac{3x^3 + 3x^2 + 2x + 1}{x^2 + 2}$$

$$\begin{array}{r|l}
 & 3x + 3 \\ \hline
x^2 + 2 & 3x^3 + 3x^2 + 2x + 1 \\
 & 3x^3 \qquad\quad + 2x \qquad\quad - \\ \hline
 & \qquad 3x^2 + \qquad 1 \\
 & \qquad 3x^2 + \qquad 2 \qquad - \\ \hline
 & \qquad\qquad\qquad 3
\end{array}$$

Dari pembagian polinom-polinom tersebut dalam Z_4 $[x]$ dari $\frac{p(x)}{g(x)} = \frac{3x^3 + 3x^2 + 2x + 1}{x^2 + 2}$ adalah $3x + 3$ dengan sisa 3.

7.3 TEOREMA SISA DAN TEOREMA FAKTOR

Definisi 7.6.

Suatu polinom tak konstan $f(x) \in R[x]$ dinamakan **polinom tidak tereduksi** (*irreducible*) atas F apabila $f(x)$ tidak dapat dinyatakan sebagai hasil kali dua polinom $g(x)$ dan $h(x)$ di $R[x]$ dengan derajat $g(x)$ dan derajat $h(x)$ kurang dari derajat $f(x)$. Sebaliknya, apabila terdapat $g(x)$ dan $h(x)$ di $R[x]$ sehingga $f(x) = g(x)h(x)$ dengan derajat $g(x)$ dan derajat $h(x)$ kurang dari derajat $f(x)$ maka $f(x)$ dinamakan **polinom tereduksi** (*reducible*).

Teorema 7.3

Polinomial $f(x)$ jika dibagi oleh $(x-a)$ dalam polinomial $F[x]$ maka sisanya adalah $f(a)$

Bukti:

Dengan menggunakan algoritma pembagian, maka

$$\exists q(x),\ r(x) \in F[x]$$

Dengan $f(x) = q(x)\ (x-a) + r(x)$, dimana jika $r(x) = 0$ atau derajat dari $r(x)$ kurang dari 1. Jadi, sisa pembagian adalah konstan, $r_0 \in F$ dan

$$f(x) = q(x)(x-a) + r_0$$

Sehingga didapat $f(a) = r_0$.

Teorema 7.4

Polinomial $(x-a)$ adalah faktor dari $f(x)$ dalam polinomial $F[x]$ jika dan hanya jika $f(a) = 0$. Suatu elemen $a \in F[x]$ dikatakan akar dari polinomial $f(a) = 0$. Sehingga berdasarkan teorema faktor tersebut, $(x\text{-}a)$ adalah faktor dari $f(x)$ jika dan hanya jika $f(a) = 0$. Suatu polinomial $f(x) \neq 0$ dan $f(x)$ bukan unit, $f(x)$ disebut *irreducible* di $F[x]$ jika:

$$f(x) = g(x) \cdot h(x)$$

Sehingga $g(x)$ unit atau $h(x)$ unit di $F[x]$. Suatu polinomial $f(x)$ disebut *reducible* di $F[x]$ jika $f(x)$ tidak *irreducible* di $F[x]$.

Contoh 7.13:

$f(x) = x^3 - 3$ tidak tereduksi di $R[x]$, karena $x^3 - 3$ tidak dapat dinyatakan sebagai perkalian dua polinom $g(x)$, $h(x) \in \mathrm{R}[x]$ dengan derajat $(g, h) <$ derajat (f).

Contoh 7.14:

$f(x) = x^2 - 3$ tereduksi di $R[x]$, karena $x^2 - 3$ dapat dinyatakan sebagai perkalian dua polinom $g(x)$, $h(x) \in R[x]$ dengan derajat $(g, h) <$ derajat (f), sehingga $x^2 - 3 = \left(x+\sqrt{3}\right)\left(x-\sqrt{3}\right)$

Contoh 7.15:

Tunjukkan bahwa polinom $p(x) = x^2 + x + 2$ tidak tereduksi atas Z_3.

Penyelesaian:

$Z_3 = \{0, 1, 2\}$, maka diperoleh:
$p(0) = 0^2 + 0 + 2 = 2$
$p(1) = 1^2 + 1 + 2 = 1$
$p(2) = 2^2 + 2 + 2 = 2$
Karena tidak terdapat $x \in Z_3$, sehingga $p(x) = 0$. Jadi, $p(x)$ tidak tereduksi atas Z_3.

Contoh 7.16:

Tentukan bahwa polinom $p(x) = x^2 + x + 1$ tereduksi atas Z_3.

Penyelesaian:

$Z_3 = \{0, 1, 2\}$, maka diperoleh:
$p(0) = 0^2 + 0 + 1 = 1$
$p(1) = 1^2 + 1 + 1 = 0$
$p(2) = 2^2 + 2 + 1 = 1$
Karena terdapat $x \in Z_3$, sehingga $p(1) = 0$. Jadi, $p(x)$ tereduksi atas Z_3.

Contoh 7.17:

a) Polinomial $h(x) = x^2 - 1$ *reducible* atas Z karena ada elemen Z yang merupakan akar dari $h(x)$ sehingga $h(x) = x^2 - 1 = (x + 1)(x - 1)$.
b) Polinomial $s(x) = 4x^2 - 1$ *irreducible* atas Z karena tidak ada elemen Z yang merupakan akar dari $s(x)$.
c) Polinomial $p(x) = x^2 - 4$ *reducible* atas Q karena terdapat $2 \in Q$ sehingga $p(2) = 0$.
d) Polinomial $q(x) = x^2 - 2$ merupakan polinomial *irreducible* atas Q karena tidak ada elemen Q yang merupakan akar dari $q(x)$.
e) Polinomial $p(x) = x^2 - 4$ *reducible* atas R karena mempunyai akar dalam R sehingga $p(x) = x^2 - 4 = (x + 2)(x - 2)$.
f) Polinomial $q(x) = x^2 - 2$ *reducible* atas R karena mempunyai akar dalam R sehingga $p(x) = x^2 - 2 = \left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)$.

Teorema 7.5

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:

Pembuktian ini menggunakan prinsip induksi pada derajat dari $p(x)$.

Polinomial berderajat 0 merupakan konstan tidak nol a, $x^0 = a$ dan jelas bahwa mempunyai akar 0. 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 $n - 1$.

Andaikan induksinya adalah bahwa $q(s)$ dan sebarang polinomial derajat $n - 1$ yang lain mempunyai paling banyak $n-1$ akar.

Misalkan $t_2, t_3, \ldots, t_k$ dengan $k \le n$ (t_1 mungkin termasuk dalam akar yang sama).

Berarti $q(x)$ mempunyai faktorisasi

$$q(x) = (x - t_2)(x - t_3) \ldots (x - t_k)\, g(x)$$

Dalam hal ini $g(x)$ mempunyai derajat $n - k$ yang tidak mempunyai akar dalam D. Akibatnya, $p(x) = (x - t_1)\, q(x) = (x - t_1)\,(x - t_2)\,(x - t_3) \ldots (x - t_k)\, g(x)$.

Misalkan s sebarang elemen dalam D yang berbeda dari $t_1, t_2, \ldots, t_k$, diperoleh:

$$p(s) = (s - t_1)(s - t_2)\,(s - t_3) \ldots (s - t_k)\, g(s)$$

Terlihat bahwa $p(s)$ merupakan perkalian dari $k + 1$ anggota tidak nol dalam suatu daerah integral, sehingga $p(s)$ tidak nol.

Hal itu berarti $p(x)$ paling banyak mempunyai k akar $t_1, t_2, \ldots, t_k$ dengan $k \le n$.

Contoh 7.18:

Akan dicari faktorisasi dari polinomial:

$$f(x) = 2x^4 + x^3 + 3x^2 + 2x + 4$$

Atas *field* .

Penyelesaian:

Terlebih dahulu kita akan menentukan akar-akar dari $f(x)$ dalam Z_5.

$Z_5 = \{0, 1, 2, 3, 4\}$

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. Oleh karena itu:

$$(2x^4 + x^3 + 3x^2 + 2x + 4) \div (x - 2) = (2x^3 + 3x + 3)$$

sehingga:

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

dengan $g(x) = 2x^3+3x+3$. Selanjutnya, $g(0)=3$, $g(1)=3$, dan $g(2)=0$, maka 2 adalah akar dari $g(x)$ dalam Z_5. Oleh karena itu:

$$(2x^3+3x+3) \div (x-2) = (2x^2+4x+1)$$

Sehingga:

$$g(x) = (x-2)(2x^2+4x+1)$$

Dalam hali ini, $h(x) = 2x^2+4x+1$ tidak tereduksi (*irreducible*) karena $h(0)=1$, $h(1)=2$, $h(3)=1$, $h(4)=4$. Akibatnya, $f(x)$ dapat difaktorkan menjadi:

$$\begin{aligned} f(x) &= 2x^4+x^3+3x^2+2x+4 \\ &= (x-2)^2\,(2x^2+4x+1) \end{aligned}$$

RANGKUMAN

1. Bentuk umum dari suatu polinomial (suku banyak) adalah:

$$p(x) = a_0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n = \sum_{i=0}^{n} a_ix_i$$

   Dimana a_i adalah koefisien dari $p(x)$. Bila $x^n \neq 0$ maka derajat $p(x)$ adalah n dan bila $n=0$ maka derajat $p(x)$ adalah nol.
2. Misalkan dua buah polinom $p(x) = a^0 + a_1\, x^1 + a_2\, x^2 + \ldots + a_n\, x^n$ dan $q(x) = b_0 + b_1\, x^1 + b_2\, x^2 + \ldots + b_m\, x^m$ dikatakan sama jika dan hanya jika $a_i = b_i$ untuk semua $i \geq 0$.
3. Misalkan dua buah polonomial $p(x) = a_0 + a_1\, x^1 + a_2\, x^2 + \ldots + a_n\, x^n$ dan $q(x) = b_0 + b_1\, x^1 + b_2\, x^2 + \ldots + b_m\, x^m$, maka hasil penjumlahan dua polinomial yaitu: $p(x) + q(x) = c_0 + c_1\, x^1 + c_2\, x^2 + \ldots + c_k\, x^k$ dimana $k = \text{maks}\{n, m\}$ untuk setiap i, $c_i = a_i + b_i$, untuk $0 \leq i \leq k$.
4. Misalkan dua buah polinomial $p(x) = a_0 + a_1\, x^1 + a_2\, x^2 + \ldots + a_n\, x^n$ dan $q(x) = b_0 + b_1\, x^1 + b_2\, x^2 + \ldots + b_m\, x^m$, maka hasil perkalian dua buah polinomial yaitu: $p(x) \cdot q(x) = c_0 + c_1\, x^1 + c_2\, x^2 + \ldots + c_k\, x^k$ dimana $k = n+m$ untuk setiap i, $c_i = a_i\, b_0 + a_{i-1}\, b_1 + \ldots + a_1\, b_{i-1} + a_0\, b_i$.
5. Misalkan R adalah suatu Ring Komutatif. $R[x]$ dikatakan sebagai Ring Polinomial atas R dengan $R[x] = \{p(x),\ q(x),\ r(x),\ \ldots\}$ untuk $p(x) = \sum_{i=0}^{n} a_ix_i$ dan $q(x) = \sum_{i=0}^{n} bx_i$, ... dan $a_i \in R$
6. Jika R suatu daerah integral, dan $p(x)$, $q(x) \in R[x]$ dengan masing-masing $p(x)$ dan $q(x)$ bukan polinomial nol, maka:

$$\deg(p(x)\cdot q(x)) = \deg p(x) + \deg q(x)$$

Jika polinomial $R[x]$ bukan daerah integral, derajat dari hasil suatu perkalian polinomial bisa lebih kecil dari derajat hasil penjumlahan polinomial tersebut.

7. Misalkan $f(x)$ dan $g(x)$ adalah dua buah polinom, dengan $f(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ dan $g(x) = b_0 + b_1 x^1 + b_2 x^2 + \dots + b_m x^m$ dimana $f(x)$, $g(x) \in R[x]$ dan $g(x) \neq 0$, maka terdapat polinom-polinom yang unik $q(x)$, $r(x) \in R[x]$ sedemikian sehingga:

$$f(x) = q(x)\cdot g(x) + r(x)$$

dengan $r(x) = 0$ atau derajat $r(x) <$ derajat $g(x)$.

Polinom-polinom $q(x)$ dan $r(x)$ ditentukan secara tunggal oleh $f(x)$ dan $g(x)$ yang diperlukan. Selanjutnya $f(x)$ disebut polinom yang dibagi, $g(x)$ disebut polinom pembagi, $q(x)$ disebut hasil bagi (*quosient*) polinom, dan $r(x)$ disebut sisa hasil bagi (reminder) polinom.

8. Suatu polinom tak konstan $f(x) \in R[x]$ dinamakan polinom tidak tereduksi (*irreducible*) atas F apabila $f(x)$ tidak dapat dinyatakan sebagai hasil kali dua polinom $g(x)$ dan $h(x)$ di $R[x]$ dengan derajat $g(x)$ dan derajat $h(x)$ kurang dari derajat $f(x)$. Sebaliknya, apabila terdapat $g(x)$ dan $h(x)$ di $R[x]$ sehingga $f(x) = g(x)\ h(x)$ dengan derajat $g(x)$ dan derajat $h(x)$ kurang dari derajat $f(x)$ maka $f(x)$ dinamakan polinom tereduksi (*reducible*).

9. Polinomial $f(x)$ jika dibagi oleh $(x - a)$ dalam polinomial $F[x]$ maka sisanya adalah $f(a)$

10. Polinomial $(x - a)$ adalah faktor dari $f(x)$ dalam polinomial $F[x]$ jika dan hanya jika $f(a) = 0$. Suatu elemen $a \in F[x]$ dikatakan akar dari polinomial $f(a) = 0$. Sehingga berdasarkan teorema faktor tersebut, $(x\text{-}a)$ adalah faktor dari $f(x)$ jika dan hanya jika $f(a) = 0$. Suatu polinomial $f(x) \neq 0$ dan $f(x)$ bukan unit, $f(x)$ disebut *irreducible* di $F[x]$ jika:

$$f(x) = g(x)\cdot h(x)$$

Sehingga $g(x)$ unit atau $h(x)$ unit di $F[x]$. Suatu polinomial $f(x)$ disebut *reducible* di $F[x]$ jika $f(x)$ tidak *irreducible* di $F[x]$.

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.

LATIHAN

1. Diketahui polinom-polinom $f(x) = 2x^4 + 3x^3 + x + 1$ dan $g(x) = x^2 + 2$. Carilah:
   a. $f(x) + g(x)$
   b. $f(x) - g(x)$
   c. $f(x) \cdot g(x)$
2. Diketahui polinom-polinom $f(x) = 2x^4 + 3x^3 + x + 1$ dan $g(x) = x^2 + 2$. Carilah:
   a. $f(x) + g(x)$ dalam $Z_5\,[x]$
   b. $f(x) - g(x)$ dalam $Z_5\,[x]$
   c. $f(x) \cdot g(x)$ dalam $Z_5\,[x]$
3. Diketahui polinom-polinom $f(x) = x^7 + x^6 + x^5 + x^4 + x + 1$ dan $g(x) = x^3 + x + 1$. Carilah:
   a. $f(x) + g(x)$ dalam $Z_2\,[x]$
   b. $f(x) - g(x)$ dalam $Z_2\,[x]$
   c. $f(x) \cdot g(x)$ dalam $Z_2\,[x]$
4. Tentukan hasil bagi dan sisa dari polinom-polinom berikut terhadap $Z_5\,[x]$, dimana $p(x) = 2x^4 + 3x^3 + x + 1$ dan $q(x) = x^2 + 2$, $p(x)$ adalah polinom yang dibagi dan $g(x)$ polinom pembagi.
5. Tentukan hasil bagi dan sisa dari polinom-polinom berikut terhadap $Z_2\,[x]$, dimana $p(x) = x^7 + x^6 + x^5 + x^4 + x + 1$ dan $q(x) = x^3 + x + 1$, $p(x)$ adalah polinom yang dibagi dan $g(x)$ polinom pembagi.
6. Tentukan apakah polinom-polinom berikut tereduksi atau tidak tereduksi:
   a. $p(x) = 5x^8 + 2x^6 + x^5 + 4x^3 + 3x + 5$ di $Z_6\,[x]$
   b. $p(x) = x^7 + 3x^5 + 2x^2 - 3$ di $Z_{10}\,[x]$
7. Tentukan semua akar-akar dari polinomial $f(x) = x^3 - x$ di dalam Z_8.
8. Apakah polinomial $f(x) = x^3 + 2x + 1$ dalam $Z_3\,[x]$ *irreducible* atas Z_3?
9. 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 $b(x) = 2x + 3$ dan koefisien-koefisien polinomial dalam Z_6.
10. Tentukan semua polinomial derajat 2 yang *irreducible* atas Z_4.

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$\textit{Tingkat penguasaan} = \frac{\textit{Banyak jawaban yang benar}}{\textit{Banyak soal}} \times 100\%$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai di bawah ini:

Rentang Nilai (%)	Kategori
90 – 100	Sangat Baik
80 – 89	Baik
70 – 79	Sedang
≤ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi ≥ 70%, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang < 70%, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

BAB 8

RING FAKTOR DARI RING POLINOMIAL

Tujuan Instruksional Umum:

Setelah mempelajari materi pada bab ini, diharapkan mahasiswa dapat mengetahui dan mengaplikasikan teorema-teorema dasar terkait ring faktor (*quotient ring*) dari sebuah ring polinomial.

Tujuan Instruksional Khusus:

Setelah diberikan penjelasan mengenai teorema-teorema dasar terkait ring faktor (*quotient ring*) dari sebuah ring polinomial, maka mahasiswa diharapkan dapat:

a. Mengaplikasikan teorema-teorema dasar terkait ring faktor (*quotient ring*) dari sebuah ring polinomial.
b. Mengaplikasikan teorema fundamental dari homomorfisma ring.
c. Menentukan sifat-sifat suatu ring faktor dari ring polinomial.
d. Menentukan banyaknya elemen suatu ring faktor dari ring polinomial.
e. Menentukan operasi hitung suatu ring faktor dari ring polinomial.
f. Menentukan invers dari *field* suatu ring polinomial.

Deskripsi Singkat:

Dalam bab ini akan dibahas tentang teorema-teorema dasar terkait ring faktor (*quotient ring*) dari sebuah ring polinomial, teorema fundamental dari homomorfisma ring, sifat-sifat suatu ring faktor dari ring polinomial, cara menentukan banyaknya elemen suatu ring faktor dari ring polinomial, cara menentukan operasi hitung suatu ring faktor dari ring polinomial, dan cara menentukan invers dari *field* suatu ring polinomial.

8.1 RING FAKTOR DARI RING POLINOMIAL

Teorema 8.1

Jika F merupakan lapangan (*field*), maka setiap ideal dalam $F[x]$ merupakan ideal utama (*ideal principal*).

Bukti:

Misal N ideal dalam $F[x]$.

1) Jika N ideal trivial $\{0\}$, maka $N=(0)$
2) Jika N mengandung suatu polinomial konstan c, maka terdapat c^{-1} dalam F sehingga $c^{-1}c=1$ berada dalam N (karena N ideal). Akibatnya N mengandung setiap polinomial yang memiliki kelipatan 1, sehingga $N=F=(1)$.
3) Misal N non trivial dan tidak mengandung konstanta yang tak nol. Akibatnya N mengandung paling sedikit polinimial berderajat positif. Misal $b(x)$ polinomial berderajat terkecil dalam ideal N. Ideal N mengandung ideal $(b(x))$.
   Akan dibuktikan bahwa $(b(x))$ tunggal mengandung N.
   Misal $a(x)$ dan $b(x)$ dalam $F[x]$, maka terdapat $q(x)$ 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 N, maka dengan mengingat N ideal diperoleh $b(x)\ q(x)$ dalam N sehingga $r(x)$ dalam N.
   Karena $b(x)$ merupakan polinomial berderajat terkecil dalam N, maka $r(x)$ harus merupakan polinomial konstan dan dengan mengingat asumsi bahawa N 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 N termuat dalam $(b(x))$.

Contoh 8.1:

Diketahui ring $R[x]$ dan ideal

$$(x^2+1)=\left\{f(x)(x^2+1) \mid f(x)\,\text{dalam}\ R[x]\right\}$$

Penyelesaian:

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 unsur kesatuan 1 x^0. Karena (x^2+1) tidak mempunyai akar real, maka (x^2+1) *irreducible* dalam $R[x]$ sehingga (x^2+1) tidak mempunyai faktor dengan derajat satu.

