LAPANGAN PERLUASAN DAN LAPANGAN BERHINGGA

SKRIPSI

Diajukan untuk memenuhi salah satu syarat
memperoleh gelar Sarjana Pendidikan
Program Studi Pendidikan Matematika

Disusun Oleh :

THERESIA YUNI WINDRATI

NIM : 91414054
NIRM : 911052010501120043

PROGRAM STUDI PENDIDIKAN MATEMATIKA
JURUSAN PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM
FAKULTAS KEGURUAN DAN ILMU PENDIDIKAN
UNIVERSITAS SANATA DHARMA
YOGYAKARTA

1997

SKRIPSI

LAPANGAN PERLUASAN DAN LAPANGAN BERHINGGA

Disusun Oleh :

THERESIA YUNI WINDRATI

NIM : 91414054
NIRM : 911052010501120043

Telah disetujui oleh :

Pembimbing

Dr. F. Susilo, S.J.

tanggal 11-9-1997

SKRIPSI

LAPANGAN PERLUASAN DAN LAPANGAN BERHINGGA

Yang dipersiapkan dan disusun oleh :

THERESIA YUNI WINDRATI

NIM : 91414054
NIRM : 911052010501120043

Telah dipertahankan di depan Dewan Penguji
Pada tanggal 26 Agustus 1997
dan dinyatakan telah memenuhi syarat

SUSUNAN DEWAN PENGUJI

	Nama Lengkap	Tanda Tangan
Ketua	: Drs. Fr. Y. Kartika Budi, M.Pd.	.....
Sekretaris	: Dr. St. Suwarsono	.....
Anggota	: Dr. F. Susilo, S.J.	.....
	Dr. Y. Marpaung	.....
	Dra. Maria Agustiani, M.Si.	.....

Yogyakarta, ... 1997
Fakultas Keguruan dan Ilmu Pendidikan
Universitas Sanata Dharma
Dekan

Dr. Paulus Suparno, S.J., M.S.T.

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Mahaesa atas rahmat dan kasihNya sehingga skripsi yang berjudul Lapangan Perluasan dan Lapangan Berhingga dapat terselesaikan.

Penyusunan skripsi ini dimaksudkan untuk memenuhi salah satu syarat memperoleh gelar Sarjana Pendidikan Program Studi Pendidikan Matematika di jurusan PMIPA fakultas Keguruan dan Ilmu Pendidikan Universitas Sanata Dharma Yogyakarta.

Pada kesempatan kali ini, penyusun ingin mengucapkan terima kasih kepada :

- Dr. Frans Susilo, S.J. selaku pembimbing yang dengan teliti dan penuh kesabaran membimbing dan memberi masukan yang berharga dalam proses penyusunan skripsi ini.
- Drs. Fr. Y. Kartika Budi, M.Pd. selaku ketua jurusan PMIPA.
- Drs. St. Susento, M.Si. selaku Ketua Program Studi Pendidikan Matematika.
- Bapak ibu dosen yang telah membimbing dan mendidik penyusun selama belajar di Universitas Sanata Dharma.
- Bapak ibu karyawan yang telah banyak membantu penyusun selama kuliah dan menyusun skripsi ini.
- Kedua orang tua dan saudara-saudara penyusun yang telah

memberikan dorongan spiritual maupun material.

- Rekan-rekan mahasiswa Pendidikan Matematika 91 yang telah memberi dukungan, semangat dan doa.
- Teman-teman kost yang telah memberi dukungan dan doa.

Penyusun menyadari bahwa masih terdapat kekurangan dalam skripsi ini, karenanya segala masukan dan saran yang membangun akan diterima dengan senang hati.

Harapan penyusun semoga skripsi ini dapat berguna bagi para pembaca.

Penyusun

DAFTAR ISI

ABSTRAK

Suatu lapangan E disebut lapangan perluasan dari lapangan F jika lapangan E memuat F sebagai lapangan bagiannya.

Jika $p(x) \in F[x]$ adalah polinomial tak teredusir atas lapangan F, maka ring faktor $K = F[x]/\langle p(x) \rangle$ merupakan lapangan perluasan dari lapangan F, dan p(x) mempunyai suatu elemen nul dalam K.

Suatu lapangan perluasan E dari lapangan F merupakan ruang vektor atas F.

Suatu elemen α di dalam lapangan perluasan E dari lapangan F dikatakan bersifat aljabar atas F jika $f(\alpha) = 0$, untuk suatu polinomial bukan nol $f(x) \in F[x]$. Suatu lapangan perluasan E dari lapangan F disebut perluasan aljabar dari F jika setiap elemennya bersifat aljabar atas F.

Lapangan perluasan E dari lapangan F disebut perluasan berhingga dari F bila dimensi dari E sebagai ruang vektor atas F adalah berhingga. Suatu lapangan perluasan berhingga E dari F merupakan perluasan aljabar dari F.

Jika E adalah lapangan perluasan dari lapangan F, maka $\bar{F}_E = \{ \alpha \in E \mid \alpha$ bersifat aljabar atas F $\}$ adalah lapangan bagian dari E, yang disebut tutupan aljabar dari F dalam E.

Untuk setiap bilangan prima p dan bilangan bulat positif n terdapat lapangan berhingga dengan ordo p^n.

ABSTRACT

A field E is called an extension field of a field F if E contains F as its subfield.

If $p(x) \in F[x]$ is an irreducible polynomial over a field F, the quotient ring $K = F[x]/\langle p(x) \rangle$ is an extension field of field F, and polynomial p(x) has a zero in this extension field K.

An extension field E of a field F is a vector space over F.

An element α of an extension field E of a field F is said to be algebraic over F if $f(\alpha) = 0$ for some non-zero polynomial $f(x) \in F[x]$. An extension field E of a field F is called an algebraic extension of F if every element in E is algebraic over F.

An extension field E of a field F is called a finite extension of F if E is of finite dimension as a vector space over F. A finite extension field E of a field F is an algebraic extension of F.

If E is an extension field of a field F, then $\overline{F}_E = \{ \alpha \in E \mid \alpha \text{ is algebraic over } F \}$ is a subfield of E, called the algebraic closure of F in E.

For every prime number p and positive integer n there exists a finite field of order p^n.

BAB I

PENDAHULUAN

1. Latar Belakang Masalah

Dalam mata kuliah Struktur Aljabar telah dibahas konsep lapangan (field). Oleh karena itu penulis tertarik untuk menyelidikinya lebih lanjut, khususnya tentang lapangan perluasan dan lapangan berhingga.

Dalam tulisan ini penulis akan membahas tentang bila suatu polinomial tak konstan $p(x) \in F[x]$ tak tereduksir atas lapangan F, sehingga polinomial tersebut tak mempunyai suatu akar α dalam F. Oleh karena itu dibentuklah lapangan perluasan E dari lapangan F yang memuat α. Elemen $\alpha \in E$ akan disebut elemen nul dari p(x) atas lapangan F.

Dalam tulisan ini juga akan ditunjukkan bahwa untuk setiap bilangan prima p dan suatu bilangan bulat positif n terdapat lapangan berhingga dengan p^n elemen.

2. Perumusan Masalah

Pokok permasalahan yang akan dibahas dalam tulisan ini dapat dirumuskan sebagai berikut :

- Apakah yang dimaksud lapangan perluasan ?
- Bagaimanakah hubungan antara lapangan perluasan dengan konsep-konsep lain yang telah dipelajari sebelumnya ?

- Bagaimanakah struktur dari lapangan berhingga ?
- Bagaimanakah hubungan antara lapangan berhingga dengan konsep-konsep lain yang telah dipelajari sebelumnya ?

3. Tujuan Penulisan

Tujuan dari penulisan ini adalah untuk memahami tentang lapangan perluasan, struktur lapangan berhingga, serta mengetahui hubungan antara lapangan perluasan, lapangan berhingga dengan konsep-konsep lain yang telah dipelajari sebelumnya.

4. Metode Penulisan

Metode yang digunakan penulis dalam meneliti topik tersebut adalah metode studi pustaka, sehingga dalam penulisan ini tidak ditemukan hal-hal yang baru.

BAB II
LANDASAN TEORI

Bab ini dibagi menjadi empat subbab. Subbab yang pertama membahas tentang Daerah Integral, subbab kedua membahas tentang Lapangan (Field), subbab ketiga tentang Isomorfisma dan Karakteristik dan subbab yang keempat tentang Ring Faktor. Subbab - subbab tersebut dibicarakan terlebih dahulu sebagai teori prasyarat untuk membicarakan teori selanjutnya.

1. Daerah Integral

Definisi 2.1.1

Ring adalah himpunan tak kosong R yang dilengkapi dengan 2 operasi yang dinamakan penjumlahan (+) dan perkalian (.) sedemikian sehingga memenuhi aksioma-aksioma berikut :

1. $(\forall\ a,b \in R)\ (a+b) \in R \wedge (a.b) \in R$
2. $(\forall\ a,b \in R)\ a+b = b+a$
3. $(\forall\ a,b,c \in R)\ (a+b)+c = a+(b+c)$
4. $(\exists\ 0 \in R)(\forall\ a \in R)(0+a = a)$
5. $(\forall\ a \in R)(\exists\ -a \in R)\ ((-a)+a = 0)$
6. $(\forall\ a,b,c \in R)\ (a.b).c = a.(b.c)$
7. $(\forall\ a,b,c \in R)\ a.(b+c) = a.b+a.c \wedge (a+b).c = a.c+b.c$

Contoh 2.1.1

Himpunan bilangan bulat ($\mathbb{Z}$),rasional ($\mathbb{Q}$),dan real ($\mathbb{R}$) membentuk ring terhadap operasi jumlahan dan perkalian biasa.