Misalkan N sembarang ideal dalam $R[x]$ yang memuat (x^2+1) secara sejati. Dengan mengingat teorema, maka $N=(p(x))$ untuk suatu $p(x)$. Karena (x^2+1) dalam N, maka $(x^2+1)=p(x)\ q(x)$ untuk suatu $q(x)$ dalam $R[x]$. Karena (x^2+1) *irreducible* dalam $R[x]$, maka $p(x)$ atau $q(x)$ suatu konstan. Jika $q(x)$ konstan, maka $N=(x^2+1)$ sehingga hal ini kontradiksi dengan kenyataan bahwa N mengandung (x^2+1) secara sejati. Akibatnya, $p(x)$ merupakan suatu polinomial konstan dan tidak nol karena N mengandung (x^2+1) secara sejati. Dengan melihat teorema 8.1 bagian ke-2 diperoleh $J=R[x]$. Sehingga diperoleh $R[x]/(x^2+1)$ *field*. Karena $R[x]/(x^2+1)$ *field*, maka juga merupakan daerah integral.

Teorema 8.2

Jika F *field* dan polinomial $p(x)$ *irreducible* dalam $F[x]$, maka ring faktor (*quotient ring*) $F[x]/(p(x))$ merupakan *field*.

Teorema 8.3 (Teorema fundamental dari homomorfisma ring)

Jika diketahui f : R→R' homomorfisma ring dengan peta $f(R)$ dan inti K, maka ring faktor R/K isomorfisma dengan $f(R)$.

Bukti:

Karena inti K dari homomorfisma ring ideal, maka ring faktor R/N terdefinisikan.

Karena K juga inti dari homomorfisma grup $f: \langle R,+\rangle \to \langle R',+\rangle$, maka dengan mendefinisikan pemetaan diperoleh:

$$g: R/K \to f(R)$$

Dengan $g(r+N)=f(r)$, diperoleh:

$$\begin{aligned} g((r+N)\ (r'+N)) &= g(rr'+N) \\ &= f(rr') \\ &= f(r)\ f(r') \\ &= g(r+N)g(r'+N) \end{aligned}$$

Sehingga terbukti g merupakan isomorfisma ring.

Contoh 8.2:

Himpunan bilangan rasional Q adalah lapangan (*field*) dan polinomial

$q(x) = x^2 - 2$ *irreducible* atas Q, maka ring faktor $Q[x]/(x^2 - 2)$ merupakan *field*. *Field* tersebut akan isomorfis dengan:

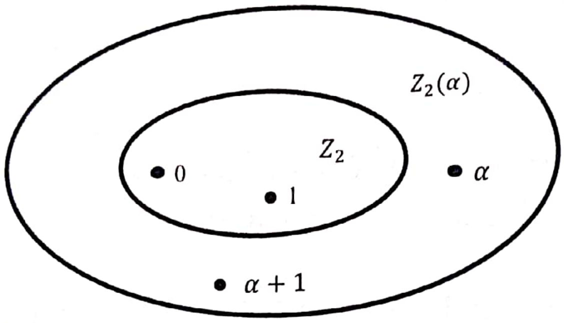
$$Q\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} \mid a, b \in Q\right\}$$

Contoh 8.3:

Himpunan bilangan bulat Z_2 merupakan *field* dan polinomi $q(x) = x^2 + x + 1$ *irreducible* atas Z_2 sehingga ring faktor $Z_2[x]/(x^2 + x + 1)$ 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. Hubungan antara Z_2 dengan $Z_2(\alpha)$ sebagai berikut:



GAMBAR 8.1. Hubungan antara Z_2 dan $Z_2(\alpha)$

Contoh 8.4:

Misalkan diketahui polinomial monik *irreducible* $p(x) = x^2 + 2x + 2$ 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* tersebut.

Bukti:

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 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:

TABEL 8.1. Tabel Penjumlahan dalam $Z_3[x]/(p(x))$

+	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
0	0	1	2	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$
1	1	2	0	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α
2	2	0	1	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$
α	α	$\alpha+1$	$\alpha+2$	2α	$2\alpha+1$	$2\alpha+2$	0	1	2
$\alpha+1$	$\alpha+1$	$\alpha+2$	α	$2\alpha+1$	$2\alpha+2$	2α	1	2	0
$\alpha+2$	$\alpha+2$	α	$\alpha+1$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1
2α	2α	$2\alpha+1$	$2\alpha+2$	0	1	2	α	$\alpha+1$	$\alpha+2$
$2\alpha+1$	$2\alpha+1$	$2\alpha+2$	2α	1	2	0	$\alpha+1$	$\alpha+2$	α
$2\alpha+2$	$2\alpha+2$	2α	$2\alpha+1$	2	0	1	$\alpha+2$	α	$\alpha+1$

Untuk memperoleh hasil dari tabel perkalian, perlu diperhatikan 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 contoh:

$$\begin{aligned}(2\alpha+1)(\alpha+2) &= 2\alpha^2+2\alpha+2\\ &= 2(\alpha+1)+2\alpha+2\\ &= 2\alpha+2+2\alpha+2\\ &= \alpha+1\end{aligned}$$

Tabel perkalian dalam $Z_3[x]/(p(x))$ dapat dinyatakan sebagai berikut:

TABEL 8.2. Tabel Perkalian dalam $Z_3[x]/(p(x))$

	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 8.5:

Misalkan diketahui polinomial *reducible* $p(x)=x^2+1$ atas *field* Z_2.

Penyelesaian:

Akan ditentukan semua elemen dari ring faktor $Z_2\ [x]/(p(x))$ dan pada saat yang sama juga akan dikonstruksikan tabel penjumlahan dan perkalian dari ring faktor 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 $Z_2\ [x]/(p(x))$ sebagai berikut:

TABEL 8.3. Tabel Operasi Penjumlahan dalam Z_2 [x]/(p(x))

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

Untuk membuat tabel operasi perkalian $Z_2\ [x]/(p(x))$ dengan memperhatikan bahwa $p(\alpha)=0$ atau:

$$\begin{aligned}\alpha^2+1 &= 0\\ \alpha^2 &= -1\\ &= 1\end{aligned}$$

Sehingga diperoleh tabel perkalian sebagai berikut:

Tabel 8.4. Tabel Operasi Perkalian dalam Z_2 [x]/(p(x))

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

Dengan demikian terbukti bahwa $Z_2\ [x]/(p(x))$ bukan merupakan *field* tetapi hanya merupakan ring komutatif dengan elemen satuan.

Contoh 8.6:

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 relatif prima atas $Z_5\ (x)$ sehingga $s(x)$ dan $t(x)$, menjadi:

$$f(x)s(x)+p(x)t(x)=1$$

Karena $p(\alpha)=0$, maka $f(\alpha)s(\alpha)=1$ sehingga:

$$(\alpha^2+3\alpha+1)^{-1}=(f(\alpha))^{-1}=s(\alpha)$$

Dalam upaya mencari $s(x)$ dan $t(x)$ dapat digunakan algoritma Euclid berikut:

$$\begin{aligned} p(x) &= f(x)(x+4)+x+3 \\ f(x) &= (x+3)x+1 \\ 1 &= f(x)-x(x+3) \\ 1 &= f(x)-x(p(x)-f(x)(x+4)) \\ 1 &= f(x)(1+x(x+4))+p(x)(-x) \end{aligned}$$

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 $Z_5(\alpha)$.

8.2 PERHITUNGAN DALAM RING FAKTOR

Jika F adalah *field*, bentuk ring faktor dari polinomial ring $F[x]$ adalah kelas yang penting dari ring yang akan digunakan untuk mengkonstruksi *field* baru. Misalkan $F[x]$ adalah ring dengan ideal principal, sehingga setiap ring faktor dari $F[x]/(p(x))$, untuk beberapa polinomial $p(x)\in F[x]$. Sekarang kita lihat pada struktur ring faktor. Elemen dari ring $F[x]/(p(x))$ adalah kelas yang ekuivalen pada hubungan $F[x]$, didefinisikan dengan:

$$f(x) \equiv g(x)\ mod(p(x)) \text{ jika dan hanya jika } f(x)-g(x)\in(p(x)).$$

Lemma 8.1

$f(x)\equiv g(x)\ mod(p(x))$ jika dan hanya jika $f(x)$ dan $g(x)$ memiliki sisa yang sama ketika dibagi dengan $p(x)$.

Bukti:

Misalkan $f(x)=q(x)\cdot p(x)+r(x)$ dan $g(x)=s(x)\cdot p(x)+t(x)$, dimana $r(x)$ dan $t(x)$ adalah nol atau memiliki derajat yang lebih kecil dari $p(x)$. Sekarang, perhatikan lemma karena pernyataan ini menunjukkan ekuivalen, yaitu:

(i) $f(x)\equiv g(x)\ mod(p(x))$

(ii) $f(x) - g(x) \in (p(x))$
(iii) $p(x) | f(x) - g(x)$
(iv) $p(x) | [\{q(x) - s(x)\} \cdot p(x) + (r(x) - t(x))]$
(v) $p(x) | [r(x) - t(x)]$
(vi) $r(x) = t(x)$

Oleh karena itu, setiap koset dari $F[x]$ dengan $(p(x))$ mengandung polinomial nol atau polinomial dari derajat yang lebih kecil dari $p(x)$.

Teorema 8.4

Jika F adalah *field*, misalkan P adalah ideal $(p(x))$ dalam $F[x]$ yang dinyatakan dengan polinomial $p(x)$ dari derajat $n > 0$. Elemen yang berbeda dari $F[x]/(p(x))$ adalah:

$$P + a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} \text{ di mana } a_0, a_1, \ldots, a_{n-1} \in F$$

Bukti:

Misalkan $P + f(x)$ menjadi setiap elemen dari $F[x]/(p(x))$ dan misalkan $r(x)$ adalah sisa ketika $f(x)$ dibagi dengan $p(x)$. Berdasarkan lemma di atas, $P + f(x) = P + r(x)$, adalah bentuk yang disarankan.

Perhatikan bahwa $P + r(x) = P + t(x)$ dimana $r(x)$ dan $t(x)$ adalah nol atau memiliki derajat yang kurang dari n. Maka,

$$r(x) \equiv t(x) mod (p(x))$$

Sehingga, berdasarkan lemma di atas, maka $r(x) = t(x)$.

Contoh 8.7:

Buatlah tabel Cayley penjumlahan dan perkalian dari $Z_2[x]/(x^2 + x + 1)$.

Penyelesaian:

Misalkan $P = (x^2 + x + 1)$, sehingga:

$$\begin{aligned} Z_2[x]/(x^2+x+1) &= \{P + a_0 + a_1 x \mid a_0, a_1 \in Z_2\} \\ &= \{P, P+1, P+x, P+x+1\} \end{aligned}$$

Tabel penjumlahan dapat dihitung dengan mudah. Sedangkan perkalian, perhatikan cara berikut:

$$\begin{aligned} (P+x)^2 &= P + x^2 \\ &= P + (x^2 + x + 1) + (x + 1) \\ &= P + x + 1 \end{aligned}$$

dan

$$
\begin{aligned}
(P+x)(P+x+1) &= P+x^2+x \\
&= P+(x^2+x+1)+1 \\
&= P+1
\end{aligned}
$$

TABEL 8.5. Tabel Operasi Penjumlahan dalam Ring $Z_2[x]/(x^2+x+1)$

$+$	P	$P+1$	$P+x$	$P+x+1$
P	P	$P+1$	$P+x$	$P+x+1$
$P+1$	$P+1$	P	$P+x+1$	$P+x$
$P+x$	$P+x$	$P+x+1$	P	$P+1$
$P+x+1$	$P+x+1$	$P+x$	$P+1$	P

TABEL 8.6. Tabel Operasi Perkalian dalam Ring $Z_2[x]/(x^2+x+1)$

$\bullet$	P	$P+1$	$P+x$	$P+x+1$
P	P	P	P	P
$P+1$	P	$P+1$	$P+x$	$P+x+1$
$P+x$	P	$P+x$	$P+x+1$	$P+1$
$P+x+1$	P	$P+x+1$	$P+1$	$P+x$

Ini adalah cara yang mudah untuk menemukan sisa dari $f(x)$ ketika dibagi dengan $p(x)$ daripada dengan mencoba pembagian algoritma secara langsung. Jika derajat $p(x)=n$ dan $P=(p(x))$, permasalahan dari menemukan sisa reduksi ke permasalahan menemukan sebuah polinomial $r(x)$ dari derajat yang kurang dari n sehingga $f(x)\equiv r(x) \mod P$. Hal ini sering dipecahkan dengan memanipulasi kongruen, menggunakan fakta bahwa $p(x)\equiv 0 \mod P$.

Pada kasus ini,

$P=(x^2+x+1)$, jadi $x^2+x+1\equiv 0 \mod P$ dan $x^2\equiv x+1 \mod P$. (Ingat, $+1=-1$ dalam Z_2). Oleh karena itu, dalam perkalian dua elemen dalam $Z_2[x]/P$, kita selalu dapat mengganti x^2 dengan $x+1$.

Sebagai contoh:

$P+x^2=P+x+1$ dan $P+x(x+1)=P+x^2+x=P+1$.

Contoh 8.8:

Misalkan $P=x^2-2$ adalah ideal principal dari $Q[x]$ dinyatakan dengan x^2-2. Temukan penjumlahan dan perkalian dari $P+3x+4$ dan $P+5x-6$ dalam ring $Q[x]/(x^2-2)=\{P+a_0+a_1x \mid a_0, a_1\in Q\}$.

Bukti:

$(P+3x+4)+(P+5x-6)=P+(3x+4)+(5x-6)=P+8x-2.$

$(P+3x+4)(P+5x-6)=P+(3x+4)(5x-6)=P+15x^2+2x-24.$

Berdasarkan pembagian logaritma, $15x^2\ 2x-24=15(x^2-2)+2x+6.$ Oleh karena itu, berdasarkan lemma di atas, $P+15x^2+2x-24=P+2x+6.$ Di mana P adalah ideal yang dinyatakan dengan $x^2-2.$

Maka, $x^2-2\equiv 0 \ mod\ P$ dan $x\hat{}2\equiv 2\ mod\ P$. Oleh karena itu, setiap kongruen modulo P, kita selalu dapat mengganti x^2 dengan 2. Sebagai contoh:

$$\begin{aligned} 15x^2+2x-24 &\equiv 15(2)+2x-24 \ mod\ P \\ &\equiv 2x+6 \ mod\ P \end{aligned}$$

Sehingga, $P+15x^2+2x-24=P+2x+6.$

Sekarang kita menjelaskan kapan sebuah faktor dari ring polinomial adalah *field*. Hasil ini menjelaskan kita untuk mengkonstruksikan banyak *field* yang baru.

Teorema 8.5

Misalkan a adalah elemen dari ring Euclidian R. Ring faktor $R/(a)$ adalah *field* jika dan hanya jika a tidak tereduksi di R.

Contoh 8.9:

$Z_p=Z/(p)$ adalah *field* jika dan hanya jika p adalah prima.

Teorema 8.6:

Ring $F[x]/(p(x))$ adalah sebuah *field* jika dan hanya jika $p(x)$ adalah *irreducible* pada *field* F. Lebih lanjut, ring $F[x]/(p(x))$ selalu mengandung sebuah subring yang isomorfik terhadap *field* F.

Bukti:

Misalkan $F=\{(p(x))+r|r\in F\}$. Ini dapat diverifikasi menjadi sebuah subring dari $F[x]/(p(x))$ yang isomorfik terhadap *field* F dengan isomorfisma yang membawa $r\in F$ ke $(p(x))+r\in F[x]/(p(x))$.

Contoh 8.10:

Tulis tabel perkalian untuk *field* $Z_3\ [x]/(x^2+1)$

Penyelesaian:

Jika $x=0, 1,$ atau 2 dalam Z_3, maka $x^2+1=1$ dan 2. Dengan teorema faktor, x^2+1 tidak memiliki faktor yang linier. Oleh karena itu, x^2+1 tidak tereduksi pada Z_3, dan ring faktor $Z_3[x]/(x^2+1)$ adalah sebuah *field*. Elemen-elemen dari *field* tersebut, dapat ditulis sebagai:

$$Z_3[x]/(x^2+1)=\{a_0+a_1x \mid a_0, a_1 \in Z_3\}$$

Dengan demikian, *field* mengandung Sembilan elemen, yaitu:

$$0, 1, 2, x, x+1, x+2, 2x, 2x+1, \text{ dan } 2x+2$$

Hal ini dapat dihitung dengan perkalian polinomial dalam $Z_3[x]$ dan mengganti x^2 dengan -1 atau 2, karena $x^2 \equiv -1 \equiv 2 \bmod (x^2+1)$.

TABEL 8.7. Tabel Perkalian dalam $Z_3[x]/(x^2+1)$

•	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

Contoh 8.11:

Tunjukkan bahwa $Q[x]/(x^3-5)=\{a_0+a_1x+a_2x^2 \mid a_i \in Q\}$ adalah *field* dan temukan invers dari elemen $x+1$.

Penyelesaian:

Dengan merasionalkan akar-akar, (x^3-5) tidak memiliki faktor linear, dan karenanya tidak tereduksi (*irreducible*) pada Q. Sehingga $Q[x]/(x^3-5)$ adalah sebuah *field*.

Jika $s(x)$ adalah invers dari $x+1$, maka $(x+1)\equiv 1 \bmod (x^3-5)$; bahwa $(x+1)s(x)+(x^3-5)\,t(x)=1$ untuk beberapa $t(x)\in Q[x]$.

Kita dapat menemukan polinomial $s(x)$ dan $t(x)$ dengan algoritma *Euclidean*, berikut:

$$\begin{array}{r|l}
 & x^2 - x + 1 \\ \hline
x+1 & x^3 + 0 + 0 - 5 \\
 & x^3 + x^2 \qquad - \\ \hline
 & \quad -x^2 \quad - 5 \\
 & \quad -x^2 - x \qquad - \\ \hline
 & \qquad\quad x - 5 \\
 & \qquad\quad x + 1 \quad - \\ \hline
 & \qquad\quad -6
\end{array}$$

Dengan demikian,
$x^3 - 5 = (x^2 - x + 1)(x + 1) - 6$
$6 \equiv (x^2 - x + 1)\ (x + 1) \ \ mod\ (x^3 - 5)$
sehingga: $1 \equiv 1/6\ (x^2 - x + 1)\ (x + 1) \ \ mod\ (x^3 - 5)$
dan
oleh karenanya, $(x+1)^{-1} = \frac{1}{6}x^2 - \frac{1}{6} + \frac{1}{6}$ dalam $Q[x]/(x^3 - 5)$

Contoh 8.12:

Tunjukkan bahwa $Z_3\ [x]/(x^3 + 2x + 1)$ adalah sebuah *field* dengan 27 elemen dan tentukan invers dari elemen x^2.

Penyelesaian:

Jika $x = 0$, 1, atau 2 dalam Z_3, maka $x^3 + 2x + 1 = 1$; karena itu $x^3 + 2x + 1$ tidak memiliki faktor linier dan *irreducible*. Oleh karena itu:

$$Z_3\ [x]/(x^3 + 2x + 1) = \{a_0 + a_1\ x + a_2\ x_2 | a_i \in Z_3\}$$

Adalah *field* yang mempunyai $3^3 = 27$ elemen.
Untuk menemukan invers dari x^2, kita mencoba algoritma Euclid ke $x^3 + 2x + 1$ dan x^2 dalam $Z_3\ [x]$.
dan invers dari x^2 dalam $Z_3\ [x]/(x^3 + 2x + 1)$ adalah $(2x^2 + 2x + 1)$

$$\begin{array}{r|l}
 & \qquad x \\ \hline
x^2 & x^3 + 2x + 1 \\
 & x^3 \qquad\qquad - \\ \hline
 & \qquad 2x + 1
\end{array}
\qquad\qquad
\begin{array}{r|l}
 & \qquad 2x + 2 \\ \hline
2x + 1 & x^2 \\
 & x^2 + 2x \qquad - \\ \hline
 & \qquad x \\
 & \qquad x + 2 \quad - \\ \hline
 & \qquad\quad 1
\end{array}$$

Kita mempunyai,

$x^3+2x+1=x(x^2)+(2x+1)$ dan $x^2=(2x+2)(2x+1)+1$.

Oleh karena itu,

$1=x^2-(2x+2)\{(x^3+2x+1)-x\cdot x^2\}$

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

Sehingga,

$1\equiv x^2(2x^2+2x+1)\ \ mod\ (x^3+2x+1)$

RANGKUMAN

1. Jika F *field*, maka setiap ideal dalam $F[x]$ merupakan ideal utama (*ideal principal*).
2. Jika F *field* dan polinomial $p(x)$ *irreducible* dalam $F[x]$, maka ring faktor (*quotient ring*) $F[x]/(p(x))$ merupakan *field*.
3. Jika diketahui $f: R\to R'$ homomorfisma ring dengan peta $f(R)$ dan inti K, maka ring faktor R/K isomorfisma dengan $f(R)$.
4. $f(x)\equiv g(x)mod(p(x))$ jika dan hanya jika $f(x)$ dan $g(x)$ memiliki sisa yang sama ketika dibagi dengan $p(x)$.
5. Jika F adalah *field*, misalkan P adalah ideal $(p(x))$ dalam $F[x]$ yang dinyatakan dengan polinomial $p(x)$ dari derajat $n>0$. Elemen yang berbeda dari $F[x]/(p(x))$ adalah:

   $P+a_0+a_1x+\ldots+a_{n-1}x^{n-1}$ di mana $a_0, a_1, \ldots, a_{n-1}\in F$
6. Misalkan a adalah elemen dari ring Euclidian R. Ring faktor $R/(a)$ adalah *field* jika dan hanya jika a tidak tereduksi di R.
7. Ring $F[x]/(p(x))$ adalah sebuah *field* jika dan hanya jika $p(x)$ adalah *irreducible* pada *field* F. Lebih lanjut, ring $F[x]/(p(x))$ selalu mengandung sebuah subring yang isomorfik terhadap *field* F.