Contoh 2.1.2

Untuk setiap bilangan bulat positif n, himpunan semua bilangan bulat modulo n ($\mathbb{Z}_n$) membentuk ring terhadap operasi $\oplus$ dan $\odot$ yang didefinisikan sebagai berikut :

$[a]\oplus[b] = [a+b]$

$[a]\odot[b] = [a.b]$

untuk setiap $[a],[b] \in \mathbb{Z}_n$

Bukti :

1. $\forall\ [a],[b] \in \mathbb{Z}_n : [a]\oplus[b] = [a+b] \in \mathbb{Z}_n \wedge [a]\odot[b] = [a.b] \in \mathbb{Z}_n$
2. $\forall\ [a],[b] \in \mathbb{Z}_n\ [a]\oplus[b] = [a+b] = [b+a] = [b]\oplus[a]$
3. $\forall\ [a],[b],[c] \in \mathbb{Z}_n\ ([a]\oplus[b])\oplus[c] = ([a+b])\oplus[c]$
   $= [(a+b)+c]$
   $= [a+(b+c)]$
   $= [a]\oplus[b+c]$
   $= [a]\oplus([b]\oplus[c])$
4. $\exists\ [0] \in \mathbb{Z}_n \ni [0]\oplus[a] = [0+a] = [a]$
5. Ambil sebarang $[a] \in \mathbb{Z}_n$ maka $\exists\ [-a] \in \mathbb{Z}_n$ sedemikian sehingga $[a]\oplus[-a] = [a+(-a)] = [a-a] = [0]$.

   Jadi $(\forall\ [a] \in \mathbb{Z}_n)\ (\exists\ [-a] \in \mathbb{Z}_n) \ni ([a]\oplus([-a]) = [0]$.

6. $\forall\ [a],[b],[c] \in \mathbb{Z}_n$ $([a]\odot[b])\odot[c] = ([a.b])\odot[c]$

$= [(a.b).c]$

$= [a.(b.c)]$

$= [a]\odot[b.c]$

$= [a]\odot([b]\odot[c])$

7. $\forall\ [a],[b],[c] \in \mathbb{Z}_n$ $[a]\odot([b]\oplus[c]) = [a]\odot([b+c])$

$= [a.(b+c)]$

$= [a.b+a.c]$

$= [a.b]\oplus[a.c]$

$= ([a]\odot[b])\oplus([a]\odot[c])$

$([a]\oplus[b])\odot[c] = ([a+b])\odot[c]$

$= [(a+b).c]$

$= [a.c+b.c]$

$= [a.c]\oplus[b.c]$

$= ([a]\odot[c])\oplus([b]\odot[c])$

Teorema 2.1.1

Bila R ring dan a,b,c ∈ R, maka berlakulah

1. Jika a+b = a+c maka b=c
2. Jika b+a = c+a maka b=c
3. -(-a) = a dan -(a+b) = (-a)+(-b)

Bukti

1. a+b = a+c

(-a)+a+b = (-a)+a+c

0+b = 0+c

b = c

2. $b+a = c+a$

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

$b+0 = c+0$

$b = c$

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

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

$-(-a) = a$

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

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

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

$-(a+b) = (-a)+(-b)$ ■

Teorema 2.1.2

Jika R ring dengan elemen identitas 0, maka untuk sebarang $a,b \in R$ berlaku :

1. $0.a = a.0 = 0$
2. $a.(-b) = (-a).b = -(a.b)$
3. $(-a).(-b) = a.b$
4. $a.(b-c) = a.b-a.c$

Bukti

1. $0.a+0.a = (0+0).a$

$= 0.a$

$= 0+0.a$

$0.a+0.a = 0+0.a$

$0.a = 0$

$$a.0+a.0 = a.(0+0)$$
$$= a.0$$
$$= 0+a.0$$
$$a.0+a.0 = 0+a.0$$
$$a.0 = 0$$

2. $$a.(-b)+a.b = a.(-b+b)$$
$$= a.0$$
$$= 0$$
$$a.(-b)+a.b = -(a.b)+a.b$$
$$a.(-b) = -(a.b)$$
$$(-a).b+a.b = (-a+a).b$$
$$= 0.b$$
$$= 0$$
$$(-a).b+a.b = -(a.b)+a.b$$
$$(-a).b = -(a.b)$$

3. $$(-a).(-b) = -(a.(-b))$$
$$= -(-(a.b))$$
$$= a.b$$

4. $$a.(b-c) .= a.(b+(-c))$$
$$= a.b+a.(-c)$$
$$= a.b+(-(a.c))$$
$$= a.b-a.c$$ ■

Definisi 2.1.2

Ring R disebut *ring komutatif* bila ($\forall$ a,b $\in$ R) a.b = b.a.

Definisi 2.1.3

Elemen e di dalam ring R disebut *elemen satuan* bila dan hanya bila $(\forall a \in R)\ a.e = e.a = a$.

Contoh 2.1.3

Bilangan 1 merupakan elemen satuan dalam ring bilangan-bilangan bulat ($\mathbb{Z}$).

Definisi 2.1.4

Suatu elemen $a \neq 0$ di dalam ring komutatif R disebut *pembagi nol* di dalam R bila dan hanya bila $(\exists b \in R,\ b \neq 0)\ a.b = 0$

Jadi ring R memuat pembagi nol bila dan hanya bila $(\exists a \neq 0)(\exists b \neq 0)\ a.b = 0$, di mana $a,b \in R$.

Ring R tidak memuat pembagi nol bila dan hanya bila $(\forall a,b \in R)\ a.b = 0 \rightarrow a=0 \vee b = 0$

Definisi 2.1.5

Ring komutatif yang memuat elemen satuan e dan tidak memuat pembagi nol disebut *daerah integral*.

Contoh 2.1.4

Ring bilangan bulat $\mathbb{Z}$ merupakan daerah integral, tetapi ring bilangan genap bukan merupakan daerah integral sebab tidak memuat elemen satuan.

Teorema 2.1.3

$\mathbb{Z}_n$ daerah integral bila dan hanya bila n adalah bilangan prima.

Bukti

1. →

   Diketahui $\mathbb{Z}_n$ daerah integral. Andaikan n bukan bilangan prima, maka n = a.b dengan a > 1 dan b >1 , di mana a,b ∈ $\mathbb{Z}$. Jadi [a]⊙[b] = [a.b] = [n] =[0]. Jadi (∃ [a]≠[0])(∃ [b]≠[0]) [a]⊙[b]= [0], yaitu $\mathbb{Z}_n$ memuat pembagi nol. Timbul kontradiksi karena $\mathbb{Z}_n$ daerah integral. Jadi n adalah bilangan prima.

2.←

   1. $\mathbb{Z}_n$ merupakan ring (contoh 2.1.2)
   2. (∀ [a],[b] ∈ $\mathbb{Z}_n$) [a]⊙[b] = [a.b] = [b.a] = [b]⊙[a]
   3. (∃ [1] ∈ $\mathbb{Z}_n$)(∀ [a] ∈ $\mathbb{Z}_n$) [1]⊙[a] = [1.a] = [a]
   4. (∀ a,b ∈ $\mathbb{Z}$) a.b = n → a = n ∨ b = n

      Maka (∀ [a],[b] ∈ Z_n) berlaku :

      [a]⊙[b] = [n] → [a] = [n] ∨ [b] = [n]

      [a]⊙[b] = [0] → [a] = [0] ∨ [b] = [0]

   Jadi $\mathbb{Z}_n$ merupakan daerah integral. ■

Teorema 2.1.4

Jika D daerah integral, a,b,c ∈ D ,a ≠ 0, dan a.b = a.c, maka b = c (hukum kanselasi kiri).

Bukti

Ambil sebarang a,b,c ∈ D sedemikian sehingga a.b =

a.c. Maka a.(b-c) = 0. Karena D daerah integral dan $a \neq 0$, maka b-c = 0, sehingga b = c. ■

Teorema 2.1.5

Jika D daerah integral, a,b c ∈ D, a ≠ 0, dan b.a = c.a, maka b = c.

Bukti

Ambil sebarang a,b,c ∈ D sedemikian sehingga b.a = c.a. Maka (b-c).a = 0. Karena D daerah integral dan $a \neq 0$,maka b-c = 0, sehingga b = c. ■

Definisi 2.1 6

Jika R ring dan S ⊆ R dengan S ≠ ∅,maka S disebut *ring bagian (subring)* dari R bila terhadap operasi yang sama dengan operasi dalam R, S juga merupakan ring.

Teorema 2.1.6

Misal (R,+,.) adalah ring dan S ⊆ R dengan S ≠ ∅. Maka S adalah ring bagian dari R bila dan hanya bila :

1. (∀ a,b ∈ S) a-b ∈ S
2. (∀ a,b ∈ S) a.b ∈ S

Bukti

1.⇒

1. Ambil sebarang elemen a dan b dari S maka -b elemen dari S, sehingga a + (-b) = a - b ∈ S
2. Ambil sebarang elemen a,b dari ring bagian S, ma-

ka $a.b \in S$.