LATIHAN

1. Berikan sifat-sifat dari ring faktor $Z_5[x]/(x^2+1)$. Berapa banyak elemen yang dimilikinya?
2. Misalkan diketahui polinomial $p(x)=2x^2+1$ atas *field* Z_3.
   a. Tunjukkan bahwa *irreducible* atas

b. Berikan sifat-sifat dari $Z_3/(2x^2+1)$

c. Tentukan semua elemen dari $Z_3/(2x^2+1)$.

3. Apakah $x^3+(x^2+1)$ dan $x+(x^2+1)$ merupakan elemen yang sama dalam ring faktor $R[x]/(x^2+1)$?

4. Hitunglah operasi dalam $Z_5\,[x]/(x^2+1)$ berikut ini:

a. $(x+(x^2+1))^2$

b. $(x+2+(x^2+1))(2x+1+(x^2+1))$

5. Hitunglah operasi dalam ring faktor $Z_{60}/(5)$ berikut ini:

a. $[43+(5)]+[7+(5)]$

b. $[-3+(5)]+[14+(5)]$

c. $[2+(5)]^5$

d. $[2+(5)]^{-1}$

Untuk soal nomor 6 sampai dengan 9, hitunglah penjumlahan dan perkalian dari elemen yang diberikan dalam ring faktor (*quotient rings*)

6. $3x+4$ dan $5x-2$ dalam $Q[x]/(x^2-7)$

7. x^2+3x+1 dan $-2x^2+4$ dalam $Q[x]/(x^3+2)$

8. x^2+1 dan $x+1$ dalam $Z_2\,[x]/(x^3+x+1)$

9. $ax+b$ dan $cx+d$ dalam $R[x]/(x^2+1)$ di mana $a, b, c, d \in R$

10. Buatlah tabel Cayley penjumlahan dan perkalian dari:

$$Z_3\,[x]/(x^2+2x+1)$$

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$\textit{Tingkat penguasaan} = \frac{\textit{Banyak jawaban yang benar}}{\textit{Banyak soal}} \times 100\%$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai di bawah ini:

Rentang Nilai (%)	Kategori
90 – 100	Sangat Baik

Rentang Nilai (%)	Kategori
80 – 89	Baik
70 – 79	Sedang
≤ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi $\geq 70\%$, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang $< 70\%$, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

BAB 9

LAPANGAN PERLUASAN (EXTENSION FIELD)

Tujuan Instruksional Umum:

Setelah mempelajari materi pada bab ini, maka diharapkan mahasiswa dapat mengaplikasikan teorema dari *extension field, splitting field, Zeros of an Irreducible Polynomial*, dan *perfect field*.

Tujuan Instruksional Khusus:

Setelah mahasiswa diberikan penjelasan terkait teorema-teorema dasar dari *extension field, splitting field, Zeros of an Irreducible Polynomial*, dan *perfect field*, maka diharapkan mahasiswa dapat:

a. Menjelaskan definisi dari *extension field, splitting field, zeros of an irreducible polynomial, perfect field*.
b. Mengaplikasikan dan membutikan teorema-teorema terkait lapangan perluasan (*extension field*).
c. Mengaplikasikan dan membutikan teorema-teorema terkait lapangan pemisah (*splitting field*).
d. Menentukan *splitting field* dari suatu polinomial.
e. Mengaplikasikan dan membutikan teorema-teorema terkait *zeros of an irreducible polynomial*.
f. Mengaplikasikan dan membutikan teorema-teorema dari lapangan sempurna (*perfect field*).

Deskripsi Singkat:

Dalam bab ini akan dibahas tentang definisi, teorema, maupun contoh terkait lapangan perluasan (*extension field*), lapangan pemisah (*splitting field*), nol dari sebuah polinomial tidak tereduksi (*Zeros of an Irreducible Polynomial*), dan lapangan sempurna (*perfect field*).

9.1 LAPANGAN PERLUASAN (EXTENSION FIELD)

Definisi 9.1

Sebuah field E dikatakan sebuah lapangan perluasan (extension field) dari field F, jika $F \subseteq E$, dimana operasi F adalah operasi E yang dibatasi pada F.

Teorema 9.1 (Teorema Kronecker)

Misal *F* adalah lapangan (*field*) dan $f(x)$ polinomial yang tidak konstan dalam $F[x]$, maka terdapat lapangan perluasan (*extension field*) *E* dari *F*, dimana $f(x)$ memiliki nol.

Bukti:

Karena $F[x]$ adalah daerah faktorisasi tunggal, $f(x)$ mempunyai faktor yang tidak dapat direduksi, misal $p(x)$. Jelas, itu sudah cukup membangun sebuah *field E* dari *F*, dimana $p(x)$ memiliki nol. Misal, untuk *E* adalah $F[x]/\langle p(x)\rangle$. Kita sudah mengetahui bahwa ini adalah sebuah *field*. Selain itu, karena pemetaan dari $\Phi : F \to E$ diberikan dengan $\Phi(a) = a + \langle p(x)\rangle$ adalah pemetaan satu-satu dengan kedua operasi, *E* mempunyai subfield yang isomorfik ke *F*. Kita mungkin menganggap *E* mengandung *F* jika teridentifikasi koset $a + \langle p(x)\rangle$ dengan perwakilan koset unik *a* yang dimiliki oleh *F*, anggap $a + \langle p(x)\rangle$ hanya sebagai *a* dan sebaliknya.

Terakhir, akan ditunjukkan bahwa $p(x)$ memiliki nol dalam *E*, ditulis:

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$$

Kemudian, dalam *E*, $x + \langle p(x)\rangle$ adalah nol dari $p(x)$, karena:

$$\begin{aligned}
p(x+\langle p(x)\rangle) &= a_n (x+\langle p(x)\rangle)^n + a_{n-1} (x+\langle p(x)\rangle)^{n-1} + \ldots + a_0 \\
&= a_n (x+\langle p(x)\rangle) + a_{n-1} (x+\langle p(x)\rangle) + \ldots + a_0 \\
&= a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 + \langle p(x)\rangle \\
&= p(x) + \langle p(x)\rangle \\
&= 0 + \langle p(x)\rangle
\end{aligned}$$

Contoh 9.1:

Misal $K = R$, $f(x) = x^2 + 1$, $f(x)$ tak tereduksi dalam *R*, maka $\langle x^2 + 1\rangle$ ideal maksimal dalam $R[x]$, jadi $R[x]/\langle x^2 + 1\rangle$ lapangan dengan:

$$\frac{R[x]}{x^2+1} = \left\{ g(x) + x^2 + 1 \mid g(x) \in R[x] \right\}$$

Ambil $\alpha = x + \langle x^2 + 1 \rangle$, maka $f(\alpha) = \left(x + x^2 + 1\right)^2 + 1 = 0 \in \dfrac{R[x]}{x^2 + 1}$

Elemen $\alpha \in F$ disebut elemen aljabar atas K jika $f(\alpha) = 0$, untuk suatu $0 \neq f(x) \in K[x]$, sebaliknya α bukan aljabar disebut transedental.

Contoh 9.2:

Misalkan $f(x) = x^2 + 1 \in Q[x]$. Maka, tunjukkan bahwa $f(x)$ adalah sebuah elemen dari $K[x] = (Q[x]/\langle x^2 + 1 \rangle)[x]$.

Penyelesaian:

Kita memiliki

$$\begin{aligned} f(x + \langle x^2 + 1 \rangle) &= (x + \langle x^2 + 1 \rangle)^2 + 1 \\ &= x^2 + \langle x^2 + 1 \rangle + 1 \\ &= x^2 + 1 + \langle x^2 + 1 \rangle \\ &= 0 + \langle x^2 + 1 \rangle \end{aligned}$$

Tentu saja, polinomial $x^2 + 1$ memiliki bilangan kompleks $\sqrt{-1}$ sebagai nol. Tetapi, hal yang ingin ditekankan di sini adalah kita telah membangun *field* yang berisi bilangan rasional dan nol untuk polinomial $x^2 + 1$ dengan hanya menggunakan bilangan rasional.

Contoh 9.3:

Misalkan $f(x) = x^5 + 2x^2 + 2x + 2 \in Z_3\,[x]$. Kemudian, faktorisasi yang tidak tereduksi dari $f(x)$ dalam Z_3 adalah $(x^2 + 1)(x^3 + 2x + 2)$. Jadi, carilah *extension field* K dari Z_3 dimana $f(x) = 0$, kita ambil $K = Z_3\,[x]/\langle x^2 + 1 \rangle$, sebuah *field* dengan 9 elemen, atau $K = Z_3\,[x]/\langle x^3 + 2x + 2 \rangle$, sebuah *field* dengan 27 elemen.

Karena setiap integral domain mengandung koefisien *field*. Kita melihat bahwa setiap polinomial yang tidak konstan dengan koefisien dari integral domain selalu nol di beberapa *field* yang mengandung koefisien ring. Contoh selanjutnya, menunjukkan bahwa tidak benar ring komutatif secara umum.

Contoh 9.4:

Misal $f(x) = 2x + 1 \in Z_4\,[x]$. Kemudian $f(x)$ tidak memiliki nol disetiap ring dari Z_4 sebagai subring, karena jika β bernilai nol seperti sebuah ring, maka:

$0 \quad = 2\beta + 1$, dan oleh karena itu

$$
\begin{aligned}
0 &= 2(2\beta + 1) \\
&= 2(2\beta) + 2 \\
&= (2 \cdot 2)\beta + 2 \\
&= 0 \cdot + 2 \\
&= 2
\end{aligned}
$$

Akan tetapi $0 \neq 2$ dalam Z_4.

Contoh 9.5:

Konstruksikan suatu *extension field* dari Q yang memiliki satu akar dari *irreducible polynomial* $p(x) = x^3 - 2$ dalam $Q[x]$.

Penyelesaian:

Berdasarkan teorema 9.1, maka diperoleh *field*

$$E = Q[x]/(x^3 - 2)$$

Mengandung Q dan berbentuk $\{a + (x^3 - 2) | a \text{ dalam } Q\}$ dan $s = x + (x^3 - 2)$ adalah akar dari $p(x)$.

Oleh karena itu merupakan isomorfis dengan *field* bagian dari $Q\left(\sqrt[3]{2}\right)$ dengan bentuk: $Q\left(\sqrt[3]{2}\right) = \left\{a + b\left(\sqrt[3]{2}\right) + c\left(\sqrt[3]{2}\right)^2 | a, b, c \text{ dalam } Q\right\}$

Teorema 9.2.

Jika $p(x)$ polinomial tidak tereduksi (*irreducible*) berderajat $n > 1$ pada F dan $\alpha = x + \langle p(x) \rangle$ dan $c + \langle p(x) \rangle$ dengan c berlaku untuk semua c dalam F, maka *extension field* $E = F[x]/\langle p(x) \rangle$ terdiri dari semua elemen berbentuk $c_{n-1} + \alpha^{n-1} + \ldots + c_1\ \alpha + c_0$ dengan semua c_j dalam F.

Bukti:

Untuk sembarang elemen $f(x) + \langle p(x) \rangle$ dari E, $f(x)$ dapat ditulis sebagai:

$$f(x) = p(x)q(x) + r(x)$$

Dengan derajat $\langle r(x) \rangle <$ derajat $\langle p(x) \rangle = n$.

Akibatnya,

$$
\begin{aligned}
f(x) + \langle p(x) \rangle &= [p(x)q(x) + r(x)] + \langle p(x) \rangle \\
&= r(x) + \langle p(x) \rangle
\end{aligned}
$$

karena

$$[p(x)q(x) + r(x)] \text{-} r(x) = p(x)q(x) \text{ dalam } \langle p(x) \rangle.$$

Polinomial $r(x)$ ditulis sebagai:

$$r(x) = c_{n-1}\,x^{n-1} + \ldots + c_1\,x + c_0$$

dan dapat dilihat bahwa elemen-elemen E mereduksi sehingga menghasilkan bentuk:

$$c_{n-1}\,x_{n-1} + \ldots + c_1\,x + c_0 + \langle p(x)\rangle$$

Karena $\alpha = x + \langle p(x)\rangle$ maka mudah dibuktikan bahwa:

$$c_{n-1}\,x^{n-1} + \ldots + c_1\,x + c_0 + \langle p(x)\rangle$$

Dapat ditulis sebagai $c_{n-1}\,\alpha^{n-1} + \ldots + c_1\,\alpha + c_0$ dengan c_i diidentifikasikan dengan $c_i + \langle p(x)\rangle$.

Selanjutnya, digunakan notasi $F(\alpha)$ dengan:

$$F(\alpha) = \{c_{n-1}\,\alpha^{n-1} + \ldots + c_1\,\alpha + c_0 | c_i \in F\}$$

Suatu *extension field* yang mengandung F dan suatu akar α dari $p(x)$. Misalkan, $F(\alpha)$ dinamakan simple *extension* dari F. Proses ini dapat berulang dalam bentuk:

$$(F(\alpha))(\beta) = F(\alpha,\beta)$$

yang dinamakan dengan perluasan berulang (iterated *extension*) dari F. Elemen s dinamakan aljabar atas F (algebraic) karena memenuhi:

$$\begin{aligned} &= s^4 + (s+1) + s^2 + 1 \\ &= s^4 + s^2 + s \\ &= s(s^3 + s + 1) \\ &= 0 \end{aligned}$$

Berarti s^2 adalah suatu akar dan dengan cara uji coba diperoleh juga $s^2 + s$ merupakan akar dari $p(x)$ yang lain.

Sehingga, semua akar s, s^2 dan $s^2 + s$ dari $p(x)$ berada pada E.

9.2 LAPANGAN PEMISAH (SPLITTING FIELD)

Definisi 9.2

Misalkan F adalah sebuah lapangan perlusan (*extension field*) dari F dan misalkan $f(x) \in F[x]$ dengan derajat sekurang-kurangnya 1. Kita katakan bahwa $f(x)$ terpisah (*splits*) di E jika ada elemen $a \in F$ dan a_1, a_2, …, $a_n \in E$ sedemikian sehingga:

$$f(x) = a(x - a_1)\,(x - a_2)\,\ldots\,(x - a_n)$$

Kita sebut E sebuah lapangan pemisah (*splitting field*) dari $f(x)$ pada F, jika:

$$E = F(a_1, a_2, \ldots, a_n)$$

Perhatikan bahwa *splitting field* dari sebuah polinomial terhadap *field* tidak hanya bergantung pada polinom, akan tetapi di *field* juga. Bahwasannya, *splitting field* dari $f(x)$ terhadap F hanyalah *field* ekstensi terkecil dari F di mana $f(x)$ terpisah.

Contoh selanjutnya menggambarkan bagaimana *spiltting field* dari polinom $f(x)$ terhadap F tergantung pada F.

Contoh 9.6:

Perhatikan polinomial $f(x) = x^2 + 1 \in Q[x]$.

Karena $x^2 + 1 = \left(x + \sqrt{-1}\right)\left(x - \sqrt{-1}\right)$, kita lihat bahwa $f(x)$ *splits* di C.
Akan tetapi *splitting field* terhadap Q adalah $Q(i) = \{r + si \mid r, s \in Q\}$. Sebuah *splitting field* untuk $x^2 + 1$ terhadap R adalah C.
Demikian juga untuk $x^2 - 2 \in Q[x]$ *splits* di R, akan tetapi sebuah spilitting *field* terhadap Q adalah $Q\left(\sqrt{2}\right) = \left\{r + s\sqrt{2} \mid r, s \in Q\right\}$.

Teorema 9.3

Misalkan F adalah sebuah *field* dan misalkan $f(x)$ adalah elemen tidak konstan dari $F[x]$. Maka, terdapat sebuah *splitting field E* untuk $f(x)$ terhadap F.

Bukti:

Kita proses dengan induksi pada derajat $f(x)$. Jika derajat $f(x) = 1$, maka $f(x)$ adalah linear. Sekarang, misalkan bahwa pernyataan benar untuk semua *field* dan semua polinomial dari derajat yang kurang dari $f(x)$. Berdasarkan teorema 9.1, terdapat sebuah perluasan E dari F dimana $f(x)$ memiliki nol, katakan a_1. Kemudian kita menuliskan $f(x) = (x - a_1)\, g(x)$, dimana $g(x) \in E[x]$. Karena derajat $g(x) <$ derajat $f(x)$, dengan induksi terdapat sebuah *field K* yang mengandung E dan semuanya bernilai nol dari $g(x)$, katakana: $a_2, \ldots, a_n$. Jelas terbukti bahwa *splitting field* dari $f(x)$ pada F adalah $F(a_1, a_2, \ldots, a_n)$.

Contoh 9.7:

Perhatikan $f(x) = x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$ terhadap Q. Jelas sekali, bahwa angka nol dari $f(x)$ dalam C adalah: $\pm\sqrt{2}$ dan $\pm\,i$. Jadi, sebuah *splitting field* untuk $f(x)$ terhdap Q adalah:

$$Q\left(\sqrt{2},i\right)=Q\left(\sqrt{2}\right)(i)=\left\{\alpha+\beta i \mid \alpha,\beta\in Q\left(\sqrt{2}\right)\right\}$$
$$=\left\{\left(a+b\sqrt{2}\right)+\left(c+d\sqrt{2}\right)i \mid a,b,c,d\in Q\right\}$$

Contoh 9.8:

Perhatikan $f(x)=x^2+x+2$ pada Z_3. Maka $Z_3(i)=\{a+bi \mid a, b\in Z_3\}$ adalah sebuah *splitting field* untuk $f(x)$ pada Z_3 karena:

$$f(x)=[x-(1+i)][x-(1-i)]$$

Pada waktu yang bersamaan, kita mengetahui dengan pembuktian Teorema Kronecker bahwa elemen $x+\langle x^2+x+2\rangle$ dari:

$$F=Z_3[x]/\langle x^2+x+2\rangle$$

adalah nol dari $f(x)$. Karena $f(x)$ mempunyai derajat 2, berdasarkan teorema faktor bahwa selain nol dari $f(x)$ harus juga dalam F. Jadi, $f(x)$ *splits* di F, dan karena F adalah ruang vector dua dimensi dalam Z_3, kita ketahui bahwa F juga sebuah *splitting field* dari $f(x)$ terhadap Z_3. Bagaimana kita memfaktorkan $f(x)$ dalam F? Pemfaktoran $f(x)$ dalam F cukup membingungkan karena kita menggunakan dua simbol x dengan dua cara yang berbeda. Cara pertama menggunakan urutan penulisan polinomial $f(x)$, dan cara yang kedua menggunakan koset representative dari elemen F. Di sini, kita menggunakan cara yang sederhana yaitu dengan mengidentifikasi koset, $1+\langle x^2+x+2\rangle$ dengan elemen 1 dalam Z_3 dan menunjukkan koset $x+\langle x^2+x+2\rangle$ oleh β. Dengan identifikasi ini, *field* $Z_3[x]/\langle x^2+x+2\rangle$ dapat direpresentasikan sebagai $\{0, 1, 2, \beta, 2\beta, \beta+1, 2\beta+1, \beta+2, 2\beta+2\}$. Elemen-elemen ini menggunakan operasi penjumlahan dan perkalian seperti polinomial, terkecuali kita menggunakan observasi bahwa $x^2+x+2+\langle x^2+x+2\rangle=0$ berarti bahwa $\beta^2+\beta+2=0$, sehingga $\beta^2=-\beta-2=2\beta+1$. Sebagai contoh:

$$(2\beta+1)(\beta+2)=2\beta^2+5\beta+2=2(2\beta+1)+5\beta+2=9\beta+4=1$$

Untuk mendapatkan faktorisasi dari $f(x)$ dalam F, kita menggunakan cara pembagian panjang sebagai berikut:

$$\begin{array}{r|l}
 & x+(\beta+1) \\
\hline
x-\beta & x^2+x+2 \\
 & \underline{x^2-\beta x \qquad\qquad -} \\
 & (\beta+1)x+2 \\
 & \underline{(\beta+1)x-(\beta+1)\beta \quad -} \\
 & (\beta+1)\beta+2=\beta^2+\beta+2=0
\end{array}$$

Jadi, $x^2+x+2=(x-\beta)(x+\beta+1)$. Kemudian, kita menemukan dua *splitting field* untuk x^2+x+2 pada Z_3, satu dari $F(a)$ dan satu yang lain dari $F[x]/\langle p(x)\rangle$ dimana $F=Z_3$ dan $p(x)=x^2+x+2$.