2.←

1. Ambil $a \in S$, maka $a-a = a+(-a) = 0 \in S$.
2. Ambil $a,0 \in S$, maka $0-a = 0+(-a) = -a \in S$.
3. Ambil $a,b \in S$, maka $-b \in S$, sehingga $a-(-b) = a+b \in S$.
4. Karena $S \subseteq$ ring R, maka berlakulah :

   4.1 $(\forall a,b,c \in S)\ (a+b)+c = a+(b+c)$

   4.2 $(\forall a,b \in S)\ a+b = b+a$

   4.3 $(\forall a,b,c \in S)\ (a.b).c = a.(b.c)$

   4.4 $(\forall a,b,c \in S)\ a.(b+c) = a.b+a.c \wedge (a+b).c = a.c+b.c$ ■

2. Lapangan (Field)

Definisi 2.2.1

Bila elemen-elemen yang tidak nol dalam suatu ring membentuk grup komutatif terhadap operasi perkalian, maka ring itu disebut *lapangan (field)*.

Teorema 2.2.1

Setiap lapangan pasti merupakan daerah integral.

Bukti

Andaikan (F,+,.) adalah suatu lapangan, maka (F,+,.) merupakan ring komutatif dan memuat elemen satuan *e*. Ambil dua elemen $a,b \in F$ sedemikian sehingga $a.b = 0$

dan $a \neq 0$. Maka $a^{-1}.(a.b) = a^{-1}.0$

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

$$e.\ b = 0$$

$$b = 0.$$

Jadi F merupakan daerah integral. ■

Teorema 2.2.2

Ring F merupakan suatu lapangan bila dan hanya bila :

1. F adalah suatu daerah integral.
2. Setiap elemen tidak nol dari F mempunyai invers terhadap operasi perkalian.

Bukti :

1.→

1. Menurut teorema 2.2.1, ring F merupakan daerah integral.
2. Definisi 2.2.1 menyatakan bahwa lapangan adalah ring yang elemen-elemen tidak nol membentuk grup komutatif terhadap operasi perkalian. Maka setiap elemen dari F-{0} punya invers.

2.←

Diketahui F adalah suatu daerah integral dan setiap elemen dari F-{0} mempunyai invers terhadap operasi perkalian. Akan dibuktikan (F-{0},.) merupakan grup komutatif.

1. Ambil sebarang $a,b \in F-\{0\}$, maka $a.b \in F-\{0\}$ karena F merupakan daerah integral.

2. Karena F-{0} $\subset$ F, maka sifat komutatif dan asosiatif terpenuhi.
3. F-{0} memuat elemen satuan, karena F merupakan daerah integral. ■

Teorema 2.2.3

Setiap daerah integral berhingga pasti merupakan Lapangan.

Bukti

Andaikan D Daerah Integral berhingga.

1. Ambil sebarang elemen $a \in D$ dan $a \neq 0$. Didefinisikan pemetaan $\theta : D \longrightarrow D$ dengan aturan $\theta(x) = a.x$, $\forall x \in D$. Ambil x dan y sebarang elemen D sedemikian sehingga $\theta(x) = \theta(y)$. Maka $a.x = a.y$, sehingga $x = y$. Jadi θ adalah pemetaan injektif.
2. Andaikan pemetaan θ tidak surjektif. Maka $\theta(D) \subset D$. Karena D berhingga maka $|\theta(D)| < |D|$. Tetapi karena $\theta : D \longrightarrow D$ pemetaan injektif maka $|\theta(D)| = |D|$. Timbul kontradiksi, jadi θ pemetaan surjektif.
3. Ambil $e \in D$, maka pasti ada $x \in D$ sedemikian sehingga $\theta(x) = e$, yaitu $a.x = e$. Jadi $(\exists\, x \in D)\ (a.x = e)$, yaitu x adalah invers dari a terhadap operasi perkalian. Terbukti D merupakan Lapangan. ■

Teorema 2.2.4

$\mathbb{Z}_n$ lapangan bila dan hanya bila n adalah bilangan prima.

Bukti

1. →

Bila $\mathbb{Z}_n$ lapangan, pastilah $\mathbb{Z}_n$ merupakan daerah integral. Menurut teorema 2.1.3, bila $\mathbb{Z}_n$ daerah integral maka n adalah bilangan prima.

2. ←

Dari teorema 2.1.3 diperoleh bahwa bila n bilangan prima, maka $\mathbb{Z}_n$ Daerah Integral. Karena $\mathbb{Z}_n$ adalah daerah integral berhingga, maka $\mathbb{Z}_n$ adalah Lapangan. ■

Definisi 2.2.3

Himpunan bagian tak kosong H dari lapangan F disebut *lapangan bagian (subfield) dari F* bila dan hanya bila H merupakan Lapangan terhadap operasi-operasi dari F.

Teorema 2.2.5

Diketahui F suatu lapangan dan $K \subset F$. K merupakan lapangan bagian dari F bila dan hanya bila :

(i). $K \neq \emptyset$

(ii) Jika $a, b \in K$ maka $a + b \in K$ dan $a.b \in K$

(iii) Jika $a \in K$ maka $-a \in K$

(iv) Jika $a \in K$ dan $a \neq 0$ maka $a^{-1} \in K$

Bukti

1. →

Diketahui K lapangan bagian dari F maka K pasti merupakan suatu lapangan. Karena K merupakan

lapangan maka K merupakan ring bagian yang memenuhi bahwa setiap elemennya yang tidak kosong mempunyai invers terhadap operasi perkalian.

Jadi (i), (ii), (iii), dan (iv) dipenuhi.

2. ←

Diketahui K merupakan suatu ring bagian .

Karena K ring bagian maka $K \neq \emptyset$. Ambil suatu elemen $a \in K$, $a \neq 0$ maka menurut yang diketahui $a^{-1} \in K$.

Karena K ring bagian maka $a.a^{-1} \in K$. Jadi $e \in K$.

Karena $K \subset F$ padahal diketahui F lapangan maka sifat komutatif dan tidak memuat pembagi nol dipenuhi di K. Jadi K adalah daerah integral, di mana tiap elemen yang tidak sama dengan nol mempunyai invers terhadap operasi perkalian. ■

3. Isomorfisma dan Karakteristik

Definisi 2.3.1.

Pemetaan $\theta : R \longrightarrow S$, di mana R dan S adalah ring, disebut *isomorfisma* bila hanya bila

1. Pemetaan θ bijektif
2. $(\forall\ a,b \in R)\ \theta(a+b) = \theta(a)+\theta(b)$

$$\theta(a.b) = \theta(a).\theta(b)$$

Jika ada suatu isomorfisma dari R kepada S maka dikatakan R *isomorfik* dengan S dan dinotasikan dengan $R \approx S$.

Contoh 2.3.1

$\mathbb{Z}_6 \approx \mathbb{Z}_2 \times \mathbb{Z}_3$

Bukti

1. Didefinisikan pemetaan $\theta : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$ dengan aturan $\theta([a]_6) = ([a]_2,[a]_3)$. Ambil sebarang $[a]_6$, $[b]_6 \in \mathbb{Z}_6$ sedemikian sehingga $[a]_6 = [b]_6$. Karena $6|a-b$, maka $2|a-b$ dan $3|a-b$. Sehingga $[a]_2 = [b]_2$ dan $[a]_3 = [b]_3$. Jadi $([a]_2,[a]_3) = ([b]_2,[b]_3)$, yaitu $\theta([a]_6) = \theta([b]_6)$. Jadi θ well-defined.
2. Ambil sebarang $([b]_2,[b]_3) \in \mathbb{Z}_2 \times \mathbb{Z}_3$ maka ada $[b]_6 \in \mathbb{Z}_6$ sedemikian sehingga $\theta([b]_6) = ([b]_2,[b]_3)$.
   Jadi θ surjektif
3. Ambil sebarang $[a],[b] \in \mathbb{Z}_6$ sedemikian sehingga $\theta([a]_6) = \theta([b]_6)$. Maka $([a]_2,[a]_3) = ([b]_2,[b]_3)$. Sehingga $[a]_2 = [b]_2$ dan $[a]_3 = [b]_3$, maka $2|(a-b)$ dan $3|(a-b)$. Oleh karena itu $6|(a-b)$, maka $[a]_6 = [b]_6$.
   Jadi θ injektif
4. Ambil sebarang $[a]_6,[b]_6 \in \mathbb{Z}_6$ maka

$$\begin{aligned}\theta([a]_6 \oplus [b]_6) &= \theta([a+b]_6)\\ &= ([a+b]_2,[a+b]_3)\\ &= ([a]_2 \oplus [b]_2,[a]_3 \oplus [b]_3)\\ &= ([a]_2,[a]_3) \oplus ([b]_2,[b]_3)\\ &= \theta[a]_6 \oplus \theta[b]_6\end{aligned}$$

Demikian pula

$$\theta([a]_6 \odot [a]_6) = \theta([a.b]_6)$$
$$= ([a.b]_2, [a.b]_3)$$
$$= ([a]_2 \odot [b]_2, [a]_3 \odot [b]_3)$$
$$= ([a]_2, [a]_3) \odot ([b]_2, [b]_3)$$
$$= \theta[a]_6 \odot \theta[b]_6$$

Jadi θ homorfisma. ■

Definisi 2.3.5

Bilangan bulat positif terkecil n sedemikian sehingga na = 0 untuk setiap a elemen ring R dinamakan *karakteristik* dari R . Jika tidak ada bilangan tersebut dikatakan karakteristik dari R sama dengan nol.

Contoh 2.3.2

Ring bilangan bulat $\mathbb{Z}$ mempunyai karakteristik sama dengan nol. Ring bilangan bulat modulo n ($\mathbb{Z}_n$) mempunyai karakteristik n, karena n[a] = [na] = [0] untuk setiap $[a] \in \mathbb{Z}_n$.