Teorema 9.4

Misalkan F adalah *field* dan misalkan $p(x)\in F[x]$ tidak tereduksi (*irreducible*) terhadap F. Jika a adalah bilangan nol dari $p(x)$ dalam beberapa perluasan E dari F, maka $F(a)$ adalah isomorfik pada $F[x]/\langle p(x)\rangle$. Lebih lanjut, jika derajat $p(x)=n$, maka setiap anggota dari $F(a)$ dapat ditulis dalam bentuk yang unik, yaitu:

$$c_{n-1}\,a^{n-1}+c_{n-2}\,a^{n-2})+\ldots+c_1\,a+c_0$$

di mana $c_0, c_1, \ldots, c_{n-1}\in F$.

Bukti:

Diserahkan kepada pembaca sebagai latihan.

Corollary 9.1 F(a) ≈ F(b)

Misalkan F adalah sebuah *field* dan misalkan $p(x)\in F[x]$ tidak tereduksi *irreducible* pada E. Jika a adalah nol dari $p(x)$ dalam beberapa perluasan E ke F dan b adalah nol dari $p(x)$ dalam beberapa perluasan E' ke F, maka *field* $F(a)$ dan $F(b)$ adalah isomorfik.

Contoh 9.9:

Perhatikan polinomial *irreducible* $f(x)=x^6-2$ pada Q. Karena $\sqrt[6]{2}$ adalah nol untuk $f(x)$, berdasarkan teorema di atas, bahwa himpunan $\{1,2^{1/6},2^{2/6},2^{3/6},2^{4/6},2^{5/6}\}$ adalah basis untuk $Q\left(\sqrt[6]{2}\right)$ pada Q. Sehingga,

$$Q\left(\sqrt[6]{2}\right)=\{a_0,a_1 2^{1/6},a_2 2^{2/6},a_3 2^{3/6},a_4 2^{4/6},a_5 2^{5/6}|a_i\in Q\}$$

Field ini adalah isomorfik ke $Q[x]/x^6-2$.

Lemma 9.1

Misalkan F adalah *field*, $p(x)\in F[x]$ *irreducible* pada F, dan misalkan a adalah bilangan nol dari $p(x)$ dalam beberapa perluasan dari F. Jika Φ adalah *field* yang isomorfisma dari F ke F dan b adalah bilangan nol dari $\Phi(p(x))$ dalam beberapa perluasan dari F, maka ada sebuah isomorfisma dari $F(a)$ ke $F(b)$ yang yang setuju dengan Φ pada F dan membawa a ke b.

Teorema 9.5:

Misalkan Φ isomorfisma dari sebuah *field* F ke *field* F' dan misalkan $f(x) \in F[x]$. Jika E adalah sebuah *splitting field* untuk $f(x)$ pada F dan E' adalah *splitting field* untuk $\Phi(f(x))$ pada F', maka ada sebuah isomorfisma dari E ke E' sepaham dengan Φ pada F.

Bukti:

Kita gunakan induksi pada derajat $f(x)$. Jika derajat $f(x)=1$, maka $E=F$ dan $E'=F'$, agar Φ ingin memetakan kepada dirinya sendiri. Jika derajat $f(x)>1$, dan misalkan $p(x)$ sebuah faktor yang tidak tereduksi pada pada $f(x)$, misalkan a adalah nol pada $p(x)$ dalam E, dan misalkan b adalah nol pada $\Phi(p(x))$ dalam E'. Berdasarkan lemma di atas, ada sebuah isomorfisma α dari $F(a)$ ke $F'(b)$ yang setuju dengan Φ pada F dan membawa a ke b. Sekarang, tulis $f(x)=(x\text{-}a)g(x)$, di mana $g(x) \in F(a)[x]$. Kemudian E adalah *splitting field* untuk $g(x)$ pada $F(a)$ dan E' adalah *splitting field* untuk $\alpha(g(x))$ pada $F'(b)$. Karena derajat $g(x) <$ derajat $f(x)$, ada sebuah isomorfisma dari E ke E' yang setuju dengan α pada $F(a)$ dan oleh karena itu dengan Φ pada F.

Corollary 9.2:

Misalkan F adalah *field* dan misalkan $f(x) \in F[x]$. Maka setiap dua *splitting field* dari $f(x)$ pada F adalah isomorfik.

Contoh 9.10:

Misalkan a adalah bilangan rasional positif dan misalkan ω adalah sebuah akar primitif satuan ke-n. Maka masing-masing

$$a^{1/n}, \omega a^{1/n}, \omega^2 a^{1/n}, \ldots, \omega^{n-1} a^{1/n}$$

adalah nol dari $x^n - a$ dalam $Q\left(\sqrt[n]{a}, \omega\right)$.

9.3 NOL DARI SEBUAH POLINOMIAL TIDAK TEREDUKSI (ZEROS OF AN IRREDUCIBLE POLYNOMIAL)

Kita mengetahui bahwa setiap polinomial yang tidak konstan pada sebuah pemisahan lapangan (*field splits*) dalam beberapa perluasan. Polinomial yang *irreducible* harus dipisahkan dengan beberapa cara yang khusus, disini kita menggunakan ilmu Kalkulus.

Definisi 9.3 Turunan (Derivative)

Misalkan $f(x) = a^n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ dari $F[x]$. Turunan (*derivative*) dari $f(x)$, dinotasikan dengan $f'(x)$ adalah polinomial:

$$na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + a_1 \text{ dalam } F[x]$$

Lemma 9.2

Misalkan $f(x)$ dan $g(x) \in F[x]$ dan misalkan $a \in F$, maka:

1) $(f(x) + g(x))' = f'(x) + g'(x)$
2) $(af(x))' = af'(x)$
3) $(f(x)g(x))' = f(x)g'(x) + g(x)f'(x)$

Teorema 9.6. (Kriteria untuk Perkalian Nol)

Sebuah polinomial $f(x)$ pada *field* F memiliki perkalian nol dalam beberapa perluasan E jika dan hanya jika $f(x)$ dan $f'(x)$ memiliki sebuah faktor persekutuan berderajat positif dalam $F[x]$.

Bukti:

Jika sebuah perkalian nol dari $f(x)$ dalam beberapa perluasan E, maka terdapat sebuah $g(x)$ dalam $E[x]$ sehingga $f(x) = (x - a)^2 g(x)$. Oleh karena itu, $f'(x) = (x - a)^2 g(x) + 2(x - a)g(x)$, kita perhatikan bahwa $f'(a) = 0$. Karena, $(x - a)$ adalah sebuah faktor dari $f(x)$ dan $f'(x)$ dalam perluasan E dari F. Sekarang jika $f(x)$ dan $f'(x)$ tidak memiliki faktor persekutuan berderajat positif dalam $F[x]$, terdapat polinomial $h(x)$ dan $k(x)$ dalam $F[x]$ sehingga $f(x)h(x) + f'(x)\, k(x) = 1$.

Perhatikan $f(x)\, h(x) + f'(x)\, k(x)$ adalah sebuah elemen dari $E[x]$, kita juga melihat bahwa $(x - a)$ adalah faktor dari 1. Oleh karena itu tidak mungkin, $f(x)$ dan $f'(x)$ harus memiliki sebuah faktor persekutuan yang berderajat positif dalam $F[x]$.

Sebaliknya, perhatikan bahwa $f(x)$ dan $f'(x)$ memiliki faktor persekutuan yang berderajat positif. Misalkan a adalah nol dari faktor persekutuan, maka a adalah nol dari $f(x)$ dan $f'(x)$. Karena a adalah nol dari $f(x)$, terdapat sebuah polinomial $q(x)$ sehingga $f(x) = (x - a)q(x)$. Dengan demikian, $f'(x) = (x - a)\, q'(x) + q(x)$ dan $0 = f'(a) = q(a)$. Sehingga, $x - a$ adalah faktor dari $q(x)$ dan a adalah perkalian nol dari $f(x)$.

Teorema 9.6. Nol dari Polinomial Tidak Tereduksi (Zeros of an Irreducible)

Misalkan $f(x)$ adalah polinomial *irreducible* pada *field* F. Jika F memiliki karakteristik 0, maka $f(x)$ tidak memiliki perkalian nol. Jika F memiliki karakteristik $p \neq 0$, maka $f(x)$ memiliki sebuah perkalian nol hanya jika $f(x) = g(x^p)$ untuk beberapa $g(x)$ dalam $F[x]$.

Contoh 9.11:

Jika $f(x) = x^{4p} + 3x^{2p} + x^p + 1$ dan $F = p \neq 0$, maka:
$g(x) = x^4 + 3x^2 + x + 1$

9.4 LAPANGAN SEMPURNA (PERFECT FIELD)

Definisi 9.4:

Sebuah *field* F dikatakan *perfect* jika F mempunyai karakteristik 0 atau jika F mempunyai karakteristik p dan $F^p = \{a^p | a \in F\} = F$.

Teorema 9.7:

Setiap *finite field* adalah *perfect*.

Bukti:

Misalkan F adalah finite *field* dari karakteristik p. Perhatikan pemetaan Φ dari F ke F didefinisikan dengan $\Phi(x) = x^p$ untuk semua $x \in F$. Kita menganggap bahwa Φ adalah *field* yang automorfisma. Jelas, $\Phi(ab) = (ab)^p = a^p b^p = \Phi(a)\,\Phi(b)$. Lebih lanjut,

$$\begin{aligned}\Phi(a+b) &= (a+b)^p \\ &= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + \binom{p}{p-1}ab^{p-1} + b^p \\ &= a^p + b^p\end{aligned}$$

Karena setiap $\binom{p}{i}$ terbagi oleh p. Akhirnya, karena $x^p \neq 0$ ketika $x \neq 0$, Ker $\Phi = \{0\}$. Maka, Φ adalah satu-satu (1-1) dank arena F merupakan finite, Φ adalah onto. Terbukti bahwa $F^p = F$.

Teorema 9.8

Jika $f(x)$ adalah polinomial yang *irreducible* pada sebuah *perfect field* F, maka $f(x)$ tidak memiliki perkalian nol.

Bukti:

Akan dibuktikan F memiliki karakteristik 0.

Misalkan kita berasumsi bahwa $f(x) \in F[x]$ adalah *irreducible* pada sebuah *perfect field* F dari karakteristik p dan bahwa $f(x)$ memiliki perkalian nol. Berdasarkan teorema di atas, kita mengetahui bahwa $f(x) = g(x^p)$ untuk $g(x) \in F[x]$, katakan $g(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$. Karena $F^p = F$, setiap a_i dalam F dapat ditulis dalam bentuk b_i^p untuk beberapa b_i dalam F. Dengan demikian:

$$
\begin{aligned}
f(x) &= g\left(x^p\right) \\
&= b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \ldots + b_1^p x^p + b_0^p \\
&= \left(b_n x^n + b_{n-1} x^{n-1} + \ldots + b_1 x + b_0\right)^p \\
&= \left(h(x)\right)^p
\end{aligned}
$$

Dimana $h(x) \in F[x]$. Akan tetapi, $f(x)$ bukan *irreducible.*

Teorema 9.9.

Misalkan $f(x)$ adalah polinomial *irreducible* pada sebuah *field* F dan misalkan E adalah *splitting field* dari $f(x)$ pada F. Maka, semua bilangan nol dari $f(x)$ dalam E memiliki perkalian yang sama.

Bukti:

Misalkan a dan b adalah dua nol yang berbeda dari $f(x)$ dalam E. Jika a mempunyai perkalian m dalam $E[x]$, maka dapat ditulis $f(x) = (x - a)^m g(x)$. Terdapat isomorfisma Φ dari E pada dirinya sendiri yang membawa a ke b dan bertindak sebagai identitas pada F. Maka,

$$f(x) = \Phi(f(x)) = (x - b)^m \, \Phi(g(x))$$

Dan kita lihat bahwa perkalian dari b adalah lebih besar atau sama dengan perkalian dari a. Dengan mempertukarkan peran a dan b, kita perlihatkan bahwa perkalian a lebih besar dari atau sama dengan perkalian b. Jadi, kita telah membuktikan bahwa a dan b mempunyai perkalian yang sama.

Corollary 9.3.

Misalkan $f(x)$ adalah sebuah polinomial yang *irreducible* pada sebuah *field* F dan misalkan E adalah *splitting field* dari $f(x)$. Maka $f(x)$ mempunyai bentuk:

$$a(x-a_1)^n (x-a_2)^n \dots (x-a_t)^n,$$

Dimana $a_1, a_2, \dots, a_t$ adalah elemen yang berbeda dari E dan $a \in F$.

Contoh 9.12:

Misalkan $F = Z_2(t)$ adalah *field* dari ring faktor $Z_2[t]$ dari polinomial dalam t yang tidak tentu dengan koefisien dari Z_2. Kita harus memperkenalkan nilai x yang lain, karena anggota dari F adalah koefisien yang dijadikan sebagai elemen di $F[x]$. Pertimbangkan $f(x) = x^2 - t \in F[x]$. Perhatikan bahwa $f(x)$ *irreducible* pada F, cukup menunjukkan bahwa itu tidak mempunyai nol dalam F. Lebih lanjut, perhatikan bahwa $h(t)/k(t)$ adalah nol di $f(x)$. Kemudian $(h(t)/k(t))^2 = t$, dan oleh karena itu $(h(t))^2 = t(k(t))^2$. Karena $h(t), k(t) \in Z_2[t]$, maka $h(t^2) = tk(t^2)$. Akan tetapi derajat $h(t^2)$ adalah genap, dan derajat $tk(t^2)$ adalah ganjil. Jadi, $f(x)$ adalah *irreducible* pada F.

Akhirnya, karena t adalah konstan di $F[x]$ dan karakteristik dari F adalah 2, kita mempunyai $f'(x) = 0$, sehingga $f'(x)$ dan $f(x)$ mempunyai $f(x)$ sebagai faktor persekutuan. Jadi, $f(x)$ memiliki perkalian nol di beberapa perluasan F. Tentu saja, hal ini memiliki perkalian nol tunggal 2 dalam $K = F[x]/\langle x^2 - t\rangle$.

RANGKUMAN

1. Sebuah *field* E dikatakan sebuah lapangan perluasan (*extension field*) dari *field* F, jika $F \subseteq E$, dimana operasi F adalah operasi E yang dibatasi pada F.
2. Misal F adalah lapangan (*field*) dan $f(x)$ polinomial yang tidak konstan dalam $F[x]$, maka terdapat lapangan perluasan (*extension field*) E dari F, dimana $f(x)$ memiliki nol.
3. Jika $p(x)$ polinomial tidak tereduksi (*irreducible*) berderajat $n > 1$ pada F dan $\alpha = x + \langle p(x)\rangle$ dan $c + \langle p(x)\rangle$ dengan c berlaku untuk semua c dalam F, maka *extension field* $E = F[x]/\langle p(x)\rangle$ terdiri dari semua elemen berbentuk $c_{n-1} + \alpha^{n-1} + \dots + c_1\alpha + c_0$ dengan semua c_j dalam F.
4. Misalkan F adalah sebuah lapangan perlusan (*extension field*) dari F

dan misalkan $f(x) \in F[x]$ dengan derajat sekurang-kurangnya 1. Kita katakan bahwa $f(x)$ terpisah (*splits*) di E jika ada elemen $a \in F$ dan a_1, $a_2, \ldots, a_n \in E$ sedemikian sehingga:

$$f(x) = ax - a_1)(x - a_2) \ldots (x - a_n)$$

Kita sebut E sebuah lapangan pemisah (*splitting field*) dari $f(x)$ pada F, jika:

$$E = F(a_1, a_2, \ldots, a_n)$$

5. Misalkan F adalah sebuah *field* dan misalkan $f(x)$ adalah elemen tidak konstan dari $F[x]$. Maka, terdapat sebuah *splitting field* E untuk $f(x)$ terhadap F.
6. Misalkan F adalah *field* dan misalkan $p(x) \in F[x]$ tidak tereduksi (*irreducible*) terhadap F. Jika a adalah bilangan nol dari $p(x)$ dalam beberapa perluasan E dari F, maka $F(a)$ adalah isomorfik pada $F[x]/\langle p(x) \rangle$. Lebih lanjut, jika derajat $p(x) = n$, maka setiap anggota dari $F(a)$ dapat ditulis dalam bentuk yang unik, yaitu:

   $$c_{n-1}\, a^{n-1} + c_{n-2}\, a^{n-2} + \ldots + c_1\, a + c_0$$

   di mana $c_0, c_1, \ldots, c_{n-1} \in F$.
7. Misalkan F adalah sebuah *field* dan misalkan $p(x) \in F[x]$ tidak tereduksi *irreducible* pada E. Jika a adalah nol dari $p(x)$ dalam beberapa perluasan E ke F dan b adalah nol dari $p(x)$ dalam beberapa perluasan E' ke F, maka *field* $F(a)$ dan $F(b)$ adalah isomorfik.
8. Misalkan F adalah *field*, $p(x) \in F[x]$ *irreducible* pada F, dan misalkan a adalah bilangan nol dari $p(x)$ dalam beberapa perluasan dari F. Jika Φ adalah *field* yang isomorfisma dari F ke F' dan b adalah bilangan nol dari $\Phi(p(x))$ dalam beberapa perluasan dari F', maka ada sebuah isomorfisma dari $F(a)$ ke $F'(b)$ yang yang setuju dengan Φ pada F dan membawa a ke b.
9. Misalkan Φ isomorfisma dari sebuah *field* F ke *field* F' dan misalkan $f(x) \in F[x]$. Jika E adalah sebuah *splitting field* untuk $f(x)$ pada F dan E' adalah *splitting field* untuk $\Phi(f(x))$ pada F', maka ada sebuah isomorfisma dari E ke E' sepaham dengan Φ pada F.
10. Misalkan F adalah *field* dan misalkan $f(x) \in F[x]$. Maka setiap dua *splitting field* dari $f(x)$ pada F adalah isomorfik.
11. Misalkan $f(x) = a^n\, x^n + a_{n-1}\, x^{n-1} + \ldots + a_1\, x + a_0$ dari $F[x]$. Turunan (*derivative*) dari $f(x)$, dinotasikan dengan $f'(x)$ adalah polinomial:

$na_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \ldots + a_1$ dalam $F[x]$

12. Misalkan $f(x)$ dan $g(x) \in F[x]$ dan misalkan $a \in F$, maka:
    a) $(f(x) + g(x))' = f'(x) + g'(x)$
    b) $(af(x))' = af'(x)$
    c) $(f(x)g(x))' = f(x)g'(x) + g(x)f'(x)$
13. Sebuah polinomial $f(x)$ pada *field* F memiliki perkalian nol dalam beberapa perluasan E jika dan hanya jika $f(x)$ dan $f'(x)$ memiliki sebuah faktor persekutuan berderajat positif dalam $F[x]$.
14. Misalkan $f(x)$ adalah polinomial *irreducible* pada *field* F. Jika F memiliki karakteristik 0, maka $f(x)$ tidak memiliki perkalian nol. Jika F memiliki karakteristik $p \neq 0$, maka $f(x)$ memiliki sebuah perkalian nol hanya jika $f(x) = g(x^p)$ untuk beberapa $g(x)$ dalam $F[x]$.
15. Sebuah *field* F dikatakan *perfect* jika F mempunyai karakteristik 0 atau jika F mempunyai karakteristik p dan $F^p = \{a^p | a \in F\} = F$.
16. Setiap *finite field* adalah *perfect*.
17. Jika $f(x)$ adalah polinomial yang *irreducible* pada sebuah *perfect field* F, maka $f(x)$ tidak memiliki perkalian nol.
18. Misalkan $f(x)$ adalah polinomial *irreducible* pada sebuah *field* F dan misalkan E adalah *splitting field* dari $f(x)$ pada F. Maka, semua bilangan nol dari $f(x)$ dalam E memiliki perkalian yang sama.
19. Misalkan $f(x)$ adalah sebuah polinomial yang *irreducible* pada sebuah *field* F dan misalkan E adalah *splitting field* dari $f(x)$. Maka $f(x)$ mempunyai bentuk:

$$a(x-a_1)^n (x-a_2)^n \ldots (x-a_t)^n,$$

Dimana $a_1, a_2, \ldots, a_t$ adalah elemen yang berbeda dari E dan $a \in F$.

LATIHAN

1. Sebutkan elemen dari $Q(\sqrt[3]{5})$.
2. Cari *splitting field* dari $x^3 - 1$ pada Q. Nyatakan jawaban Anda dalam bentuk $Q(a)$.
3. Cari *splitting field* dari $x^4 + 1$ pada Q.
4. Cari *splitting field* dari $x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$ pada Q.