Teorema 2.3.1

Bila ring R mempunyai elemen satuan e, maka karakteristik dari ring R adalah n bila dan hanya bila n adalah bilangan bulat positif terkecil sedemikian sehingga ne= 0. Jika tidak ada bilangan yang memenuhi sifat tersebut,

maka ring R tersebut mempunyai karakteristik sama dengan nol.

Bukti

1. ⇒

Andaikan ring R mempunyai karakteristik n. Maka n adalah bilangan bulat positif terkecil sedemikian sehingga untuk setiap elemen $a \in R$ berlaku $na = 0$. Karena $e \in R$, maka dipenuhi $ne = 0$.

2. ⇐

Andaikan n adalah bilangan bulat positif terkecil sedemikian sehingga $ne = 0$. Akan dibuktikan bahwa n merupakan karakteristik dari ring R. Ambil sebarang $a \in R$, maka $na = a+a+a+...+a$ (n suku)

$= a(e+e+e+....+e)$ (n suku)

$= a(ne)$

$= a0 = 0$

Jadi terbukti bahwa n adalah karakteristik dari ring R.

Andaikan karakteristik ring R adalah $n \neq 0$. Maka n adalah bilangan bulat positif terkecil sedemikian sehingga $na = 0$ untuk setiap $a \in R$. Jadi $ne = 0$. Jadi ada bilangan bulat positif terkecil yang memenuhi $ne = 0$. ■

Teorema 2.3.2

Jika D daerah integral, maka karakteristik dari D adalah

nol atau prima.

Bukti

D Daerah Integral dengan elemen satuan e.

Andaikan karakteristik D adalah n dan $n \neq 0$, maka ne = 0. Andaikan n bukan bilangan prima, maka n = rs, di mana $1<r<n$ dan $1<s<n$. Selanjutnya

ne = rs(e)

ne = e+e+e+...+e (rs suku)

= ee+ee+ee+...+ee (rs suku)

=(e+e+e+...+e)(e+e+e+...+e)
r suku s suku

= (re)(se)

Jadi (re)(se) = 0.

Karena D Daerah Integral, maka re = 0 atau se = 0.

Padahal $re \neq 0$ dan $se \neq 0$.

Timbul kontradiksi.

Terbukti n adalah bilangan prima atau nol. ■

Teorema 2.3.3

Bila D adalah daerah integral dan karakteristik dari D = 0, maka D memuat ring bagian yang isomorfik dengan $\mathbb{Z}$.

Bukti

Diketahui D adalah daerah integral dengan elemen satuan e. Perhatikan relasi $\theta : \mathbb{Z} \longrightarrow D$ dengan aturan $\theta(n) = n.e, \forall\ n \in \mathbb{Z}$.

1. Akan dibuktikan relasi $\theta : \mathbb{Z} \longrightarrow D$ dengan aturan $\theta(n) = n.e$, $\forall\, n \in \mathbb{Z}$ merupakan pemetaan. Ambil sebarang $a,b \in \mathbb{Z}$ sedemikian sehingga $a = b$. Karena $a.e = b.e$, maka $\theta(a) = \theta(b)$.

2. Akan dibuktikan bahwa pemetaan θ merupakan isomorfisma dari $\mathbb{Z}$ ke $\theta(\mathbb{Z})$.

   (i). Ambil 2 elemen sebarang $m, n \in \mathbb{Z}$ sedemikian sehingga $\theta(m) = \theta(n)$ maka diperoleh

   $$m.e = n.e$$
   $$m.e - n.e = 0$$
   $$(m - n).e = 0$$

   Karena karakteristik dari D adalah nol maka

   $$m - n = 0$$
   $$m = n$$

   Jadi pemetaan θ injektif.

   (ii). Ambil 2 elemen sebarang $m, n \in \mathbb{Z}$. Maka

   $$\theta(m+n) = (m+n).e$$
   $$= m.e + n.e$$
   $$= \theta(m) + \theta(n)$$
   $$\theta(m.n) = (m.n).e$$
   $$= \underbrace{e+e+e+\ldots+e}_{m.n \text{ suku}}$$
   $$= \underbrace{ee+ee+ee+\ldots+ee}_{m.n \text{ suku}}$$

$\theta(m.n) = (\underbrace{e+e+e+...+e}_{m \text{ suku}})(\underbrace{e+e+e+...+e}_{n \text{ suku}})$

$= (m.e).(n.e)$

$= \theta(m).\theta(n)$

Jadi terbukti bahwa pemetaan θ merupakan isomorfisma dari $\mathbb{Z}$ ke $\theta(\mathbb{Z})$, sehingga $\mathbb{Z} \approx \theta(\mathbb{Z})$.

3. Akan dibuktikan bahwa $\theta(\mathbb{Z})$ merupakan ring bagian dari D.

Karena $(\mathbb{Z},+)$ grup dan θ homomorfisma, maka $\theta(\mathbb{Z})$ merupakan grup terhadap operasi penjumlahan. Sekarang tinggal membuktikan bahwa operasi perkalian bersifat tertutup di $\theta(\mathbb{Z})$.

Ambil elemen sebarang $m, n \in \theta(\mathbb{Z})$ maka terdapat $a, b \in \mathbb{Z}$ sedemikian sehingga $\theta(a) = m$ dan $\theta(b) = n$.

Karena $a, b \in \mathbb{Z}$ maka $a.b \in \mathbb{Z}$ sehingga $\theta(a.b) \in \theta(\mathbb{Z})$.

Selanjutnya $\theta(a.b) = \theta(a).\theta(b)$

$= m.n \in \theta(\mathbb{Z})$.

Jadi operasi perkalian bersifat tertutup di $\theta(\mathbb{Z})$.

Terbukti bahwa $\theta(\mathbb{Z})$ merupakan ring bagian dari D. ■

Teorema 2.3.4

Bila D daerah integral dan karakteristik dari D adalah bilangan prima p, maka D memuat ring bagian yang isomorfik dengan $\mathbb{Z}_p$.

Bukti

Diketahui D daerah integral dengan elemen satuan e.

Perhatikan relasi $\theta : \mathbb{Z}_p \longrightarrow D$ dengan aturan $\theta([n]) = n.e$, $\forall [n] \in \mathbb{Z}_p$.

1. Akan dibuktikan bahwa relasi $\theta : \mathbb{Z}_p \longrightarrow D$ dengan aturan $\theta([n]) = n.e$ merupakan pemetaan. Ambil sebarang $[a], [b] \in \mathbb{Z}_p$ sedemikian sehingga $[a]=[b]$. Karena $[a] = [b]$, maka $a-b = k.p$, di mana $k \in \mathbb{Z}$. Sehingga $(a-b).e = k.p.e$. Karena karakteristik dari D adalah p, maka $a.e-b.e = 0$. Jadi $a.e = b.e$, yaitu $\theta([a]) = \theta([b])$.
2. Akan dibuktikan bahwa pemetaan θ adalah suatu isomorfisma dari $\mathbb{Z}_p$ ke $\theta(\mathbb{Z}_p)$.

   (i). Ambil 2 elemen sebarang $[m], [n] \in \mathbb{Z}_p$ sedemikian sehingga $\theta([m]) = \theta([n])$. Maka diperoleh $m.e = n.e$

   $$m.e - n.e = 0$$

   $$(m - n).e = 0$$

   Karena karakteristik dari D adalah bilangan prima p dan $m - n < p$, maka haruslah $m - n = 0$. Sehingga $m = n$.

   Jadi θ pemetaan injektif.

   (ii). Ambil 2 elemen sebarang $[m]. [n] \in \mathbb{Z}_p$

   Maka $\theta([m] \oplus [n]) = \theta([m+n])$

   $$= (m + n)\, e$$

   $$= me + ne$$

   $$= \theta([m]) + \theta([n]).$$

   $$\theta([m] \odot [n]) = \theta([m.n])$$

$$\theta([m]\odot[n]) = (m.n).e$$

$$= (\underbrace{e+e+e+\ldots+e}_{m.n \text{ suku}})$$

$$= (\underbrace{ee+ee+ee+\ldots+ee}_{m.n \text{ suku}})$$

$$= (\underbrace{e+e+e+\ldots+e}_{m \text{ suku}})(\underbrace{e+e+e+\ldots+e}_{n \text{ suku}})$$

$$= (m.e)(n.e) = \theta([m]).\theta([n]).$$

Jadi terbukti bahwa $\mathbb{Z}_p$ isomorfik dengan $\theta(\mathbb{Z}_p)$.

3. Akan dibuktikan bahwa $\theta(\mathbb{Z}_p)$ merupakan ring bagian dari D.

Karena $(\mathbb{Z}_p,+)$ grup dan θ homorfisma, maka $\theta(\mathbb{Z}_p)$ merupakan grup terhadap operasi jumlahan. Tinggal membuktikan bahwa operasi perkalian bersifat tertutup di $\theta(\mathbb{Z}_p)$. Ambil sebarang elemen $m, n \in \theta(\mathbb{Z}_p)$. Maka terdapat $[a], [b] \in \mathbb{Z}_p$ sedemikian sehingga $\theta([a]) = m$ dan $\theta([b]) = n$. Karena $[a],[b] \in \mathbb{Z}_p$, maka $[a]\odot[b] \in \mathbb{Z}_p$, sehingga $\theta([a]\odot[b]) \in \theta(\mathbb{Z}_p)$.

Selanjutnya $\theta([a]\odot[b]) = \theta([a]).\theta([b]) = m.n \in \theta(\mathbb{Z}_p)$.