5. Cari sebuah polinomial $p(x)$ dalam $Q[x]$ agar $Q\left(\sqrt{1+\sqrt{5}}\right)$ merupakan ring isomorfik ke $Q[x]/\langle p(x)\rangle$.
6. Misalkan $F=Z_2$ dan misalkan $f(x)=x^3+x+1\in F[x]$. Andaikan a adalah nol dari $f(x)$ dalam beberapa perluasan di F. Berapa banyak elemen dari $F(a)$? Nyatakan setiap anggota dari $F(a)$ dalam istilah a.
7. Cari semua ring automorfisma dari $Q\left(\sqrt[3]{5}\right)$.
8. Andaikan β adalah nol dari $f(x)=x^4+x^2+1$ dalam beberapa perluasan *field* E di Z_2. Nyatakan $f(x)$ sebagai hasil dari faktor linier dalam $E[x]$.
9. Nyatakan x^8-x sebagai hasil dari *irreducible* pada Z_2.
10. Buktikan bahwa $Q\left(\sqrt{3}\right)$ dan $Q\left(\sqrt{-3}\right)$ adalah ring isomorfik atau bukan.
11. Jika β adalah nol dari x^4+x^2+1 pada Z_2, temukan nol yang lain.
12. Tunjukkan bahwa $x^{21}+2x^8+1$ tidak mempunyai perkalian nol di setiap perluasan dari Z_3.
13. Tunjukkan bahwa $x^{21}+2x^9+1$ mempunyai perkalian nol di beberapa perluasan dari Z_3.
14. Temukan *splitting field* untuk $f(x)=(x^2+x+2)\ (x^2+2x+2)$ pada $Z_3[x]$. Tulis $f(x)$ hasil dari faktor linear.
15. Misalkan F adalah sebuah *field* dengan karakteristik $p\neq 0$. Tunjukkan bahwa polinomial $f(x)=x^{p^n}-x$ pada F mempunyai nol yang lain.

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$\boxed{\textit{Tingkat penguasaan} = \frac{\textit{Banyak jawaban yang benar}}{\textit{Banyak soal}}\times 100\%}$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai berikut ini.

Rentang Nilai (%)	Kategori
90 – 100	Sangat Baik
80 – 89	Baik
70 – 79	Sedang
$\leq$ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi $\geq$ 70%, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang < 70%, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

BAB 10

DAERAH FAKTORISASI TUNGGAL DAN DAERAH EUCLID

Tujuan Instruksional Umum:

Setelah mempelajari materi pada bab ini, maka diharapkan mahasiswa dapat mengaplikasikan definisi dan teorema terkait daerah faktorisasi tunggal, daerah ideal utama, bilangan aljabar, dan daerah Euclid.

Tujuan Instruksional Khusus:

Setelah diberikan penjelasan terkait dan teorema-teorema dasar terkait daerah faktorisasi tunggal, daerah ideal utama, dan daerah Euclid, maka diharapkan mahasiswa dapat:

a. Menjelaskan definisi dari daerah faktorisasi tunggal.
b. Menjelaskan definisi dari daerah ideal utama.
c. Menjelaskan definisi dari daerah Euclid.
d. Menjelaskan definisi bilangan aljabar.
e. Mengaplikasikan dan membuktikan teorema-teorema terkait daerah faktorisasi tunggal.
f. Menentukan FPB dari polinomial yang tidak tereduksi (*irreducible*).
g. Mengaplikasikan dan membuktikan teorema-teorema terkait daerah ideal utama.
h. Mengaplikasikan dan membuktikan teorema-teorema terkait daerah Euclid.

Deskripsi Singkat:

Dalam bab ini akan dibahas tentang definisi, teorema, lemma, maupun contoh terkait daerah faktorisasi tunggal, daerah ideal utama, bilangan aljabar dan daerah Euclid.

10.1 DAERAH FAKTORISASI TUNGGAL

Definisi 10.1.

Andaikan D merupakan *integral domain* dan $a, b \in D$. Jika terdapat $c \in D$ sehingga $b = ac$, maka dikatakan a membagi b (a faktor dari b) atau dapat ditulis dengan $a|b$. Simbol $a \nmid b$ menyatakan a tidak habis membagi b.

Contoh 10.1:

Pada *integral domain* Z, $3|12$ karena terdapat $4 \in Z$, sehingga $12 = 3 \cdot 4$. Tetapi $4 \nmid 10$ karena untuk setiap $a \in Z$, $4 \cdot a \neq 10$.
Pada integral domain R, $4|10$ karena terdapat $2\frac{1}{2} \in R$, sehingga $10 = 4 \cdot 2\frac{1}{2}$.

Definisi 10.2:

Diketahui $a = a(x)$ dan $b = b(x)$ elemen $F[x]$ yang tidak nol. Faktor persekutuan terbesar (*greatest common divisor*) dari a dan b (dinotasikan dengan (a,b)) adalah polinomial monik $d = d(x)$ sehingga:

i) d membagi a dan b
ii) Jika c sembarang elemen $F[x]$ yang membagi a dan b, maka c membagi d.

Contoh 10.2:

Perhatikan ring Z_{10}. Maka $[4] = [4][6]$ dan $[6] = [4][4]$. Hal ini menunjukkan bahwa [4] dan [6] merupakan masing-masing faktor persekutuan (common divisor). Oleh karena itu, [4] dan [6] harus menjadi faktor persekutuan terbesar dari [4] dan [6]. Selanjutnya, [4] dan [6] berasosiasi karena [9] adalah sebuah unit dan $[6] = [9][4]$.

Contoh: 10.3:

Ring E bilangan genap, 2 tidak memiliki pembagi. Oleh karena itu, 2 dan tidak ada bilangan bulat genap lain yang memiliki faktor persekutuan.

Contoh 10.4:

Dalam daerah $Z\left[i\sqrt{5}\right]$, buktikan bahwa:

(a) $\gcd\left(2, 1 + i\sqrt{5}\right) = 1$

(b) $\gcd 6\left(1-i\sqrt{5}\right)$ dan $3\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)$ tidak ada.

penyelesaian:

(a) Dalam $Z\left[i\sqrt{\ }\right]$, unsur satuan adalah 1 dan -1.

Misalkan $a+ib\sqrt{5}=\gcd\left(2,1+i\sqrt{5}\right)$. Maka $\left(a+ib\sqrt{5}\right)|2$.

Dengan demikian, $2=\left(a+ib\sqrt{5}\right)\left(c+id\sqrt{5}\right)$ untuk beberapa $c+id\sqrt{5}\in Z\left[i\sqrt{5}\right]$. Hal ini berimplikasi bahwa:

$$4=\left(a^2+5b^2\right)\left(c^2+5d^2\right)$$

karena itu,

$$a^2+5b^2=2,\qquad c^2+5d^2=2 \tag{10.1}$$

atau

$$a^2+5b^2=4,\qquad c^2+5d^2=1 \tag{10.2}$$

atau

$$a^2+5b^2=1,\qquad c^2+5d^2=4 \tag{10.3}$$

Dari persamaan (10.1) tidak dapat ditemukan untuk setiap c, $d\in Z$. Hanya solusi integral dari $a^2+5b^2=4$ yaitu $a=\pm 2$ dan $b=0$ dan hanya solusi integral $a^2+5b^2=1$ yaitu $a=\pm 1$ dan $b=0$. Kemudian, dari persamaan (10.2) dan (10.3) kita menemukan $\gcd\left(2,1+\ \sqrt{5}\right)=1$ atau 2. Jika $\gcd\left(2,1+i\sqrt{5}\right)=2$, maka $2,|\left(1+i\sqrt{5}\right)$. Oleh karena itu, $1+i\sqrt{5}=2\left(p+iq\sqrt{5}\right)$ untuk beberapa $p+iq\sqrt{5}\in Z\left[i\sqrt{5}\right]$. Hal ini berimplikasi bahwa $2q=1=2q$. Tetapi tidak ada bilangan bulat p dan q sehingga $2p=1=2q$. Oleh karena itu, $\gcd\left(2,1+i\sqrt{5}\right)=1$.

(b) Perhatikan terdapat $\gcd\left(6\left(1-i\sqrt{5}\right),3\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)\right)$. Maka $\gcd\left(6\left(1-i\sqrt{5}\right),3\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)\right)=3\left(1-i\sqrt{5}\right)$ $\gcd\left(2,1+i\sqrt{5}\right)=3\left(1-i\sqrt{5}\right)$. Selanjutnya, $\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)=6$. Karena 6 adalah faktor persekutuan dari $6\left(1-i\sqrt{5}\right)$ dan $3\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)$. Konsekuensinya, $6\,|\,3\left(1-i\sqrt{5}\right)$. Hal ini berimplikasi $2|\left(1-i\sqrt{5}\right)$, yang tidak benar dalam $Z\left[i\sqrt{5}\right]$.

Oleh karena itu, $\gcd\left(6\left(1-i\sqrt{5}\right),3\left(1+i\sqrt{5}\right)\left(1-i\sqrt{5}\right)\right)$ tidak ada.

Contoh 10.5:

Dalam $Z[i]$, temukan $\gcd(9-5i, -9+13i)$

Penyelesaian:

Misalkan $Z[i]$ adalah daerah Euclid, maka nilai didefinisikan dengan: $N(a+bi) = a^2 + b^2$. Sekarang, $N(9-5i) = 106$ dan $N(-9+13i) = 250$.

Langkah 1:

$$\begin{aligned}
\frac{-9+13i}{9-5i} &= \frac{(-9+13i)(9+5i)}{106} \\
&= \frac{-81-45i+117i-65}{106} \\
&= \frac{-146+72i}{106} \\
&= -\frac{146}{106} + \frac{72i}{106} \\
&= \left(-1-\frac{40}{106}\right) + \left(1-\frac{34}{106}\right)i \\
&= (-1+i) - \frac{40+34i}{106}
\end{aligned}$$

Dengan demikian,

$$\begin{aligned}
-9+13i &= (-1+i)(9-5i) - \frac{40+34i}{106}(9-5i) \\
&= (-1+i)(9-5i) - \frac{360+306i-200i+170}{106} \\
&= (-1+i)(9-5i) - \frac{530+106i}{106} \\
&= (-1+i)(9-5i) + (-5-i)
\end{aligned}$$

Catat bahwa $N(-5-i) < N(9-5i)$.

Langkah 2

$$\begin{aligned}
\frac{9-5i}{-5-i} &= \frac{9-5i}{-5-i} \times \frac{-5+i}{-5+i} \\
&= \frac{-45+9i+25i+5}{26}
\end{aligned}$$

$$= \frac{-40+34i}{26}$$
$$= \frac{-20+17i}{13}$$
$$= \frac{-20}{13} + \frac{17}{13}i$$
$$= \left(-1-\frac{7}{13}\right) + \left(1+\frac{4}{13}\right)i$$
$$= (-1+i) + \frac{-7+4i}{13}$$

Dengan demikian,

$$9-5i = (-1+i)(-5-i) + \frac{-7+4i}{13}(-5-i)$$
$$= (-1+i)(-5-i) + \frac{35+7i-20i+4}{13}$$
$$= (-1+i)(-5-i) + \frac{39-13i}{13}$$
$$= (-1+i)(-5-i) + (3-i)$$

Catat bahwa $N(3-i) < N(-5-i)$

Langkah 3:

$$\frac{-5-i}{3-i} = \frac{-5-i}{3-i} \times \frac{3+i}{3+i}$$
$$= \frac{-15-5i-3i+1}{10}$$
$$= \frac{-14-8i}{10}$$
$$= \frac{-7-4i}{5}$$
$$= \frac{-7}{5} - \frac{4}{5}i$$
$$= \left(-1-\frac{2}{5}\right) - \left(1-\frac{1}{5}\right)i$$
$$= (-1-i) + \frac{-2+i}{5}$$

Dengan demikian,

$$\begin{aligned}-5-i &= (-1-i)(3-i)+\frac{-2+i}{5}(3-i)\\ &= (-1-i)(3-i)+\frac{-6+2i+3i+1}{5}\\ &= (-1-i)(3-i)+\frac{-5+5i}{5}\\ &= (-1-i)(3-i)+(-1+i)\end{aligned}$$

Catat bahwa $N(-1+i) < N(3-i)$

Langkah 4

$$\begin{aligned}\frac{3-i}{-1+i} &= \frac{-5-i}{(-1+i)}\times\frac{-1-i}{(-1-i)}\\ &= \frac{-3-3i+i-1}{2}\\ &= \frac{-4-2i}{2}\\ &= -2-i\end{aligned}$$

Dengan demikian,
$3\text{-}i = (-2-i)\ (-1+i)\ +\ 0$
Oleh karena itu, $\gcd(9-5i, -9+13i) = -1+i$

Teorema 10.1

Jika diketahui $a(x)$ dan $b(x)$ dalam $F[x]$, maka $a(x)$ dan $b(x)$ mempunyai FPB dalam $F[x]$ dan terdapat polinomial $s(x)$ dan $t(x)$ dalam $F[x]$ sehingga:

$$s(x)a(x)+t(x)b(x)=d(x)$$

Bukti:

Misalkan $a=a(x)$ dan $b(x)$, maka dibentuk himpunan $J=\{ua+vb|u, v$ dalam $F[x]\}$. Akan dibuktikan bahwa J ideal dalam $F[x]$. Namun, karena setiap ideal dalam bentuk $J=(d(x))$ untuk suatu $d(x)$ dalam $F[x]$, maka $d=sa+bt$ untuk suatu s dan t dalam $F[x]$. Dengan tidak membuang sifat umum, dianggap bahwa d monik.

Akan ditunjukkan bahwa d merupakan FPB dari a dan b. Karena $a=1\cdot a+0\cdot b$ dan $b=0\cdot a+1\cdot b$, 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 $d=sa+tb$

dan g membagi kedua suku pada ruas kanan, maka g membagi d.

Berarti d memenuhi syarat sebagai FPB dari a dan b.

Contoh 10.6:

Polinomial $p(x)=x^2-2$ *irreducible* pada *field* Q yang diperoleh dengan menggabungkan akar dari polinomial $p(x)$ yaitu $\alpha=\sqrt{2}$ pada Q.
Akan dicari invers perkalian dari elemen $4+3\sqrt{2}$
Polinomial $f(x)=3x+4$ dan $p(x)$ prima relative atas 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 $p\left(\sqrt{2}\right)=0$, maka diperoleh:

$$f\left(\sqrt{2}\right)\left(\frac{3}{2}\sqrt{2}-2\right)=1$$

Sehingga:

$$\left(4+3\sqrt{2}\right)^{-1}=f\left(\sqrt{2}\right)^{-1}$$
$$=\frac{3}{2}\sqrt{2}-2$$

Contoh 10.7:

Akan ditentukan FPB dari $a=x^6+2x^5+x^2+2$ dan $b=2x^4+x^3+2x+1$ atas Z_3.

Penyelesaian:

$a=b\cdot(2x^2+x+2)+(2x^3+2x+2)$
$b=(2x^3+2x^2+2)\cdot(x+1)+(x^2+1)$
$(2x^3+2x^2+2)=(x^2+2)\cdot(2x+2)+(2x+1)$
$(x^2+2)=(2x+1)\cdot(2x+2)+0$

Sisa tidak nol yang terakhir yaitu $(2x+1)$ digandakan dengan $2^{-1}=2$ dan diperoleh $x+2$.

Berarti FPB dari a dan b adalah $x+2$.

Definisi 10.3

Misalkan D daerah integral dan $a,\ b \in D$. Dimana a dan b dikatakan berasosiasi apabila terdapat unit $u \in D$, sehingga $a = bu$.

Contoh 10.8:

Elemen unit pada daerah integral (*integral domain*) Z adalah 1 dan -1. Dengan demikian setiap $x \in Z$ berasosiasi dengan x dan $-x$.

Definisi 10.4

Misalkan D daerah integral (integral domain), $p \in D - \{0\}$ dan p bukan unsur satuan. p dinamakan elemen tidak tereduksi (*irreducible*) atas D jika setiap faktorisasi $p = ab$ mengakibatkan a atau b unsur satuan. Jika p dapat difaktorkan menjadi $p = ab$ dengan a,b bukan unsur satuan, maka p dinamakan elemen tereduksi.

Contoh 10.9:

Pada daerah integral Z, 5 merupakan elemen tidak tereduksi karena faktorisasi dari 5 hanya $5 = 1 \cdot 5 = 5 \cdot 1 = (-1) \cdot (-5) = (-5) \cdot (-1)$ dengan 1 dan -1 merupakan elemen satuan di Z. Akan tetapi 14 merupakan elemen tereduksi karena 14 dapat dinyatakan sebagai $2 \cdot 7$.

Definisi 10.5

Misalkan D daerah integral. D dinamakan **daerah faktorisasi tunggal** jika memenuhi syarat berikut

i) Setiap $p \in D - \{0\}$, p bukan unsur satuan dapat dinyatakan sebagai hasil kali sejumlah elemen berhingga yang tidak tereduksi.

ii) Jika $p_1\, p_2 \ldots p_r$ dan $q_1\, q_2 \ldots q_s$ merupakan dua jenis faktorisasi dari suatu elemen $p \in D$ dengan p_i, q_i elemen tidak tereduksi, maka $r = s$. Jika diubah urutan, diperoleh p_i berasosiasi dengan q_i.

Contoh 10.10:

Buktikan bahwa Z merupakan daerah faktorisasi tunggal, dimana $12 \in Z$ berlaku $12 = 2 \cdot 2 \cdot 3 = (-2) \cdot (2) \cdot (-3)$. Jelas terbukti bahwa 2 berasosiasi dengan -2 dan 3 berasosiasi dengan -3.

Untuk selanjutnya, kita akan membahas bahwa setiap daerah ideal utama merupakan daerah faktorisasi tunggal.

Teorema 10.2

Misalkan D adalah daerah ideal utama. Jika $N_1 \subset N_2 \subset \ldots$ merupakan ideal ideal-ideal di D, maka terdapat bilangan bulat positif r sehingga $N_r = N_s$ untuk semua $s \geq r$.

Bukti:

Misalkan $N_1 \subset N_2 \subset \ldots$ merupakan ideal-ideal di D. Dapat ditulis dalam bentuk:

$$N = \bigcup_i Ni$$

Ditunjukkan N ideal di D.

(i) Ambil sembarang $a, b \in N$
Maka terdapat i dan j sehingga $a \in N_i$ dan $b \in N_j$
Karena $N_1 \subset N_2 \subset \ldots$ maka $N_i \subset N_j$ atau $N_j \subset N_i$
Misalkan $N_i \subset N_j$
Maka, $a, b \in N_j$
Karena N_j ideal maka $a - b, ab \in N_j$.
Jadi $a - b, ab \in N$.

(ii) Ambil sembarang $a \in N$ dan $d \in D$
Karena $a \in N$, maka $a \in N_k$ untuk suatu $k \in Z^+$
Karena N_k ideal maka $ad, da \in N_k$
Jadi, $ad, da \in N$.

Dari (i) dan (ii) dapat disimpulkan bahwa N ideal di D.
Karena D daerah ideal utama maka $N = \langle c \rangle$ untuk suatu $c \in D$.
Akibatnya $c \in N_r$ untuk suatu $r \in Z^+$.
Untuk $s \geq r$ diperoleh $\langle c \rangle \subset N_r \subset N_s \subset N = \langle c \rangle$.
Sehingga $N_r = N_s$.
Jadi, terbukti bahwa terdapat $r \in Z^+$ sehingga $N_r = N_s$ untuk semua $s \geq r$.

Teorema 10.3.

Misalkan D daerah integral dan $a, b \in D$, maka:

(i) $\langle a \rangle \subset \langle b \rangle$ jika dan hanya jika $b | a$

(ii) $\langle a \rangle = \langle b \rangle$ jika dan hanya jika a dan b berasosiasi.

Bukti:

Diserahkan kepada pembaca sebagai latihan.

Teorema 10.4:

Misalkan D daerah ideal utama. Jika $a \in D-\{0\}$, a bukan unit maka a dapat dinyatakan sebagai hasil kasil elemen-elemen tak tereduksi.

Bukti:

Ambil sembarang $a \in D - \{0\}$, a bukan unsur satuan.

Claim

a mempunyai faktor elemen tak tereduksi.

Bukti:

Jika a tidak tereduksi maka bukti claim selesai.

Misalkan a tereduksi.

Maka $a = a_1 b_1$ untuk suatu $a_1, b_1 \in D$ dan keduanya bukan unsur satuan.

Berdasarkan teorema 10.3 diperoleh $\langle a \rangle \subset \langle a_1 \rangle$.

Jika $\langle a \rangle = \langle a_1 \rangle$ maka a dan a_1 berasosiasi sehingga a_1 unsur satuan.

Bertentangan dengan a_1 bukan unsur satuan.

Jadi $\langle a \rangle \neq \langle a_1 \rangle$

Jika a_1 tidak tereduksi maka bukti claim selesai. Misalkan a_1 tereduksi.

Maka $a_1 = a_2\, b_2$ untuk suatu a_2, $b_2 \in D$ dan keduanya bukan unsur satuan.

Berdasarkan Teorema di atas diperoleh $\langle a_1 \rangle \subset \langle a_2 \rangle$, $\langle a_1 \rangle \neq \langle a_2 \rangle$.

Jika proses ini dilanjutkan, maka diperoleh rangkaian ideal-ideal di D, yaitu:

$$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \ldots$$

Berdasarkan Teorema 10.2 haruslah terdapat $r \in Z^+$ sehingga $\langle a_r \rangle = \langle a_s \rangle$ untuk semua $s \geq r$.

Hal ini menunjukkan bahwa a_r merupakan elemen tidak tereduksi.

Jadi, claim terbukti, yaitu a mempunyai faktor elemen tidak tereduksi.

Teorema 10.5

Misalkan D daerah integral dan $p \in D$, maka $\langle p \rangle$ merupakan ideal maksimal jika dan hanya jika p elemen tidak tereduksi.

Bukti:

Diserahkan kepada pembaca sebagai latihan.

Teorema 10.6

Misalkan D daerah ideal utama dan p, a, $b \in D$. Jika p tidak tereduksi dan $p|ab$, maka $p|ab$ atau $p|b$.

Bukti:

Misalkan p elemen tidak tereduksi dan $p|ab$.
Karena $p|ab$, maka $ab = dp$ untuk suatu $d \in D$.
Akibatnya $ab \in \langle p \rangle$
Karena $\langle p \rangle$ ideal maksimal, maka $\langle p \rangle$ prima.
Akibatnya $a \in \langle p \rangle$ atau $b \in \langle p \rangle$.
Dengan demikian, $a = pd_1$ atau $b = pd_2$ untuk suatu d_1, $d_2 \in D$.
Jadi, $p|a$ atau $p|b$.

Teorema 10.7

Misalkan D daerah ideal utama dan $p \in D$ elemen tidak tereduksi. Jika $p|a_1\, a_2 \ldots a_n$ dengan $a_i \in D$, maka $p|a_i$ untuk paling sedikit satu nilai i.

Definisi 10.6

Misalkan D daerah integral dan $p \in D - \{0\}$, p bukan unsur satuan, p dinamakan elemen prima jika $p \mid ab$ maka $p \mid a$ atau $p \mid b$.

Contoh 10.11:

3 merupakan elemen prima dalam daerah integral Z karena jika a, $b \in Z$ dan $3|ab$ maka $3|a$ atau $3|b$.

Teorema 10.8:

Setiap daerah ideal utama merupakan daerah faktorisasi tunggal.

Bukti:

Akan ditunjukkan bahwa faktorisasi dalam daerah ideal utama tunggal.

Misalkan a dapat difaktorkan menjadi $a=p_1 p_2 \dots p_r$ dan $a=q_1 q_2 \dots q_s$ dengan p_i, q_i elemen tidak tereduksi.
Maka $p_1 \mid (q_1 q_2 \dots q_s)$
Akibatnya $p_1 \mid Q_j$ untuk suatu $j \in Z^+$.

Apabila perlu dengan mengubah urutan, maka dapat diasumsikan $j=i$, sehingga $p_1 \mid q_1$. Akibatnya $q_1 = p_1 u_1$ untuk suatu $u_1 \in D$.

Karena p_1 tidak teredukasi, maka u_1 unit. Dengan demikian p_1 dan q_1 berasosiasi.

Diperoleh $p_1 p_2 \dots p_t = p_1 u_1 q_2 \dots q_s$. Berdasarkan hukum kanselasi di D diperoleh $p_2 p_3 \dots p_t = u_1 q_2 \dots q_s$.

Apabila proses tersebut dilanjutkan, maka diperoleh $1 = u_1 u_2 \dots u_r q_{r+1} \dots q_s$.

Karena q_i tidak tereduksi, maka $r=s$, dan karena u_i unsur satuan di D, maka p_i berasosiasi dengan q_i. Dengan demikian, terbukti bahwa daerah ideal utama merupakan daerah faktorisasi tunggal.

Lemma 10.1 (Gauss)

Jika $f(x)$ dan $g(x)$ polinomial primitif dalam $Z[x]$ maka hasil kalinya $f(x)g(x)$ juga polinomial primitif.

Teorema 10.9.

Himpunan polinomial $Z[x]$ merupakan daerah faktorisasi tunggal.

Bukti:

Akan dibuktikan bahwa sembarang polinomial tidak konstan $f(x)$ dalam $Z[x]$ dapat difaktorkan secara tunggal sebagai hasil kali polinomial tidak tereduksi dan hasil pemfaktoran tunggal.

Kasus 1: Primitif

Dalam $Q[x]$, $f(x)$ mempunyai faktor tunggal

$$f(x) = q_1(x)\, q_2(x) \dots q_k(x)$$

Polinomial-polinomial $q_j(x)$ dapat ditulis sebagai $c_j \cdot Q_j(x)$ dengan $Q_j(x)$ primitif dan diperoleh:

$$f(x) = c_1 c_2 \dots c_k\, Q_1(x)\, Q_2(x) \dots Q_k(x)$$

Karena $Q_j\,(x)$ sekawan dengan $Q_j\,(x)$ maka $Q_j\,(x)$ juga tidak tereduksi. Dengan mengingat lemma Gaus, maka $Q_1\,(x)\,Q_2\,(x)\,\ldots\,Q_k\,(x)$ primitif. Karena $f(x)$ primitif dan sama dengan $1 \cdot f(x)$ 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 tidak tereduksi dalam $Z[x]$.

Misalkan dimiliki suatu faktorisasi tidak tereduksi $f(x) = s_1\,(x)\,s_2\,(x)\,\ldots\,s_m\,(x)$ dalam $Z[x]$ maka $s_i\,(x)$ haruslah primitif dengan membandingkan faktorisasi dalam $Q[x]$ diperoleh $m = k$ dan s_i dalam $Q[x]$ sekawan dengan Q_j. Akan tetapi primitif-primitif ini harus 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 tersebut berarti faktorisasi dalam $Z[x]$ adalah tunggal.

Kasus 2: Tidak Primitif

Karena $f(x)$ tidak primitif maka $f(x) = c_j \cdot F(x)$ dengan $F(x)$ primitif dan c_j bilangan bulat positif yang tunggal, sehingga:

$$\begin{aligned} f(x) &= c_j \cdot F(x) \\ &= p_1\,p_2 \cdots p_u\;\; Q_1\,(x)\,Q_2\,(x)\,\ldots\,Q_k\,(x) \end{aligned}$$

Hal ini terjadi karena Z merupakan daerah faktorisasi tunggal dan bersama dengan kasus 1 disimpulkan bahwa terdapat faktorisasi tunggal untuk $f(x)$.

Contoh 10.12:

Polinomial $p(x) = x^4 + 4x^3 - 3x - 2$ dapat difaktorkan menjadi:

$$p(x) = x^4 + 4x^3 - 3x - 2 = (x+1)^2\,(x-1)(x+2)$$

pemfaktoran ini dikatakan karena tidak memiliki bentuk pemfaktoran yang lain.

Teorema 10.10

Diketahui $g(x) = \sum_{i=0}^{n} a_i x^i$ 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 $g(x)$ tidak tereduksi atas Q.

Contoh 10.13:

Polinomial x^4+1 dapat difaktorisasi menjadi atas polinomial tidak tereduksi atas $R[x]$ menjadi:

$$x^4+1=\left(x^2-\sqrt{2}x+1\right)\left(x^2+\sqrt{2}x+1\right)$$

Akan tetapi tidak dapat difaktorkan menjadi polinomial atas $Q[x]$ sehingga merupakan polinomial tidak tereduksi dalam $Q[x]$. Selanjutnya, polinomial x^4+1 dapat difaktorisasi menjadi polinomial tidak tereduksi atas $C[x]$ 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 x^4+1 merupakan polinomial tidak tereduksi dalam $Q[x]$.

10.2 DAERAH EUCLID

Definisi 10.7

Suatu daerah integral D dinamakan **daerah Euclid** jika terdapat pemetaan:

$\varphi: D-\{0\} \rightarrow Z^{+}\cup\{0\}$ sehingga memenuhi

(*i*) Untuk setiap a, $b\in D-\{0\}$, $\varphi(a)\leq\varphi(ab)$

(ii) Untuk setiap a, $b\in D$, $a\neq 0$ terdapat q, $r\in D$, $a\neq 0$ sehingga $a=b\,q+r$ dengan $r=0$ atau $\varphi(r)<\varphi(b)$.

Contoh 10.14:

Z dengan pemetaan $\varphi(a)=|a|$ merupakan daerah Euclid. Jika F *field*, maka $F[x]$ merupakan daerah Euclid dengan pemetaan $\varphi(f(x))=\alpha(f(x))$.

Teorema 10.11

Misalkan D daerah Euclid dan $a\in D-\{0\}$. Maka:

(*i*) $\varphi(1)\leq\varphi(a)$

(ii) $\varphi(1)=\varphi(a)$ jika dan hanya jika a unsur satuan.

Bukti:

(*i*) Karena $a=a\cdot 1$ maka $\varphi(1)\leq\varphi(1\cdot a)=\varphi(a)$

(ii) Misalkan $\varphi(1)=\varphi(a)$

Karena 1, $a\in D$, maka terdapat q, $r\in D$ sehingga $1=aq+r$ dengan $r=0$ atau $\varphi(r)<\varphi(a)$.

Karena $\varphi(a)=1$, maka $r=0$ atau $\varphi(r)<1$. Akan tetapi karena $\varphi(1)\leq\varphi(x)$ untuk setiap $x\in D-\{0\}$, maka tidak mungkin terjadi $r\neq 0$ dengan $\varphi(r)<1$. Dengan demikian $r=0$. Jadi, $1=aq$, sehingga dapat disimpulkan bahwa a unsur satuan.

Misalkan a unit, maka terdapat $b\in D$ sehingga $ab=1$. Akibatnya, $\varphi(a)\leq\varphi(ab)=\varphi(1)$.
Akan tetapi berdasarkan (i), di mana $\varphi(1)\leq\varphi(a)$.
Dengan demikian diperoleh $\varphi(a)=\varphi(1)$.

Teorema 10.12

Setiap daerah Euclid merupakan daerah ideal utama.

Bukti:

Misalkan D daerah Euclid dengan pemetaan φ dan N ideal di D. Jika $N=\{0\}$, maka $N=\langle 0\rangle$, sehingga N merupakan ideal utama.
Misalkan $N\neq\{0\}$.
Dibentuk $S=\{\varphi(a)|a\in N-\{0\}\}$. Karena $S\subset Z^+$ maka terdapat elemen minimal di S. Misalkan $\varphi(b)$ elemen minimal di S.
Akan ditunjukkan $N=\langle b\rangle$.
Ambil sembarang $x\in N$. Maka terdapat q, $r\in D$ sehingga $x=bq+r$ dengan $r=0$ atau $\varphi(r)<\varphi(b)$. Dari $x=bq+r$ diperoleh $r=x\text{-}bq$.
Karena x, $a\in N$ dan N ideal, maka $r=x-bq\in N$.
Karena $\varphi(b)$ elemen minimal di S, maka tidak mungkin $\varphi(r)<\varphi(b)$.
Jadi, $r=0$. Akibatnya, $x=bq$, sehingga $x\in\langle b\rangle$. Dengan demikian, $N\subset\langle b\rangle$.
Akan tetapi, karena $a\in N$, maka $\langle b\rangle\subset N$.
Jadi, $N=\langle b\rangle$, sehingga N merupakan ideal utama.

Karena setiap ideal di D merupakan ideal utama, maka D merupakan daeraah ideal utama.

Contoh 10.15:

Z dengan pemetaan $\varphi(a)=|a|$ merupakan daerah Euclid. Berdasarkan teorema sebelumnya, Z merupakan daerah ideal utama. Setiap ideal di Z berbentuk nZ.

Teorema 10.13 (Algoritma Euclid)

Misalkan D daerah Euclid dengan fungsi φ dan a, $b \in D - \{0\}$. Berdasarkan syarat ke (ii) pada teorema sebelumnya yang berbunyi $\varphi(1) = \varphi(a)$ jika dan hanya jika a unsur satuan, dari daerah Euclid diperoleh:

$a = bq_1 + r_1$ dengan $r = 0$ atau $\varphi(r_1) < \varphi(b)$. Jika $r_1 \neq 0$, maka $b = r_1 q_2 + r_2$ dengan $r_2 = 0$ atau $\varphi(r_2) < \varphi(r_2)$.

Secara umum, $r_{i-1} = r_i q_{i+1} + r_{i+1}$ dengan $r_{i+1} = 0$ atau $(r_{i+1}) < \varphi(r_i)$. Maka:

(i) Terdapat s sehingga $r_s = 0$

(ii) Jika $r_1 = 0$, maka $(a, b) = b$

(iii) Misalkan $r_1 \neq 0$. Jika r_s bilangan pertama bernilai 0 dari r_1, r_2, ... maka $(a, b) = r_{s-1}$

(iv) Jika $(a, b) = d$ maka terdapat m, $n \in Z$ sehingga $d = ma + nb$.

Bukti:

(i) Karena $\varphi(r_i) < \varphi(r_{i-1})$ dan $\varphi(r_i)$ bilangan bulat tak negatif, maka setelah beberapa langkah diperoleh $r_s = 0$ untuk suatu $s \in Z^+$.

(ii) Jika $r_1 = 0$ maka $a = bq_1$ sehingga $(a, b) = b$.

Bukti (iii) dan (iv) diserahkan kepada pembaca sebagai latihan.

Teorema 10.14

Algoritma Euclid berlaku dalam $F[x]$ yaitu untuk sembarang polinomial $a(x)$, $b(x)$ dengan $b(x)$ mempunyai koefisien $b_n \neq 0$, barisan perulangan dari algoritma pembagian dapat dinyatakan sebagai berikut:

$a(x) \ = b(x)\, q_1\, (x) + r_1\, (x),$

$b(x) \ = r_1\, (x)\, q_2\, (x) + r_2\, (x),$

$r_1\, (x) = r_2\, (x)\, q_3\, (x) + r_3\, (x),$

....

....

Dengan $(a,b) = b_{n-1}$ atau (a,b) sama dengan sisa pembagian yang terakhir yang tidak nol dibagi dengan koefisien pemimpin untuk membuat polinomial monik.

Contoh 10.16

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 $a=b(x)$

$x^2=a-(x^4+x^3+x)b$

ekuivalen dengan

$[1 - (x^4+x^3+x)]$

kemudian

$x=b-(x+1)x^2$

ekuivalen dengan

$[0\ \ 1]-(x+1)[1-(x^4+x^3+x)]$

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 $(x+1)$ *mod* 2, maka diperoleh:

$x=(x+1)a+(x^5+x^3+x^2+x+1)b$

Teorema 10.15

Jika F adalah *field*, maka ring polinomial $F[x]$ adalah daerah Euclid (*Euclidean* domain).

Bukti:

$F[x]$ adalah integral domain. Didefinisikan: v: $F[x]\rightarrow Z^{\#}$ dengan

$$v(f(x)) = \deg f(x)$$

Untuk semua $f(x)\in F[x]\backslash\{0\}$. Karena $\deg f(x)\geq 0$, $v(f(x))\in Z^{\#}$ untuk semua $f(x)\in F[x]\backslash\{0\}$. Misalkan $f(x)$, $g(x)\in F[x]$, $g(x)\neq 0$, terdapat $q(x)$, $r(x)\in F[x]$ sehingga:

$f(x)=q(x)g(x)+r(x)$, di mana antara $r(x)=0$ atau $\deg r(x)<\deg g(x)$.

Karenanya,

$f(x)=q(x)g(x)+r(x)$, di mana antara $r(x)=0$ atau $v(r(x))<v(g(x))$.

Misalkan

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n,\ a_n \neq 0$$

dan

$$g(x) = b_0 + b_1 x + \ldots + b_m x^m,\ b_m \neq 0$$

maka

$$f(x)g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots + a_n b_m x^{n+m}$$

Karena F adalah *field* dan $a_n \neq 0$, $b_m \neq 0$, kita menemukan bahwa $a_n b_m \neq 0$. Hal ini berimplikasi bahwa deg $(f(x)g(x)) = n + m$. Sehigga $v(f(x)) = \deg(f(x)) = n \leq n + m = \deg(f(x)g(x)) = v(r(x))v(g(x))$.

Oleh karena itu, $F[x]$ adalah daerah Euclid (Euclidean domain).

Contoh 10.17:

Setiap *field* dapat menjadi sebuah daerah Euclid dengan $v(a) = 1$ untuk semua $a \neq 0$. Dengan kata lain $(a = (ab^{-1})\ b + 0)$.

Definisi 10.8

Himpunan bagian $Z[i] = \{a + bi | a, b \in Z\}$ dari bilangan kompleks disebut himpunan bilangan bulat Gaussian (*Gaussian Integers*).

Teorema 10.16:

Himpunan $Z[i]$ dari bilangan bulat Gaussian adalah subring dari C. Unsur satuan (unit) dari $Z[i]$ adalah ± 1 dan $\pm i$.

Bukti:

Hal tersebut mudah untuk membuktikan bahwa $Z[i]$ adalah subring dari C. Karena C adalah sebuah *field*, $Z[i]$ pasti merupakan daerah integral.

Misalkan $a + bi$ adalah unsur satuan dari $Z[i]$, maka terdapat $c + di \in Z[i]$ sehingga: $(a + bi)(c + di) = 1$. Hal ini berimplikasi bahwa:

$$1 = \overline{1} = \overline{(a+bi)(c+di)} = \overline{(a+bi)}\,\overline{(c+di)} = (a-bi)(c-di)$$

di mana *bar* dinotasikan dengan konjugasi kompleks (*complex conjugate*). Sehingga: $1 = (a^2 + b^2)(c^2 + d^2)$ dan karena $1 = (a^2 + b^2)$. Karenanya, $a = 0$, $b = \pm 1$, atau $a = \pm 1$, $b = 0$, terbukti bahwa hanya unsur satuan dari $Z[i]$ adalah ± 1, $\pm i$.

Teorema 10.17

Ring $Z[i]$ dari Gaussian integers menjadi sebuah daerah Euclid ketika kita memisalkan fungsi:

$$N: Z[i]\backslash\{0\} \to Z^{+}$$

Didefinisikan dengan $N(a+bi)=(a+bi)(a-bi)=a^2+b^2$ untuk semua a, $b\in Z$, disajikan sebagai fungsi v.

Bukti:

Secara jelas bahwa $N(a+bi)$ adalah bilangan bulat positif untuk setiap elemen yang bukan nol $a+bi\in Z[i]$. Misalkan $a+bi$, $c+di \in Z[i]\backslash\{0\}$. Selanjutnya,

$$\begin{aligned} N((a+bi)(c+di)) &= N(ac-bd+(bc+ad)i) \\ &= (ac-bd)^2+(bc+ad)^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= N((a+bi)(c+di)) \end{aligned}$$

Dari sini, dapat menunjukkan bahwa $N(a+bi) \leq N((a+bi)(c+di))$.

Hal itu, tetap memperlihatkan bahwa untuk $a+bi$ dan $c+di\neq 0$ dalam $Z[i]$, terdapat $q_0+q_1 i$, $r_0+r_1 i\in Z[i]$ sehingga:

$$a+bi=(q_0+q_1 i)(c+di)+(r_0+r_1 i)$$

di mana $r_0+r_1 i=0$ atau $N(r_0+r_1 i)<N(c+di)$. Kita bekerja ke belakang untuk memperlihatkan pemilihan $q_0+q_1 i$. Jika terdapat sebuah elemen $q_0+q_1 i$, maka dalam C

$$\begin{aligned} r_0+r_1{}^{i} &= (a+bi)-(c+di)(q_0+q_1 i) \\ &= (c+di)[(a+bi)\,(c+di)^{-1}\,(q_0+q_1{}^{i})] \end{aligned}$$

Misalkan $(a+bi)\,(c+di)^{-1}=u+vi$, di mana u dan v adalah bilangan rasional. Maka,

$$\begin{aligned} r_0+r_1{}^{i} &= (c+di)[(u+vi)-(q_0+q_1 i)] \\ &= (c+di)[(u-q_0)+(v-q_1)i] \\ &= [c(u-q_0)-d(v-q_1)]+[c(v-q_1)-d(u-q_0)]i \end{aligned}$$

Selanjutnya,

$$\begin{aligned} N(r_0+r_1{}^{i}) &= [c(u-q_0)-d(v-q_1)]^2+[c(v-q_1)-d(u-q_0)]^2 \\ &= (c^2+d^2)[(u-q_0)^2+(v-q_1)^2] \end{aligned}$$

Oleh karena itu, $N(r_0+r_1{}^{i})<N(c+di)$ jika $(u-q_0)^2+(v-q_1)^2<1$. Kita sekarang menentukan sebuah elemen $q_0+q_1 i\in Z[i]$ sehingga ketidaksamaan yang terakhir berlaku. Ambil bilangan bulat q_0 dan q_1 sehingga $(u-q_0)^2 \leq \frac{1}{4}$ dan $(v-q_1)^2 \leq \frac{1}{4}$. Maka $(u-q_0)^2+(v-q^1)^2<1$.

Misalkan:

$$r_0 + r_1{}' = (a+bi) - (c+di)(q_0 + q_1{}')$$

maka $a+bi=(c+di)(q_0+q_1{}')+(r_0+r_1{}')$, di mana r_0+r_1 $i=0$ atau $N(r_0+r_1{}')<N(c+di)$.