Jadi operasi perkalian bersifat tertutup di $\theta(\mathbb{Z}_p)$.

Terbukti bahwa $\theta(\mathbb{Z}_p)$ merupakan ring bagian dari D. ■

4. Ring Faktor

Definisi 2.4.1

Jika pemetaan $\theta : R \longrightarrow S$ adalah suatu homomorfisma ring,

maka *kernel* θ adalah himpunan semua elemen $r \in R$ sedemikian sehingga $\theta(r) = 0_s$. Kernel θ biasa disingkat dengan *ker* θ.

Definisi 2.4.2

Ring bagian I dari ring R dinamakan *ideal* dalam R jika $a.r \in I$ dan $r.a \in I$, $\forall\ a \in I$ dan $r \in R$.

Contoh 2.4.1

$\mathbb{E} = \{ 2.n \mid n \in \mathbb{Z} \}$ merupakan ideal dalam $\mathbb{Z}$.

Bukti

$\mathbb{E} \subset \mathbb{Z}$ dan $\mathbb{E} \neq \emptyset$.

Ambil elemen sebarang $a,b \in \mathbb{E}$ di mana $a = 2.m$ dan $b = 2.n$, $m,n \in \mathbb{Z}$. Maka diperoleh $a-b = 2.m-2.n = 2.(m-n) = 2k$ di mana $k = m-n \in \mathbb{Z}$. Jadi $a-b \in \mathbb{E}$. Selanjutnya $a.b = 2.m.2.n = 2.(2.m.n) = 2.p$ di mana $p = 2.m.n \in \mathbb{Z}$. Jadi $a.b \in \mathbb{E}$. Sehingga menurut teorema 2.1.6, $\mathbb{E}$ merupakan ring bagian dari $\mathbb{Z}$.

Ambil elemen sebarang $a \in \mathbb{E}$ di mana $a = 2.k$, $k \in \mathbb{Z}$ dan $n \in \mathbb{Z}$, maka $a.n = (2.k).n = 2.(k.n) \in \mathbb{E}$ dan $n.a = n.(2.k) = (n.2).k = (2.n).k = 2.(n.k) \in \mathbb{E}$. Jadi $\mathbb{E} = \{2.n \mid n \in \mathbb{Z} \}$ merupakan ideal dalam $\mathbb{Z}$. ■

$\mathbb{Z}$ merupakan ring bagian dari $\mathbb{Q}$, tetapi $\mathbb{Z}$ bukan ideal dalam $\mathbb{Q}$, sebab ada elemen $\mathbb{Z}$ yaitu $3 \in \mathbb{Z}$ dan $\frac{1}{2} \in \mathbb{Q}$

sehingga diperoleh $3.\frac{1}{2} = \frac{3}{2} \notin \mathbb{Z}$. Jadi $\mathbb{Z}$ bukan ideal dalam $\mathbb{Q}$.

Teorema 2.4.1

Jika pemetaan θ : R——>S adalah homomorfisma ring, maka kernel θ adalah suatu ideal di dalam R.

Bukti

Karena R,S merupakan grup abel terhadap operasi penjumlahan dan θ homomorfisma , maka $\theta(0_R) = 0_S$. Jadi Ker $\theta \neq \emptyset$. Ambil sebarang $a,b \in$ Ker θ. Maka $\theta(a-b) = \theta(a+(-b)) = \theta(a)+\theta(-b) = \theta(a)-\theta(b) = 0_s-0_s = 0_s$. Jadi $a-b \in$ Ker θ. Selanjutnya $\theta(a.b) = \theta(a).\theta(b) = 0_s.0_s = 0_s$. Jadi $a.b \in$ Ker θ. Sehingga Ker θ merupakan ring bagian dari ring R.

Ambil sebarang $a \in$ Ker θ dan $r \in$ R. Maka $\theta(a.r) = \theta(a).\theta(r) = 0_s.\theta(r) = 0_s$, dan $\theta(r.a) = \theta(r).\theta(a) = \theta(r).0_s = 0_s$. Jadi $a.r \in$ Ker θ dan $r.a \in$ Ker θ. ■

Teorema 2.4.2

Jika R ring komutatif dengan elemen satuan e, dan $a \in R$, maka himpunan semua kelipatan a, yaitu { r.a| $r \in R$ }, merupakan ideal dalam R (yang akan dinotasikan sebagai <a>).

Bukti

1. Perhatikan bahwa $0.a = 0 \in \langle a \rangle$.

Jadi $\langle a \rangle \neq \emptyset$.

2. Ambil dua elemen sebarang $x, y \in \langle a \rangle$. Maka $x = a.r_1$ dan $y = a.r_2$ di mana $r_1, r_2 \in R$, sehingga $x + y = a.r_1 + a.r_2 = a.(r_1 + r_2) = a.r_3$, di mana $r_3 = r_1 + r_2 \in R$. Jadi $x + y \in \langle a \rangle$.
3. Ambil sebarang $x \in \langle a \rangle$. Maka $x = a.r$, di mana $r \in R$, sehingga $-x = -(a.r) = a(-r)$, di mana $-r \in R$. Jadi $-x \in \langle a \rangle$.
4. Ambil sebarang elemen $x \in \langle a \rangle$ dan $b \in R$. Maka $x = a.r$ di mana $r \in R$, sehingga diperoleh $x.b = (a.r).b = a.(r.b)$. Karena $r.b \in R$, maka $x.b \in \langle a \rangle$. Terbukti bahwa $\langle a \rangle$ merupakan ideal dalam R. ■

Definisi 2.4.3

Ideal yang dihasilkan oleh a, yaitu $\langle a \rangle = \{r.a \mid r \in R\}$, disebut *ideal utama*.

Contoh 2.4.2

$\langle 5 \rangle = \{ 5.n \mid n \in \mathbb{Z} \}$ adalah ideal utama dalam $\mathbb{Z}$.

Teorema 2.4.3

Ideal $\langle a \rangle$ dalam ring R merupakan ideal terkecil yang memuat a.

Bukti

Ambil sebarang ideal I yang memuat a ($a \in I$). Ambil sebarang $x \in \langle a \rangle$, maka terdapat $r \in R$ sedemikian

sehingga $x = a.r$. Karena $a \in I$, $r \in R$ dan I ideal, maka $a.r \in I$. Jadi $x \in I$, sehingga terbukti bahwa $\langle a \rangle \subseteq I$ ■

Teorema 2.4.4

Jika F lapangan, maka F tidak mempunyai ideal kecuali $\langle 0 \rangle$ dan F sendiri.

Bukti

Andaikan I ideal dalam F dan $I \neq \langle 0 \rangle$. Akan dibuktikan $I = F$. Ambil sebarang elemen x dalam I dan $x \neq 0$. Maka $x \in F$ dan $x^{-1} \in F$. Karena $x \in I$, $x^{-1} \in F$ dan I ideal maka $x.x^{-1} = e \in I$. Ambil sebarang $y \in F$. Maka $e.y = y \in I$. Jadi $F \subseteq I$ .....(1)

Karena I ideal dalam F, maka $I \subseteq F$.....(2)

Dari (1) dan (2) diperoleh $I = F$. ■

Definisi 2.4.4

Bila R ring, I ideal dalam ring R dan $a \in R$, maka $I+a = \{ n+a \mid n \in I \}$ disebut *koset kanan* dari I dalam ring R.

Teorema 2.4.5

Jika R adalah ring dan I adalah ideal dalam ring R, maka $R/I = \{ I + a \mid a \in R \}$ dengan operasi :

$(I+a)+(I+b) = I+a+b$

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

merupakan ring. Ring R/I disebut *Ring faktor* dari ring R

oleh ideal I.

Bukti

1. Ambil sebarang $I+a, I+b \in R/I$ maka menurut definisi penjumlahan di R/I

   $(I+a) + (I+b) = I + (a+b)$

   Karena R ring maka $a+b \in R$ sehingga $I + (a+b) \in R/I$. Ambil $I+a_1, I+a_2, I+b_1, I+b_2 \in R/I$, di mana $I+a_1 = I+a_2$ dan $I+b_1 = I+b_2$. Akan dibuktikan bahwa $I + (a_1+b_1) = I + (a_2+b_2)$. Karena $I+a_1 = I+a_2$ maka $a_1 = n+a_2$, $n \in I$. Dan juga karena $I+b_1 = I+b_2$ maka $b_1 = m+b_2$, $m \in I$. Maka didapat $a_1+b_1 = n+a_2+m+b_2 = n+m+a_2+b_2$. Karena $n \in I$, $m \in I$ dan I ideal, maka $n+m \in I$. Jadi $a_1+b_1 = k + a_2 + b_2$, di mana $k = n+m \in I$ sehingga $a_1+b_1 \in I + (a_2+b_2)$. Jadi terbukti bahwa $I + (a_1+b_1) = I + (a_2+b_2)$. Jadi operasi jumlahan dalam R/I tertutup dan well defined.

2. Ambil $I+a, I+b \in R/I$ maka menurut definisi operasi perkalian dalam R/I berlaku $(I+a).(I+b) = I + a.b$. Karena R ring dan $a,b \in R$, maka $a.b \in R$ sehingga $I + a.b \in R/I$.