Definisi 10.9:

Misalkan R sebuah ring komutatif dengan elemen 1. Jika setiap ideal dari R adalah ideal principal, maka R disebut sebuah *ring ideal principal* (*principal ideal ring*). Sebuah integral domain yang juga ring *ideal principal* disebut sebuah daerah *ideal principal* (*principal ideal domain*).

Teorema 10.18:

Setiap daerah Euclid adalah *Principal Ideal Domain* (PID)

Bukti:

Misalkan E adalah daerah Euclid dengan nilai Euclid v. Kita ingin menunjukkan setiap ideal di E adalah *ideal principal*. Misalkan I adalah ideal di E. Karena E adalah ring komutatif dengan elemen 1, cukup menunjukkan $I=Ea$ untuk $a\in E$. Jika I adalah ideal nol, maka $I=E0$. Sekarang, perhatikan $I\neq\{0\}$. Maka I mengandung elemen tidak nol. Misalkan $P=\{v(x)|0\neq x\in I\}$. Ini adalah himpunan tidak kosong dari bilangan bulat tidak negatif. Dengan menggunakan prinsip yang baik, kita menemukan bahwa P mengandung sebuah elemen terkecil. Oleh karena itu, terdapat sebuah elemen $a\in I$, $a\neq 0$ sehingga $v(a)\geq 0$ dan $v(a)\leq v(b)$ untuk semua $b\in I$, $b\neq 0$. Kita sekarang menunjukkan bahwa $I=Ea$. Karena I adalah sebuah ideal dan $a\in I$, itu menunjukkan bahwa $Ea\subseteq I$. Misalkan $b\in I$, karena E adalah daerah Euclid, terdapat q, $r\in E$ sehingga $b=aq+r$, dimana $r=0$ atau $v(r)<v(a)$. Selanjutnya, $r=b-qa\in I$. Jika $r\neq 0$, maka $v(r)\in P$. Hal ini kontradiksi minimalitas dari $v(a)$ karena $v(r)<v(a)$. Oleh karena itu, $r=0$ dan juga $b=qa\in Ea$. Hal ini membuktikan bahwa $I\subseteq Ea$. Karena $I=Ea$.

Teorema 10.19

Misalkan R adalah ring komutatif dengan elemen 1. Tunjukkan kondisi berikut ekuivalen.

(*i*) R adalah *field*

(ii) $R[x]$ adalah daerah Euclid

(iii) $R[x]$ adalah PID

Bukti:

Misalkan $a \in R$ dan $a \neq 0$. Pertimbangkan $I = \langle a, x \rangle$, ideal dari $R[x]$ dihasilkan dengan a dan x. Karena $R[x]$ adalah PID, terdapat $f(x) \in R[x]$ sehingga $I = \langle f(x) \rangle$. Selanjutnya, a, $x \in \langle f(x) \rangle$. Oleh karena itu, terdapat $g(x)$ dan $h(x)$ dalam $R[x]$ sehingga $f(x)g(x) = a$ dan $f(x)h(x) = x$. Karena $f(x)$ $g(x) = a$, kita harus memiliki $\deg f(x) = 0$ dan juga $f(x) \in R$. Misalkan $f(x) = b$, selanjutnya $bh(x) = x$ berimplikasi bahwa $bc = 1$ untuk beberapa $c \in R$. Dengan demikian, b adalah unit dan juga $I = \langle b \rangle = R[x]$. Dari sini, kita memiliki $1 \in I$. Oleh karena itu, $1 = af_1(x) + xf_2(x)$ untuk beberapa $f_1(x)$, $f_2(x) \in R[x]$. Hal ini beramplikasi bahwa $1 = da$ untuk beberapa $d \in R$. Oleh karena itu, a adalah sebuah unsur satuan (unit) dalam R dan juga R adalah sebuah *field*.

Contoh 10.18:

Misalkan n adalah bilangan bulat bebas kuadrat (sebuah bilangan bulat yang berbeda dari 0 dan 1, yang tidak habis dibagi bilangan bulat kuadrat manapun. Misalkan $Z\left[\sqrt{n}\right] = \left\{a + b\sqrt{n} \mid a, b \in Z\right\}$. Tunjukkan bahwa $Z\left[\sqrt{n}\right]$ adalah daerah integral. Didefinisikan $N : Z\left[\sqrt{n}\right] \to Z^{\#}$ dengan:

$$N\left(a + b\sqrt{n}\right) = \left(a + b\sqrt{n}\right)\left(a - b\sqrt{n}\right) = a^2 - nb^2$$

a) Misalkan $x \in Z\left[\sqrt{n}\right]$. Buktikan bahwa $N(x) = 0$ jika dan hanya jika $x = 0$.

b) Buktikan bahwa $N(xy) = N(x)N(y)$ untuk semua $x, y \in Z\left[\sqrt{n}\right]$.

c) Misalkan $x \in Z\left[\sqrt{n}\right]$. Buktikan bahwa $N(x) = \pm 1$ jika dan hanya jika x adalah sebuah unit (unsur satuan) dalam $Z\left[\sqrt{n}\right]$.

Penyelesaian:

Misalkan $x = \left(a + b\sqrt{n}\right)$ dan $y = \left(c + d\sqrt{n}\right)$ adalah dua elemen dalam $Z\left[\sqrt{n}\right]$. Selanjutnya, $x - y = (a - c) + (b - d)\sqrt{n} \in Z\left[\sqrt{n}\right]$ dan $xy = (ac + nbd) + (ad + bc)\sqrt{n} \in Z\left[\sqrt{n}\right]$.

Kita memiliki $0 = 0 + 0\sqrt{n} \in Z\left[\sqrt{n}\right]$ dan $1 = 1 + 0\sqrt{n} \in Z\left[\sqrt{n}\right]$. Selanjutnya, dengan mudah diperiksa bahwa $Z\left[\sqrt{n}\right]$ adalah daerah integral (*integral domain*).

a) Misalkan $x = \left(a + b\sqrt{n}\right)$, maka $N(x) = a^2 - nb^2$. Seharusnya, $N(x) = 0$.

Jika $b \neq 0$, maka $n = \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2$, yang kontradiksi dengan assumsi bahwa n adalah bilangan bulat bebas kuadrat. Oleh karena itu, $a = 0$ dan $b = 0$, maka $x = 0$. Hal ini berbanding terbalik.

b) Misalkan $x = \left(a + b\sqrt{n}\right)$ dan $y = \left(c + d\sqrt{n}\right)$.
Selanjutnya,

$$\begin{aligned}
N(xy) &= \left[(ac + nbd) + (ad + bc)\sqrt{n}\right]\left[(ac + nbd) - (ad + bc)\sqrt{n}\right] \\
&= (ac + nbd)^2 - (ad + bc)^2 n \\
&= a^2c^2 + n^2b^2d^2 - a^2d^2n - b^2c^2n \\
&= \left(a^2 - nb^2\right)\left(c^2 - nd^2\right) \\
&= N(x)N(y)
\end{aligned}$$

c) Misalkan $x = a + b\sqrt{n}, N(x) = \pm 1$ jika dan hanya jika: $\left(a + b\sqrt{n}\right)\left(a - b\sqrt{n}\right) = \pm 1$ jika dan hanya jika $a + b\sqrt{n}$ membagi 1, yaitu jika $a + b\sqrt{n}$ dan hanya jika adalah unit (unsur satuan) dalam $Z\left[\sqrt{n}\right]$.

Contoh 10.19:

Tunjukkan bahwa $Z\left[\sqrt{n}\right]$ adalah daerah Euclid untuk $n = -1, -2, 2, 3$.

Penyelesaian:

Berdasarkan definisi $v : Z\left[\sqrt{n}\right] \setminus \{0\} \to Z^{\#}$ dengan $v\left(a + b\sqrt{n}\right) = \left|N\left(a + b\sqrt{n}\right)\right|$ Misalkan . Selanjutnya,

$$\begin{aligned}
v\left(\left(a + b\sqrt{n}\right)\left(c + d\sqrt{n}\right)\right) &= \left|N\left(\left(a + b\sqrt{n}\right)\left(c + d\sqrt{n}\right)\right)\right| \\
&= \left|\left(a^2 - nb^2\right)\left(c^2 - nd^2\right)\right| \\
&= \left|\left(a^2 - nb^2\right)\right|\left|\left(c^2 - nd^2\right)\right| \\
&\geq \left|\left(a^2 - nb^2\right)\right| \\
&= v\left(\left(a + b\sqrt{n}\right)\right)
\end{aligned}$$

Misalkan $a + b\sqrt{n}, c + d\sqrt{n} \in Z\left[\sqrt{n}\right]$ dengan $c + d\sqrt{n} \neq 0$. Kita ingin menunjukkan bahwa terdapat $q_0 + q_1\sqrt{n}, r_0 + r_1\sqrt{n} \in Z\left[\sqrt{n}\right]$ sehingga:

$$\left(a+b\sqrt{n}\right) = \left(c+d\sqrt{n}\right)\left(q_0 + q_1\sqrt{n}\right) + \left(r_0 + r_1\sqrt{n}\right)$$

Di mana antara $r_0 + r_1\sqrt{n} = 0$ atau $\left|r_0^2 - nr_1^2\right| < \left|\left(c^2 - nd^2\right)\right|$. Kita bekerja ke belakang, untuk melihat bagaimana memilih $q_0 + q_1\sqrt{n}$. Jika ada sebuah elemen $q_0 + q_1\sqrt{n}$ terdapat dalam $Z\left[\sqrt{n}\right]$, kemudian dalam $Q\left[\sqrt{n}\right]$

$$\begin{aligned} r_0 + r_1\sqrt{n} &= \left(a+b\sqrt{n}\right) - \left(c+d\sqrt{n}\right)\left(q_0 + q_1\sqrt{n}\right) \\ &= \left(c+d\sqrt{n}\right)\left[\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right)^{-1} - \left(q_0 + q_1\sqrt{n}\right)\right] \end{aligned}$$

Misalkan $\left(a+b\sqrt{n}\right)\left(c+d\sqrt{n}\right)^{-1} = u + v\sqrt{n}$, di mana u dan v adalah bilangan rasional. Maka,

$$\begin{aligned} r_0 + r_1\sqrt{n} &= \left(c+d\sqrt{n}\right)\left[\left(u+v\sqrt{n}\right) - \left(q_0 + q_1\sqrt{n}\right)\right] \\ &= \left(c+d\sqrt{n}\right)\left[\left(u-q_0\right) + \left(v-q_1\right)\sqrt{n}\right] \\ &= c\left[\left(u-q_0\right) + d\left(v-q_1\right)n\right] + \left[c\left(v-q_1\right) + d\left(u-q_0\right)\right]\sqrt{n} \end{aligned}$$

Selanjutnya

$$\begin{aligned} v\left(r_0 + r_1\sqrt{n}\right) &= \left|\left[c\left(u-q_0\right) + d\left(v-q_1\right)n\right]^2 + \left[c\left(v-q_1\right) + d\left(u-q_0\right)\right]^2 n\right| \\ &= \left|\left(c^2 - nd^2\right)\left[\left(u-q_0\right)^2 - n\left(v-q_1\right)^2\right]\right| \\ &< \left|\left(c^2 - nd^2\right)\right| \end{aligned}$$

Jika $\left|\left(u-q_0\right)^2 - n\left(v-q_1\right)^2\right| < 1$. Kita sekarang menemukan sebuah elemen $q_0 + q_1\sqrt{n} \in Z\left[\sqrt{n}\right]$ seperti $\left|\left(u-q_0\right)^2 - n\left(v-q_1\right)^2\right| < 1$.

Ambil bilangan bulat q_0 dan q_1 seperti $\left(u-q_0\right)^2 \le \frac{1}{4}$ dan $\left(v-q_1\right)^2 \le \frac{1}{4}$.
Untuk $n = -1$ atau -2,

$$\left|\left(u-q_0\right)^2 - n\left(v-q_1\right)^2\right| \le \frac{1}{4} + (-n)\frac{1}{4} < 1$$

Untuk $n = 2$ atau 3,

$$-\frac{n}{4} \le \left(u-q_0\right)^2 - n\left(v-q_1\right)^2 \le \frac{1}{4}$$

Maka $\left|(u-q_0)^2 - n(v-q_1)^2\right| < 1$ untuk $n = -1,\ -2$,atau $2,\ 3$. Oleh karena itu, terdapat $q_0 + q_1\sqrt{n}, r_0 + r_1\sqrt{n} \in Z\left[\sqrt{n}\right]$. Sehingga:

$$\left(a + b\sqrt{n}\right) = \left(c + d\sqrt{n}\right)\left(q_0 + q_1\sqrt{n}\right) + \left(r_0 + r_1\sqrt{n}\right)$$

Di mana antara $r_0 + r_1\sqrt{n} = 0$ atau $\left|r_0^2 - nr_1^2\right| < \left|\left(c^2 - nd^2\right)\right|$.

Contoh 10.20:

Misalkan $Z\left[i\sqrt{3}\right] = \left\{a + bi\sqrt{3} | a,b \in Z\right\}$ .Didefinisikan $v : Z\left[i\sqrt{3}\right] \setminus \{0\} \to Z^{\#}$ dengan $v\left(a + bi\sqrt{3}\right) = a^2 + 3b^2$. Tunjukkan bahwa v bukan nilai Euclid dalam $Z\left[i\sqrt{3}\right]$

Penyelesaian:

Akan dibuktikan v adalah nilai Euclid. Sekarang 2 dan $1 + i\sqrt{3}$ adalah elemen dari $Z\left[i\sqrt{3}\right]$. Seharusnya, terdapat $q_0 + q_1 i\sqrt{3}, r_0 + r_1 i\sqrt{3} \in Z\left[i\sqrt{3}\right]$, sehingga:

$$2 = \left(1 + i\sqrt{3}\right)\left(q_0 + q_1 i\sqrt{3}\right) + \left(r_0 + r_1 i\sqrt{3}\right)$$

Di mana antara $r_0 + r_1 i\sqrt{3} = 0$ atau $r_0^2 + 3r_1^2 < 4$. Jika , maka:

$$2 = \left(1 + i\sqrt{3}\right)\left(q_0 + q_1 i\sqrt{3}\right)$$

Hal ini berimplikasi pada:

$$4 = v(2) = v\left(\left(1 + i\sqrt{3}\right)\left(q_0 + q_1 i\sqrt{3}\right)\right) = 4\left(q_0^2 + 3q_1^2\right)$$

.

Maka $q_0^2 + 3q_1^2 = 1$, yang menunjukkan bahwa $q_0 = \pm 1, q_1 = 0$. Sebagai hasilnya, $2 = 1 + i\sqrt{3}$ atau $2 = -1\left(1 + i\sqrt{3}\right)$, sebuah kontradiksi. Seharusnya sekarang $r_0^2 + 3r_1^2 < 4$. Maka $r_0^2 + 3r_1^2 = 1, 2$ atau 3 . Karena r_0 dan r_1 adalah bilangan bulat $r_0^2 + 3r_1^2 \neq 2$. Seharusnya $r_0^2 + 3r_1^2 = 1$. Maka, $r_0 = \pm 1, r_1 = 0$. Sehingga:

$$2 = \left(1 + i\sqrt{3}\right)\left(q_0 + q_1 i\sqrt{3}\right) + \left(r_0 + r_1 i\sqrt{3}\right)$$

di mana

$$2 = q_0 - 3q_1 + r_0$$

dan

$$0 = q_1 + q_0 + r\_1$$

Jika $r_0 = 1$ dan $r_1 = 0$, maka $q_0 - 3q_1 = 1$ dan $q_1 + q_0 = 0$. Hal ini berimplikasi kepada $-2q_1 = 1$, yang tidak mungkin. Demikian pula, untuk setiap kasus yang tersisa, kita dapat menunjukkan kontradiksi. Juga dari $r_0^2 + 3r_1^2 = 3$, kita juga menunjukkan kontradiksi. Oleh karena itu, bukan nilai *Euclidean* dalam $Z\left[i\sqrt{3}\right]$.

10.3 BILANGAN ALJABAR

Jika K adalah *field extension* dari F, elemen $k \in K$ disebut **aljabar** pada F jika terdapat $a_0, a_1, \ldots, a_n \in F$, yang semuanya tidak nol, sehingga:

$$a_0 + a_1 k + \ldots + a_n k^n = 0$$

Dengan kata lain, k adalah akar dari sebuah polinomial yang bukan nol di $F[x]$. Elemen yang bukan aljabar pada F disebut **transcendental** pada F.

Contoh 10.21:

$5, \sqrt{3}, i, \sqrt[n]{7} + 3$ semuanya adalah algebraic pada Q, karena mereka adalah akar-akar polinom $x - 5, x^2 - 3, x^2 + 1, (x-3)^n - 7$.

Contoh 10.22:

Tentukan sebuah polinomial dalam $Q[x]$ dengan $\sqrt[3]{2} + \sqrt{5}$ sebagai akarnya.

Penyelesaian:

Misalkan $x = \sqrt[3]{2} + \sqrt{5}$. kita harus mengeliminasi akar pangkat dua dan pangkat tiga dari persamaan ini. Kita memiliki $x - \sqrt{5} = \sqrt[3]{2}$, sehingga $\left(x - \sqrt{5}\right)^3 = 2$ atau $x^3 - 3\sqrt{5}x^2 + 15x - 5\sqrt{5} = 2$. Karena itu, $x^3 + 15x - 2 = \sqrt{5}\left(3x^2 + 5\right)$, jadi $(x^3 + 15x - 2)^2 = 5(3x^2 + 5)^2$. Oleh karena itu, $\sqrt[3]{2} + \sqrt{5}$ adalah akar dari polinomial $x^6 - 15x^4 - 4x^3 + 75x^2 - 60x - 121 = 0$.

Tidak semua bilangan riel dan kompleks adalah aljabar pada Q. Bilangan π dan e dapat dibuktikan *transcendental* pada Q. Karena π *transcendental*, kita memiliki:

$$Q(\pi) = \left\{ \frac{a_0 + a_1\pi + \ldots + a_n\pi^n}{b_0 + b_1\pi + \ldots + b_m\pi^m} \middle| a_i, b_j \in Q; \text{tidak semua } b_j \text{ adalah nol} \right\}$$

Contoh 10.23:

Apakah cos(2π/5) merupkan aljabar atau transcendental pada Q?

Penyelesaian:

Berdasarkan teorema De Moivre's, maka:

$$\left(\cos\frac{2\pi}{5}+i\sin\frac{2\pi}{5}\right)^5=\cos 2\pi+i\sin 2\pi=1$$

Ambil bagian riel dan tulis $c=\cos\frac{2\pi}{5}$ dan $=\sin\frac{2\pi}{5}$, sehingga kita memiliki:

$$(c-s)^5=c^5-10s^2c^3+5s^4c=1$$

Karena $s^2+c^2=1$ maka $s^2=1-c^2$, kita memiliki:

$$c^5-10\left(1-c^2\right)c^3+5\left(1-c^2\right)^2c=1$$

Bahwa $16c^5-20c^3+5c-1=0$ dan oleh karena itu, $c=\cos\frac{2\pi}{5}$ adalah aljabar pada Q.

Teorema 10.20

Misalkan α adalah aljabar pada F dan misalkan $p(x)$ polinomial tidak tereduksi dari derajat n pada F dengan α sebagai akar. Dengan demikian,

$$F(\alpha)\cong F[x]/(p(x))$$

dan elemen dari $F(\alpha)$ dapat ditulis dalam bentuk:
$c_0+c_1\alpha+c_2\alpha^2+\ldots+c_{n-1}\alpha^{n-1}$ di mana $c_i\in F$

Corollary 10.1

Jika α adalah akar dari polinomial $p(x)$ dari derajat n, tidak tereduksi pada F, dengan demikian $[F(\alpha):F]=n$.

Bukti:

Berdasarkan $[F(\alpha):F]=[F[x]/(p(x)):F]=n$

Contoh 10.24:

$$Q\left(\sqrt{2}\right)\cong Q[x]/\left(x^2-2\right)\text{dan}\left[Q\left(\sqrt{2}\right):Q\right]=2$$

$Q(\sqrt[4]{7}i) \cong Q[x]/(x^4 - 7)$ dan $[Q(\sqrt[4]{7}i) : Q] = 4$ karena $\sqrt[4]{7}i$ adalah akar dari $x^4 - 7$, yang tidak tereduksi pada Q.

Lemma 10.1

Misalkan $p(x)$ adalah polinomial *irreducible* pada *field* F. Maka F memiliki sebuah *finite field extension* k dalam $p(x)$ memiliki sebuah akar.

Bukti:

Misalkan $p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$ dan dinotasikan ideal $(p(x))$ dengan P. Dengan $K = F[x]/P$ adalah *field extension* dari F derajat n di mana elemen koset berbentuk $P + f(x)$. Elemen $P + x \in K$ adalah akar dari $p(x)$ karena:

$$\begin{aligned}
&a_0 + a_1 (P+x) + a_2 (P+x)^2 + \ldots + a_n (P+x)^n \\
&= a_0 + (P + a_1 x) + (P + a_2 x^2) + \ldots + (P + a_n x^n) \\
&= P + (a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n) \\
&= P + p(x) \\
&= P + 0
\end{aligned}$$

dan ini adalah elemen nol dari *field* K.