   Ambil $I+a_1, I+b_1, I+a_2, I+b_2 \in R/I$ di mana $I+a_1 = I+a_2$ dan $I+b_1 = I+b_2$. Akan dibuktikan bahwa $I + (a_1.b_1) = I + (a_2.b_2)$. Karena $I+a_1 = I+a_2$, maka $a_1 = n+a_2$, di mana $n \in I$. Demikian pula karena $I+b_1 = I+b_2$, maka $b_1 = m+b_2$, di mana $m \in I$. Maka didapat

$a_1.b_1 = (n+a_2).(m+b_2) = (n+a_2).m + (n+a_2).b_2 = n.m + a_2.m + n.b_2 + a_2.b_2$. Perhatikan bahwa $n.m + a_2.m + n.b_2 \in I$, sebab $n,m \in I$, $a_2, b_2 \in R$, dan I ideal. Jadi $a_1.b_1 = j + a_2.b_2$, di mana $j = n.m + a_2.m + n.b_2 \in I$, sehingga $a_1.b_1 \in I + a_2.b_2$. Terbukti bahwa $I + (a_1.b_1) = I + (a_2.b_2)$. Jadi operasi perkalian dalam R/I tertutup dan well defined.

3. Ambil sebarang I+a, I+b, $\in$ R/I dengan a,b $\in$ R. Maka

$$\begin{aligned}(I+a) + (I+b) &= I + (a+b)\\ &= I+(b+a)\\ &= (I+b)+(I+a).\end{aligned}$$

4. Ambil I+a, I+b, I+c $\in$ R/I dengan a,b,c $\in$ R . Maka

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

5. Ada elemen identitas yaitu I+0, di mana 0 elemen identitas dalam R : Untuk sebarang elemen I + a $\in$ R/I berlaku $(I+a) + (I+0) = I + (a + 0) = I+a$.

6. Setiap elemen I+a $\in$ R/I mempunyai invers terhadap operasi penjumlahan, yaitu I + (-a) :

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

7. Ambil I+a, I+b, I+c $\in$ R/I dengan a,b,c $\in$ R. Maka

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

$$((I+a).(I+b)).(I+c) = I + (a.(b.c))$$
$$= (I+a).\ (I + (b.c))$$
$$= (I+a).((I+b).(I+c))$$

8. Ambil $I+a,\ I+b,\ I+c \in R/I$ dengan $a,b,c \in R$. Maka

$$(I+a).((I+b) + (I+c)) = (I+a).\ (I + (b+c))$$
$$= I + (a.(b+c))$$
$$= I + (a.b+a.c)$$
$$= (I+a.b) + (I+a.c)$$
$$= (I+a).(I+b) + (I+a).(I+c)$$

$$((I+a) + (I+b)).\ (I+c) = (I + (a+b)).\ (I+c)$$
$$= (I + (a+b).c)$$
$$= I + (a.c+b.c)$$
$$= (I + a.c) + (I + b.c)$$
$$= (I+a).(I+c) + (I+b).(I+c)$$

Terbukti bahwa R/I merupakan ring. ■

Teorema 2.4.6

Bila R adalah ring komutatif, maka ring faktor R/I komutatif.

Bukti

Ambil sebarang $I+a,\ I+b \in$ ring faktor R/I. Maka

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

Terbukti bahwa ring faktor R/I bersifat komutatif. ■

Teorema 2.4.7

Bila R adalah ring yang memuat elemen satuan e, maka ring faktor R/I memuat elemen satuan, yaitu I+e.

Bukti

Ambil sebarang I+a ∈ ring faktor R/I . Karena e ∈ R maka I+e ∈ R/I. Maka untuk sebarang elemen I + a ∈ R/I berlaku (I+e).(I+a) = I + (e.a) = I+a.

Terbukti bahwa ring faktor R/I memuat elemen satuan, yaitu I+e. ■

Sebelum kita membahas tentang ring faktor polinomial baiklah terlebih dulu kita membahas tentang konsep-konsep dasar ring polinomial.

Definisi 2.4.5

Jika R ring, maka suatu *polinomial* dalam x dengan koefisien dalam R, yang dilambangkan dengan p(x), adalah suatu jumlahan yang dinyatakan dalam bentuk :

$$\sum_{i=o}^{\sim} a_i x^i = a_o + a_1 x + a_2 x^2 + \ldots + a_n x^n + \ldots$$

di mana $a_i \in R$ dan $a_i = 0$ untuk semua kecuali berhingga banyak nilai i, dengan i bilangan bulat non negatif. Elemen-elemen $a_1, a_2, a_3, \ldots, a_i$ disebut *koefisien-koefisien* dari p(x). Nilai terbesar dari i sedemikian sehingga $a_i \neq 0$ disebut *derajat dari p(x)*, ditulis d(p(x)). Bila tidak ada nilai i tersebut, maka p(x)

dikatakan mempunyai derajat sama dengan nol. Dan a_i disebut *koefisien utama dari p(x)*.

Himpunan polinomial-polinomial dalam x dengan koefisien di dalam R dilambangkan dengan R[x].

Definisi 2.4.6

Penjumlahan dan perkalian polinomial dalam x atas ring R didefinisikan sebagai berikut :

Jika $f(x) = a_o + a_1 x + \ldots + a_n x^n + \ldots$

$g(x) = b_o + b_1 x + \ldots + b_n x^n + \ldots$

maka $f(x) + g(x) = \sum_{i=o}^{\sim} (a_i + b_i)\, x^i$

dan $f(x).g(x) = \sum_{k=o}^{\sim} c_k\, x^k$ di mana $c_k = \sum_{i=o}^{k} a_i\, b_{k-i}$

Definisi 2.4.7

Jika $p(x) = \sum_{i=o}^{\sim} a_i\, x^i = a_o + a_1 x + \ldots + a_n x^n + \ldots$

dan $g(x) = \sum_{i=o}^{\sim} b_i\, x^i = b_o + b_1 x + \ldots + b_n x^n + \ldots$

maka $p(x) = g(x)$ bila dan hanya bila untuk semua i dalam $\mathbb{Z}$, $i \geq 0$, $a_i = b_i$.

Teorema 2.4.8

Jika R ring komutatif, maka R[x] adalah ring komutatif terhadap operasi yang didefinisikan pada definisi 2.4.6 diatas.

Bukti

Untuk setiap $f(x) = \sum_{i=o}^{\sim} a_i x^i$, $g(x) = \sum_{i=o}^{\sim} b_i x^i$ dan $h(x) = \sum_{i=o}^{\sim} c_i x^i$ di dalam R[x] berlaku :

1. $f(x) + g(x) = \sum_{i=o}^{\sim} (a_i + b_i)\ x^i \in R[x]$ sebab $a_i + b_i$ di dalam R untuk setiap i .

2. $f(x)\ g(x)$ didalam R[x] sebab $a_i . b_{n-i}$ di dalam R untuk setiap a_i , b_{n-i} di dalam R.

3. $f(x) + g(x) = \sum_{i=o}^{\sim} a_i x^i + \sum_{i=o}^{\sim} b_i x^i$

$$= \sum_{i=o}^{\sim} (a_i + b_i)\ x^i$$

$$= \sum_{i=o}^{\sim} (b_i + a_i)\ x^i$$

$$= \sum_{i=o}^{\sim} b_i x^i + \sum_{i=o}^{\sim} a_i x^i$$

$$= g(x) + f(x)$$

4. $[f(x)+g(x)]+h(x) = \left[\sum_{i=o}^{\sim} (a_i + b_i)\ x^i \right] + \sum_{i=o}^{\sim} c_i x^i$

$$= \sum_{i=o}^{\sim} ((a_i + b_i) + c_i)\ x^i$$

$$= \sum_{i=o}^{\sim} (a_i + (b_i + c_i))\ x^i$$

$$= \sum_{i=o}^{\sim} a_i x^i + \sum_{i=o}^{\sim} (b_i + c_i) x^i$$

$$= \sum_{i=o}^{\sim} a_i x^i + \left[\sum_{i=o}^{\sim} b_i x^i + \sum_{i=o}^{\sim} c_i x^i \right]$$

$$= f(x) + [g(x) + h(x)]$$

5. Terdapat polinomial identitas yaitu $\sum_{i=o}^{\sim} 0x^i$ di dalam

R[x] sedemikian sehingga

$$\sum_{i=o}^{\sim} 0x^i + \sum_{i=o}^{\sim} a_i x^i = \sum_{i=o}^{\sim} (0+a_i)\, x^i = \sum_{i=o}^{\sim} a_i x^i$$

6. Untuk setiap $f(x) = \sum_{i=o}^{\sim} a_i x^i \in R[x]$ ada $-f(x)$, yaitu $\sum_{i=o}^{\sim}(-a_i)x^i \in R$ sedemikian sehingga

$$\begin{aligned} f(x) + (-f(x)) &= \sum_{i=o}^{\sim} a_i x^i + \sum_{i=o}^{\sim}(-a_i)x^i \\ &= \sum_{i=o}^{\sim} (a_i + (-a_i))x^i \\ &= \sum_{i=o}^{\sim} 0\, x^i \end{aligned}$$

7. $$(f(x).g(x)).h(x) = \left[\left(\sum_{i=o}^{\sim} a_i x^i\right)\left(\sum_{i=o}^{\sim} b_i x^i\right)\right]\left(\sum_{i=o}^{\sim} c_i x^i\right)$$

$$= \left[\sum_{i=o}^{\sim}\left(\sum_{k=o}^{i} a_k . b_{i-k}\right) x^i\right]\left(\sum_{i=o}^{\sim} c_i x^i\right)$$

$$= \sum_{l=o}^{\sim}\left[\sum_{i=o}^{l}\left(\sum_{j=o}^{i} a_j . b_{i-j}\right) c_{l-i}\right] x^l$$

$$= \sum_{l=o}^{\sim}\left[\sum_{i+j+k=l} a_i . b_j . c_k\right] x^l$$

$$= \sum_{l=o}^{\sim}\left[\sum_{p=o}^{\sim} a_{l-p}\left(\sum_{s=o}^{p} b_s . c_{p-s}\right)\right] x^l$$

$$= \left(\sum_{i=o}^{\sim} a_i x^i\right)\left[\sum_{p=o}^{\sim}\left(\sum_{s=o}^{p} b_s . c_{p-s}\right) x^p\right]$$

$$= \left(\sum_{i=o}^{\sim} a_i x^i\right)\left[\left(\sum_{i=o}^{\sim} b_i x^i\right)\left(\sum_{i=o}^{\sim} c_i x^i\right)\right]$$

$$= f(x).((g(x).h(x))$$

8. $f(x)\ [g(x) + h(x)]$

$$= \sum_{i=o}^{\sim} a_i x^i \left[\sum_{i=o}^{\sim} (b_i + c_i)\ x^i \right]$$

$$= \sum_{n=o}^{\sim} \left[\sum_{i=o}^{n} (a_i . (b_{n-i} + c_{n-i})) \right] x^n$$

$$= \sum_{n=o}^{\sim} \left[\sum_{i=o}^{n} (a_i . b_{n-i} + a_i . c_{n-i}) \right] x^n$$

$$= \sum_{n=o}^{\sim} \left[\sum_{i=o}^{n} a_i . b_{n-i} \right] x^n + \sum_{n=o}^{\sim} \left[\sum_{i=o}^{n} a_i . c_{n-i} \right] x^n$$

$$= \left[\sum_{i=o}^{\sim} a_i x^i \right] . \left[\sum_{i=o}^{\sim} b_i x^i \right] + \left[\sum_{i=o}^{\sim} a_i x^i \right] . \left[\sum_{i=o}^{\sim} c_i x^i \right]$$

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

9. $f(x).g(x) = \left[\sum_{i=o}^{\sim} a_i x^i \right] . \left[\sum_{i=o}^{\sim} b_i x^i \right]$

$$= \sum_{n=o}^{\sim} \left[\sum_{i=o}^{n} a_i . b_{n-i} \right] x^n$$

$$= \sum_{n=o}^{\sim} \left[\sum_{i=o}^{n} b_i . a_{n-i} \right] x^n$$

$$= \left[\sum_{i=o}^{\sim} b_i x^i \right] . \left[\sum_{i=o}^{\sim} a_i x^i \right]$$

$$= g(x).f(x)$$

■

Teorema 2.4.9

Jika R mempunyai elemen satuan e, maka R[x] juga mempunyai elemen satuan, yaitu ex^o.

Bukti

Untuk setiap $f(x) = \sum_{i=o}^{\sim} a_i x^i$ berlaku :

$$\left[\sum_{i=o}^{\sim} a_i x^i\right]\left[ex^o\right] = \sum_{i=o}^{\sim}\left[a_i x^i\, ex^o\right] = \sum_{i=}^{\sim}(a_i.e)x^{i+o}$$

$$= \sum_{i=o}^{\sim} a_i x^i \qquad \blacksquare$$

Teorema 2.4.10

Jika R adalah ring komutatif yang tidak memuat pembagi nol, maka ring R[x] juga tidak memuat pembagi nol.

Bukti

Diketahui R adalah ring komutatif yang tidak memuat pembagi nol. Misalkan f(x), g(x) di dalam R[x] di mana $f(x) \neq 0$ dengan koefisien utama yaitu $a_m \neq 0$ dan $g(x) \neq 0$ dengan koefisien utama yaitu $b_n \neq 0$. Maka

$f(x).g(x) = a_o b_o + (a_o b_1 + a_1 b_o)x + \ldots + a_m b_n\, x^{m+n} \neq 0$

sebab $a_m b_n \neq 0$.

Jadi R[x] tidak memuat pembagi nol. $\blacksquare$

Akibat

Jika R daerah integral, maka R[x] daerah integral.

Bukti

Dari teorema 2.4.8, 2.4.9, 2.4.10 diperoleh kesimpulan

bahwa jika R daerah integral, maka R[x] adalah daerah integral. ■

Teorema 2.4.11

Jika R suatu lapangan dan $f(x) \neq 0$, $g(x) \neq 0$ di dalam R[x], maka $d(f(x).g(x)) = d(f(x)) + d(g(x))$.

Bukti

Misalkan $d(f(x)) = n$ dan $d(g(x)) = m$. Maka

$f(x) = a_o + a_1 x + \ldots + a_n x^n$, $a_n \neq 0$

$g(x) = b_o + b_1 x + \ldots + b_m x^m$, $b_m \neq 0$

Dari definisi operasi perkalian dua polinomial diperoleh :

$f(x).g(x) = a_o b_o + (a_o b_1 + a_1 b_o) x + \ldots + a_n b_m x^{n+m}$.

Jadi $d(f(x).g(x)) = m+n$, yaitu $d(f(x).g(x)) = d(f(x)) + d(g(x))$. ■

Definisi 2.4.8

Bila $f(x), g(x), h(x) \in R[x]$ dan $d(f(x)) \geq 1$, maka f(x) disebut polinomial *tak teredusir* bila dan hanya bila jika $f(x) = g(x).h(x)$, maka $d(g(x)) = 0$ atau $d(h(x)) = 0$.

Teorema 2.4.12 (Algoritma Pembagian)

Jika f(x) dan g(x) di dalam F[x] di mana F suatu lapangan, dan $g(x) \neq 0$, maka ada dengan tunggal polinomial q(x) dan r(x) atas F sedemikian sehingga

$f(x) = g(x).q(x) + r(x)$ dengan $r(x) = 0$ atau $d(r(x)) < d(g(x))$. Polinomial-polinomial $q(x)$ dan $r(x)$ tersebut berturut-turut disebut *hasil bagi* dan *sisa* pembagian $f(x)$ oleh $g(x)$.

Bukti

1. Jika $d(f(x)) < d(g(x))$, maka ada $q(x) = 0$ dan $r(x) = f(x)$ sehingga $f(x) = g(x) \cdot 0 + r(x)$ dengan $d(r(x)) < d(g(x))$.
2. Andaikan $f(x) = \sum_{i=0}^{m} a_i x^i$ di mana $a_m \neq 0$ dan $g(x) = \sum_{i=0}^{n} b_i x^i$ dengan $m \geq n$. Akan dibuktikan dengan induksi matematik.

   Jika $m = 0$, maka $f(x) = a_o$ dan $g(x) = b_o$. Jadi ada $q(x) = b_o^{-1}.a_o$ dan $r(x) = 0$ sedemikian sehingga $a_o = b_o.b_o^{-1}.a_o + 0$.

   Andaikan algoritma pembagian dipenuhi untuk derajat $f(x) < m$.

   Andaikan $f_1(x) = f(x) - a_m.b_n^{-1}x^{m-n}g(x)$. Maka derajat $f_1(x) <$ derajat $f(x)$, sebab

   $f_1(x) = f(x) - (a_m.b_n^{-1}x^{m-n}g(x))$

   $= (a_o + a_1x^1 + a_2x^2 + \ldots + a_{m-1}x^{m-1} + a_mx^m) - (a_m.b_n^{-1}x^{m-n})(b_o + b_1x^1 + \ldots + b_{n-1}x^{n-1} + b_nx^n)$

   $= (a_o + a_1x^1 + a_2x^2 + \ldots + a_{m-1}x^{m-1} + a_mx^m) - (a_m.b_o.b_n^{-1}x^{m-n} + a_m.b_1.b_n^{-1}x^{m-n+1} + \ldots + a_m.b_{n-1}.b_n^{-1}x^{m-1} + a_m.b_n.b_n^{-1}x^m)$

   $= (a_o + a_1x^1 + a_2x^2 + \ldots + a_{m-1}x^{m-1} + a_mx^m) -$

$$(a_m . b_o . b_n^{-1} x^{m-n} + a_m . b_1 . b_n^{-1} x^{m-n+1} + \ldots +$$
$$a_m . b_{n-1} . b_n^{-1} x^{m-1} + a_m . e . x^m)$$
$$= (a_o + a_1 x^1 + a_2 x^2 + \ldots + a_{m-1} x^{m-1} + a_m x^m) - (a_m . b_o . b_n^{-1} x^{m-n} + a_m . b_1 . b_n^{-1} x^{m-n+1} + \ldots + a_m . b_{n-1} . b_n^{-1} x^{m-1} + a_m x^m)$$
$$= (a_o + a_1 x^1 + a_2 x^2 + \ldots + (a_{m-1} - a_m . b_{n-1} . b_n^{-1}) x^{m-1} .$$

Jadi menurut pengandaian di atas terdapat polinomial $q_1(x)$ dan $r_1(x)$ sedemikian sehingga $f_1(x) = g(x) . q_1(x) + r_1(x)$ dengan $r_1(x) = 0$ atau $d(r_1(x)) < d(g(x))$.

Jadi $f(x) - a_m . b_n^{-1} x^{m-n} g(x) = g(x) . q_1(x) + r_1(x)$.

$f(x) = g(x) . q_1(x) + a_m . b_n^{-1} x^{m-n} . g(x) + r_1(x)$

$f(x) = g(x)[q_1(x) + a_m b_n^{-1} x^{m-n}] + r_1(x)$.

Jadi ada $q(x) = q_1(x) + a_m . b_n^{-1} x^{m-n}$ dan $r(x) = r_1(x)$ sedemikian sehingga $f(x) = g(x) . q(x) + r(x)$.