Teorema 10.21

Jika $f(x)$ adalah setiap polinomial pada *field* F, ada sebuah *extension field* K dari F di mana $f(x)$ terpisah dalam faktor linier.

Contoh 10.25:

Temukan $\left[Q\left(\cos\frac{2\pi}{5}\right) : Q\right]$

Penyelesaian:

Pada contoh sebelumnya, kita ketahui bahwa $\cos\frac{2\pi}{5}$ merupakan aljabar pada Q dan akar polinomial $16x^5 - 20x^3 + 5x - 1$. Dengan menggunakan cara yang sama, kita dapat menunjukkan bahwa $\cos\frac{2k\pi}{5}$ juga merupakan akar dari persamaan untuk setiap $k \in Z$.

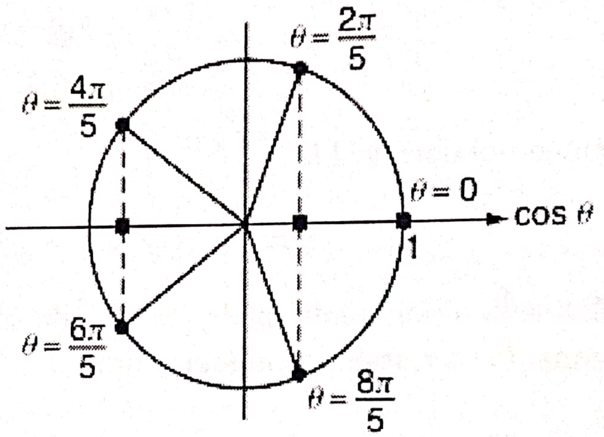
Akar-akar nya adalah 1, $\cos\frac{2\pi}{5} = \cos\frac{8\pi}{5}$, dan $\cos\frac{4\pi}{5} = \cos\frac{6\pi}{5}$. Oleh karena itu, $(x - 1)$ adalah faktor dari polinomial dan

$$16x^5 - 20x^3 + 5x - 1 = (x-1)\left(16x^4 + 16x^3 - 4x^2 - 4x + 1\right)$$
$$= (x-1)\left(4x^2 + 2x - 1\right)^2$$

Itu menunjukkan bahwa $\cos\frac{2\pi}{5}$ dan $\cos\frac{4\pi}{5}$ adalah akar-akar dari kuadrat $4x^2 + 2x - 1$ jadi dengan rumus kuadrat, akar-akar ini adalah $\frac{\left(-1 \pm \sqrt{5}\right)}{4}$. Karena $\cos\frac{2\pi}{5}$ positif, maka:

$$\cos\frac{2\pi}{5} = \frac{\left(\sqrt{5}-1\right)}{4} \text{ dan } \cos\frac{4\pi}{5} = \frac{\left(-\sqrt{5}-1\right)}{4}$$

Oleh karena itu, $Q\left(\cos\frac{2\pi}{5}\right) \cong Q[x]/\left(4x^2 + 2x - 1\right)$ karena $4x^2 + 2x - 1$ adalah *irreducible* pada Q. Berdasarkan *Corollary* di atas, $\left[Q\left(\cos\frac{2\pi}{5}\right) : Q\right] = 2$.



GAMBAR 10.1. Nilai dari $\cos\left(\frac{2k\pi}{5}\right)$

RANGKUMAN

1. Andaikan D merupakan integral domain dan $a,b \in D$. Jika terdapat $c \in D$ sehingga $b = ac$, maka dikatakan a membagi b (a faktor dari b) atau dapat ditulis dengan $a|b$. Simbol $a \nmid b$ menyatakan a tidak habis membagi b.
2. Diketahui $a = a(x)$ dan $b = b(x)$ elemen $F[x]$ yang tidak nol. Faktor persekutuan terbesar (greatest common divisor) dari a dan b (dinotasikan dengan (a,b)) adalah polinomial monik $d = d(x)$ sehingga:
   (i) d membagi a dan b

(ii) Jika c sembarang elemen $F[x]$ yang membagi a dan b, maka c membagi d.

3. Jika diketahui $a(x)$ dan $b(x)$ dalam $F[x]$, maka $a(x)$ dan $b(x)$ mempunyai FPB dalam $F[x]$ dan terdapat polinomial $s(x)$ dan $t(x)$ dalam $F[x]$ sehingga:

$$s(x)a(x)+t(x)b(x)=d(x)$$

4. Misalkan D daerah integral dan a, $b \in D$. Dimana a dan b dikatakan berasosiasi apabila terdapat unit $u \in D$, sehingga $a=bu$.
5. Misalkan D daerah integral, $p \in D - \{0\}$ dan p bukan unsur satuan. p dinamakan elemen tidak tereduksi (*irreducible*) atas D jika setiap faktorisasi $p=ab$ mengakibatkan a atau b unsur satuan. Jika p dapat difaktorkan menjadi $p=ab$ dengan a,b bukan unsur satuan, maka p dinamakan elemen tereduksi.
6. Misalkan D adalah daerah ideal utama. Jika $N_1 \subset N_2 \subset$ merupakan ideal ideal-ideal di D, maka terdapat bilangan bulat positif r sehingga $N_r = N_s$ untuk semua $s \geq r$.
7. Misalkan D daerah ideal utama. Jika $a \in D - \{0\}$, a bukan unit maka a dapat dinyatakan sebagai hasil kasil elemen-elemen tak tereduksi.
8. Misalkan D daerah integral dan $p \in D$, maka $\langle p \rangle$ merupakan ideal maksimal jika dan hanya jika p elemen tidak tereduksi.
9. Misalkan D daerah ideal utama dan p, a, $b \in D$. Jika p tidak tereduksi dan $p|ab$, maka $p|ab$ atau $p|b$.
10. Misalkan D daerah ideal utama dan $p \in D$ elemen tidak tereduksi. Jika $p|a_1\ a_2 \ldots \mathrm{a_n}$ dengan $a_i \in D$, maka $p|a_i$ untuk paling sedikit satu nilai i.
11. Misalkan D daerah integral dan $p \in D - \{0\}$, p bukan unsur satuan, p dinamakan elemen prima jika $p|ab$ maka $p|a$ atau $p|b$.
12. Setiap daerah ideal utama merupakan daerah faktorisasi tunggal.
13. Jika $f(x)$ dan $g(x)$ polinomial primitif dalam $Z[x]$ maka hasil kalinya $f(x)g(x)$ juga polinomial primitif.
14. Himpunan polinomial $Z[x]$ merupaka daerah faktorisasi tunggal.
15. 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 $\mathrm{a_n}$ dan p^2 tidak membagi a_0, maka $g(x)$ tidak tereduksi atas Q.
16. Suatu daerah integral D dinamakan daerah Euclid jika terdapat pemetaan: $\varphi: D - \{0\} \rightarrow Z^+ \cup \{0\}$ sehingga memenuhi:

(i) Untuk setip $a, b \in D - \{0\}$, $\varphi(a) \leq \varphi(ab)$

(ii) Untuk setiap $a, b \in D$, $a \neq 0$ terdapat $q, r \in D, a \neq 0$ sehingga $a = bq + r$ dengan $r = 0$ atau $\varphi(r) < \varphi(b)$.

17. Misalkan D daerah Euclid dan $a \in D - \{0\}$. Maka:

(i) $\varphi(1) \leq \varphi(a)$

(ii) $\varphi(1) = \varphi(a)$ jika dan hanya jika a unsur satuan.

18. Setiap daerah Euclid merupakan daerah ideal utama.

19. Misalkan D daerah Euclid dengan fungsi φ dan $a, b \in D - \{0\}$. Berdasarkan syarat ke (ii) pada teorema sebelumnya yang berbunyi $\varphi(1) = \varphi(a)$ jika dan hanya jika a unsur satuan, dari daerah Euclid diperoleh: $a = b\text{-}q_1 + r_1$ dengan $r = 0$ atau $\varphi(r_1) < \varphi(b)$. Jika $r_1 \neq 0$, maka $b = r_1 q_2 + r_2$ dengan $r_2 = 0$ atau $\varphi(r_2) < \varphi(r_2)$. Secara umum, $r_{i-1} = r_i q_{i+1} + r_{i+1}$ dengan $r_{i+1} = 0$ atau $(r_{i+1}) < \varphi(r_i)$. Maka:

(i) Terdapat s sehingga $r_s = 0$

(ii) Jika $r_1 = 0$, maka $(a, b) = b$

(iii) Misalkan $r_1 \neq 0$. Jika r_s bilangan pertama bernilai 0 dari $r_1, r_2, \ldots$ maka $(a, b) = r_{s-1}$

(iv) Jika $(a,b) = d$ maka terdapat $m, n \in Z$ sehingga $d = ma + nb$.

20. Algoritma Euclid berlaku dalam $F[x]$ yaitu untuk sembarang polinomial $a(x)$, $b(x)$ dengan $b(x)$ mempunyai koefisien $b_n \neq 0$, barisan perulangan dari algoritma pembagian dapat dinyatakan sebagai berikut:

$$a(x) = b(x)q_1(x) + r_1(x),$$
$$b(x) = r_1(x)q_2(x) + r_2(x),$$
$$r_1(x) = r_2(x)q_3(x) + r_3(x),$$

....

....

Dengan $(a, b) = b_{n-1}$ atau (a,b) sama dengan sisa pembagian yang terakhir yang tidak nol dibagi dengan koefisien pemimpin untuk membuat polinomial monik.

21. Jika F adalah *field*, maka ring polinomial $F[x]$ adalah daerah Euclid (Euclidean domain).

22. Himpunan bagian $Z[i] = \{a + bi \mid a, b \in Z\}$ dari bilangan kompleks disebut himpunan bilangan bulat Gaussian (Gaussian Integers).

23. Himpunan $Z[i]$ dari bilangan bulat Gaussian adalah subring dari C.

Unsur satuan (unit) dari $Z[i]$ adalah ± 1 dan $\pm i$.

24. Ring $Z[i]$ dari Gaussian integers menjadi sebuah daerah Euclid ketika kita memisalkan fungsi:

$$N: Z[i]\backslash\{0\} \rightarrow Z^{\#}$$

Didefinisikan dengan $N(a+bi)=(a+bi)(a-bi)=a^2+b^2$ untuk semuaa, $b \in Z$, disajikan sebagai fungsi v.

25. Misalkan R sebuah ring komutatif dengan elemen 1. Jika setiap ideal dari R adalah *ideal principal*, maka R disebut sebuah ring ideal principal (*principal ideal ring*). Sebuah integral domain yang juga ring ideal principal disebut sebuah daerah ideal principal (principal ideal domain).
26. Setiap daerah Euclid adalah *Principal Ideal Domain* (PID)
27. Misalkan R adalah ring komutatif dengan elemen 1. Tunjukkan kondisi berikut ekuivalen.
    (i) R adalah *field*
    (ii) $R[x]$ adalah daerah Euclid
    (iii) $R[x]$ adalah PID
28. Jika K adalah *field extension* dari F, elemen $k \in K$ disebut aljabar pada F jika terdapat $a_0, a_1, \ldots, a_n \in F$, yang semuanya tidak nol, sehingga:

$$a_0 + a_1 k + \ldots + a_n k^n = 0$$

Dengan kata lain, k adalah akar dari sebuah polinomial yang bukan nol di $F[x]$. Elemen yang bukan aljabar pada F disebut transcendental pada F.

29. Misalkan α adalah aljabar pada F dan misalkan $p(x)$ polinomial tidak tereduksi dari derajat n pada F dengan α sebagai akar. Dengan demikian,

$$F(\alpha) \cong F[x]/(p(x))$$

dan elemen dari $F(\alpha)$ dapat ditulis dalam bentuk:

$$c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1} \text{ di mana } c_i \in F$$

30. Jika α adalah akar dari polinomial $p(x)$ dari derajat n, tidak tereduksi pada F, dengan demikian $[F(\alpha): F] = n$.
31. Misalkan $p(x)$ adalah *polinomial irreducible* pada *field* F. Maka F memiliki sebuah *finite field extension* K dalam $p(x)$ memiliki sebuah akar.
32. Jika $f(x)$ adalah setiap polinomial pada *field* F, ada sebuah *extension field* K dari F di mana $f(x)$ terpisah dalam faktor linier.

LATIHAN

1. Gunakan algoritma Euclid untuk menentukan FPB dari pasangan polinomial $x^5 - 4x$ dan $x^4 - 4$.
2. Tentukan FPB $d(x)$ jika diberikan $a(x)$ dan $b(x)$ atas Z_2 dan nyatakan $d(x)$ dalam bentuk $s(x)a(x) + t(x)b(x)$ jika diketahui:
$$a(x) = x^6 + x^3 + x^2 + x \text{ dan } b(x) = x^5 + x^4 + 1$$
3. Nyatakan faktorisasi dari polinomial $2x^3 + 21x^2 - 5$ atas Q.
4. Nyatakan faktorisasi dari polinomial $x^4 + x^3 + x + 1$ dan $x^5 + x + 1$ terhadap Z_2.
5. Buktikan bahwa $Z\left[\sqrt{3}\,i\right]$ bukan daerah ideal utama karena bukan daerah faktorisasi tunggal.

Untuk latihan nomor 6 sampai dengan 8, dalam setiap kasus, temukan sebuah polinomial dalam $F[x]$ dengan x sebagai sebuah akar.

6. $x = \sqrt{2} + \sqrt{6}, F = Q$
7. $x = \pi + ei, F = R$
8. $x = \dfrac{\sqrt[3]{3}}{\sqrt{2}}, F = Q$
9. Tunjukkan bahwa $\theta = 2k\pi/7$ dengan persamaan $\cos 4\theta - \cos 3\theta = 0$ untuk setiap bilangan bulat. Oleh karena itu, carilah sebuah polinomial yang tidak tereduksi pada Q dengan $\cos\left(\dfrac{2\pi}{7}\right)$ sebagai sebuah akar.
10. Buktikan bahwa bilangan aljabar $A = \{x \in C \mid x \text{ adalah aljabar pada } Q\}$ dari sebuah subfield dari C.
11. Temukan semua asosiasi dari $2 + x - 3x^2$ dalam $Z[x]$.
12. Tunjukkan bahwa [4] dan [6] adalah berasosiasi dalam Z_{10}.
13. Dalam $Z[i]$, temukan gcd$(2 - 7i, 2 + 11i)$. Selain itu, temukan x dan y dalam $Z[i]$ sehingga gcd$(2 - 7i, 2 + 11i) = x(2 - 7i) + y(2 + 11i)$
14. Dalam $Z\left[\sqrt{3}\right]$, untuk $9 + 5\sqrt{3}$ dan $1 + 7\sqrt{3}$, temukan $q_0 + q_1\sqrt{3}$, $r_0 + r_1\sqrt{3} \in Z\left[\sqrt{3}\right]$ sehingga:
$$9 + 5\sqrt{3} = \left(q_0 + q_1\sqrt{3}\right)\left(1 + 7\sqrt{3}\right) + r_0 + r_1\sqrt{3}$$
di manaantara $r_0 + r_1\sqrt{3} = 0$ atau $\left|r_0^2 + r_1^2\right| < 146$.
15. Perhatikan integral domain $Z[i]$. Temukan $q_0 + q_1 i, r_0 + r_1 i \in Z[i]$ sehingga:

$$3+7i=(q_0+q_1 i)(1+2i)+r_0+r_1 i$$

di mana antara $r_0+r_1 i=0$ atau $\left|r_0^2+r_1^2\right|<5$.

RENCANA TINDAK LANJUT

Setelah mahasiswa menjawab soal latihan pada setiap akhir bab, maka jawaban mahasiswa dikoreksi secara bersama-sama di kelas. Kemudian, masing-masing mahasiswa menghitung tingkat penguasaan materi dengan menggunakan rumus sebagai berikut:

$$\textit{Tingkat penguasaan}=\frac{\textit{Banyak jawaban yang benar}}{\textit{Banyak soal}}\times 100\%$$

Klasifikasikan tingkat penguasaan terhadap materi yang telah diajari dengan rentang nilai di bawah ini:

Rentang Nilai (%)	**Kategori**
90 – 100	Sangat Baik
80 – 89	Baik
70 – 79	Sedang
≤ 69	Kurang

Jika mahasiswa mendapatkan tingkat penguasaan materi ≥ 70%, maka mahasiswa tersebut dapat melanjutkan ke bab berikutnya. Namun, jika tingkat penguasaan mahasiswa berada pada rentang < 70%, maka mahasiswa tersebut dianjurkan untuk mengulang materi pada bab ini, terutama pada materi yang belum dikuasai.

DAFTAR PUSTAKA

Aslan Lubis. 2010. *Teori Gelanggang (Struktur Aljabar II)*. Medan: Fakultas Tarbiyah IAIN Sumatera Utara.

Fraleigh, J.B.. 1989. *A First Course in Abstract Algebra. Fourth Edition*. Canada: Addison-Wesley Publishing Company.

Frank Ayres, JR. 1965. *Theory and Problems of Modern Algebra*. New York: Schaum's Outline Series Megraw-Hill Book Company.

Gilbert, William J. 1976. *Modern Algebra with Application*. New York: John Willey & Sons.

Herstein, *I.N.*. 1975. *Topics in Algebra. Second Edition*. Singapore: John Wiley & Sons.

Isnarto. 2008. *Pengantar Struktur Aljabar 2*. Semarang: Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Negeri Semarang.

Joseph *A.* Gallian. 2012. *Contemporary Abstract Algebra (8th edition)*. University of Minnesota, Duluth, USA, Heath and Company.

Lang, *S.*. 1993. *Algebra. Third Edition*. New York: Addison-Wesley Publishing Company.

Malik, *D.S.*, Moderson, J.*M.*, Sen, *M.K.*. Sen. 2007. *MTH 581-582 Introduction to Abstract Algebra*. New York: McGraw-Hill Companies, Inc.

Setiawan, Adi. 2014. *Dasar-Dasar Aljabar Modern: Teori Grup dan Teori Ring*. Salatiga: Tisara Grafika.

Suryanti, Sri. 2018. *Teori Ring*. Gresik: Universitas Muhammadiyah Gresik (UMG) Press.

Panggabean, Ellis *M.* 2015. *Struktur Aljabar II*. Medan: Fakultas Keguruan dan Ilmu Pendidikan Universitas Muhammadiyah Sumatera Utara.

Prihandoko, Antonius *C.* 2009. *Pengantar Teori Ring dan Implementasinya*. Jember: Fakultas Keguruan dan Ilmu Pendidikan Universitas Jember.

TENTANG PENULIS

Siti Maysarah, M.Pd., lahir di Tanjung Morawa Kabupaten Deli Serdang Sumatra Utara pada tanggal 31 Agustus 1987. Lulus Sarjana (S-1) pada Program Studi Pendidikan Matematika Fakultas Tarbiyah IAIN Sumatera Utara pada tahun 2011. Tahun 2013 melanjutkan S-2 di Program Sudi Pendidikan Matematika Universitas Negeri Medan dan meraih gelar Magister Pendidikan pada tahun 2015.

Menjadi dosen tetap pada Program Studi Pendidikan Matematika UIN Sumatera Utara dari tahun 2015 sampai dengan sekarang. Saat ini aktif dalam mengajar matakuliah struktur aljabar grup dan struktur aljabar ring. Beberapa matakuliah yang pernah diajarkan, diantaranya: aljabar linier, program linier, matematika keuangan, dan desain media pembelajaran matematika.

STRUKTUR ALJABAR RING

Buku ajar ini disusun berdasarkan pada rumusan Capaian Pembelajaran Program Studi (CP-Prodi) dan rumusan Capaian Pembelajaran Mata Kuliah (CP-MK) yang tertuang pada Rencana Pembelajaran Semester (RPS) pada Program Studi Pendidikan Matematika Fakultas Ilmu Tarbiyah dan Keguruan UIN Sumatera Utara Medan. Buku ajar ini terdiri dari 10 bab, yang terdiri dari: Ring (Gelanggang), Daerah Integral dan Field, Subring, Ideal, Ring Faktor, Ring Homomorfisma, Ring Faktor dari Ring Polinomial, Lapangan Perluasan (*Extension Field*), Daerah Faktorisasi Tunggal, dan Daerah Euclid. Buku ajar ini ditulis dalam rangka melengkapi perangkat pembelajaran pada matakuliah struktur aljabar ring, yang merupakan matakuliah penting dari Program Studi Pendidikan Matematika. Setiap materi disajikan dalam bentuk definisi, teorema, lemma, contoh dan bukan contoh, serta diakhiri dengan latihan untuk mengukur pemahaman mahasiswa dalam menguasai materi pada matakuliah ini.

Buku *Struktur Aljabar Ring* ini dapat membantu mahasiswa dalam menguasai materi pada matakuliah ini. Sehingga nantinya dapat melahirkan pemikiran mahasiswa yang logis, kritis, sistematis, dan inovatif dalam menyelesaikan masalah.

DITERBITKAN ATAS KERJA SAMA

ISBN 978-623-218-699-6

9 786232 186996