Selanjutnya akan dibuktikan bahwa $g(x)$ dan $r(x)$ tunggal.

Andaikan ada polinomial lain yaitu $q_2(x)$ dan $r_2(x) \in F[x]$, sedemikian sehingga $f(x) = g(x).q_2(x) + r_2(x)$ dengan $r_2(x) = 0$ atau $d(r_2(x)) < d(g(x))$. Maka $g(x).q(x) + r(x) = g(x).q_2(x) + r_2(x)$, sehingga $g(x)[q(x)-q_2(x)] = r_2(x) - r(x)$.

Karena $r_2(x) - r(x) = 0$ atau derajat $[r_2(x)-r(x)]$ < derajat $g(x)$, dan $g(x) \neq 0$, maka haruslah $q(x)-q_2(x) = 0$.

Jadi $q_2(x) = q(x)$ dan $r_2(x) = r(x)$. ■

Contoh 2.4.3

$f(x) = 8x^4 + 18x^3 + 3x^2 - 12x + 5 \in \mathbb{R}[x]$ dan

$g(x) = 2x + 1 \in \mathbb{R}[x]$

$$
\begin{array}{r|l}
 & 4x^3 + 7x^2 - 2x - 5 \\
\hline
2x + 1 & 8x^4 + 18x^3 + 3x^2 - 12x + 5 \\
 & \underline{8x^4 + 4x^3} \quad - \\
 & 14x^3 + 3x^2 \\
 & \underline{14x^3 + 7x^2} \quad - \\
 & -4x^2 - 12x \\
 & \underline{-4x^2 - 2x} \quad - \\
 & -10x + 5 \\
 & \underline{-10x - 5} \quad - \\
 & 10
\end{array}
$$

Dari perhitungan di atas dihasilkan

$q(x) = 4x^3 + 7x^2 - 2x - 5$ dan $r(x) = 10$. Jadi

$$8x^4 + 18x^3 + 3x^2 - 12x + 5 = (2x + 1)(4x^3 + 7x^2 - 2x - 5) + 10$$

Contoh 2.4.4

$f(x) = x^4 + x^3 + 4x^2 + x \in \mathbb{Z}_5[x]$

$g(x) = x^2 + 4x \in \mathbb{Z}_5[x]$

$$
\begin{array}{r}
x^2 + 2x + 1 \\
x^2 + 4x \;\overline{)\; x^4 + x^3 + 4x^2 + x} \\
\underline{x^4 + 4x^3} \quad - \\
2x^3 + 4x^2 \\
\underline{2x^3 + 3x^2} \quad - \\
x^2 + x \\
\underline{x^2 + 4x} \quad - \\
2x
\end{array}
$$

Diperoleh $q(x) = x^2 + 2x + 1$ dan $r(x) = 2x$.

Jadi $x^4 + x^3 + 4x^2 + x = (x^2 + 4x)(x^2 + 2x + 1) + 2x$.

Teorema 2.4.13

Jika $f(x) \in F[x]$ dan $c \in F$, maka sisa pembagian $f(x)$ oleh $x-c$ adalah $f(c)$.

Bukti

Andaikan hasil bagi $f(x)$ oleh $x-c$ adalah $q(x) \in F[x]$ dan sisanya r. Maka $f(x) = (x-c).\, q(x) + r$. Bila c disubtitusikan untuk x, maka diperoleh :

$f(c) = (c-c).\, q(c) + r$

$= 0.\, q(c) + r$

$= r$

Jadi sisa pembagi $f(x)$ oleh $x-c$ adalah $r = f(c)$. ■

Teorema di atas dikenal sebagai *Teorema Sisa*.

Jika $f(x), g(x) \in F[x]$ dengan $g(x) \neq 0$, maka $f(x)$

dikatakan *habis dibagi* oleh g(x), jika f(x) = g(x).q(x). Dalam hal ini g(x) disebut *faktor* dari f(x), dan dikatakan g(x) *membagi* f(x), dan ditulis dengan notasi g(x)|f(x).

Teorema 2,4 14

Jika f(x) ∈ F[x] dan c ∈ F, maka x-c merupakan faktor dari f(x) bila dan hanya bila f(c) = 0.

Bukti

1. ⇒

Diketahui f(x) ∈ F[x], c ∈ F, dan x-c faktor dari f(x). Karena x-c faktor dari f(x), maka f(x) = (x-c).q(x). Jika diambil x = c, maka diperoleh f(c) = 0.

2. ⇐

Diketahui c ∈ F dan f(c) = 0. Menurut teorema 2.4.13 f(x) = (x-c).q(x) + f(c). Karena f(c) = 0 maka f(x) = (x-c)q(x), yaitu x-c faktor dari f(x). ■

Definisi 2.4.9

Elemen c ∈ F disebut *akar* dari polinomial f(x) ∈ F[x] jika f(c) = 0 .

Menurut teorema 2.4.14, c adalah akar dari f(x) bila dan hanya bila x-c merupakan faktor dari f(x).

Teorema 2.4.15

Jika F lapangan, $f(x) \in F[x]$, $f(x) \neq 0$ dan derajat $f(x)=n$, maka $f(x)$ mempunyai paling banyak n akar di F.

Bukti

Diketahui derajat dari $f(x) = n$.

Andaikan $r_1, r_2, r_3, \ldots, r_n$ adalah akar-akar berlainan dari $f(x)$. Sehingga $f(x) = (x-r_1).f_1(x)$ dengan derajat $f_1(x) = n-1$. Karena r_2 merupakan akar dari $f(x)$, maka $f(r_2) = 0$.

Sehingga $f(r_2) = (r_2-r_1).f_1(r_2)$

$0 = (r_2-r_1).f_1(r_2)$

Karena $r_1 \neq r_2$ dan F[x] daerah integral, maka haruslah $f_1(r_2) = 0$. Jadi $x-r_2$ merupakan faktor dari $f_1(x)$. Sehingga diperoleh :

$f(x) = (x-r_1).(x-r_2).f_2(x)$ dengan derajat $f_2(x) = n-2$.

Dengan cara yang sama akhirnya diperoleh

$f(x) = a.(x-r_1).(x-r_2)\ldots(x-r_n)$ di mana $a \neq 0$ merupakan koefisien utama dari $f(x)$. Misalkan r akar dari $f(x)$. Maka $f(r) = a.(r-r_1)(r-r_2)\ldots(r-r_n)$

$0 = a.(r-r_1).(r-r_2)\ldots(r-r_n)$

Karena F[x] tidak memuat pembagi nol dan $a \neq 0$, maka pastilah salah satu diantara $r-r_i = 0$ di mana $i = 1,2,3,\ldots,n$. Jadi r adalah salah satu dari $r_1, r_2, \ldots, r_n$. Jadi terbukti bahwa $f(x)$ dengan derajat n mempunyai paling banyak n akar yang berlainan. ■

Definisi 2.4.10

Misalkan a(x) dan b(x) adalah polinomial atas lapangan F yang tidak keduanya polinomial nol. *Faktor persekutuan* dari a(x) dan b(x) adalah polinomial h(x) sedemikian sehingga $h(x) \mid a(x)$ dan $h(x) \mid b(x)$.

Suatu polinomial $d(x) \in F[x]$ disebut *faktor persekutuan terbesar* (FPB) dari a(x) dan b(x) jika :

(i) d(x) merupakan faktor persekutuan dari a(x) dan b(x).

(ii) Untuk sebarang $h(x) \in F[x]$ yang merupakan faktor persekutuan dari a(x) dan b(x), maka $h(x) \mid d(x)$.

Teorema 2.4.16

Jika $f(x)$ dan $g(x) \in F[x]$ di mana F lapangan dan $f(x)$ dan $g(x)$ bukan keduanya polinomial nol, maka ada polinomial $h(x)$ yang merupakan FPB dari $f(x)$ dan $g(x)$.

Bukti

Jika $g(x) \neq 0$, maka menurut algoritma pembagian ada dengan tunggal polinomial $q_1(x)$ dan $r_1(x)$ yang memenuhi $f(x) = g(x).q_1(x) + r_1(x)$ dengan $r_1(x) = 0$ atau $d(r_1(x)) < d(g(x))$.

(i). Bila $r_1(x) = 0$, maka $g(x)$ merupakan FPB dari $f(x)$ dan $g(x)$.

(ii). Jika $r_1(x) \neq 0$, maka dengan algoritma pembagian didapat $q_2(x)$ dan $r_2(x)$ sedemikian sehingga :

$g(x) = r_1(x).q_2(x) + r_2(x)$ dengan $r_2(x) = 0$ atau $d(r_2(x)) < d(r_1(x))$. Dengan mengulangi algoritma tersebut beberapa kali akan diperoleh :

$f(x) = g(x).q_1(x) + r_1(x)$, $d(r_1(x)) < d(g(x))$

$g(x) = r_1(x)q_2(x) + r_2(x)$, $d(r_2(x)) < d(r_1(x))$

.

.

$r_{i-2}(x) = r_{i-1}(x)\, q_i(x) + r_i(x)$ dengan $d(r_i(x)) < d(r_{i-1}(x))$

$r_{i-1}(x) = r_i(x)\, q_{i+1}(x)$

Karena $d(g(x)) > d(r_1(x)) > d(r_2(x)) > \ldots$, maka pada akhirnya akan diperoleh sisa polinomial nol Andaikan $r_i(x)$ adalah sisa terakhir yang tidak nol. Perhatikan bahwa $r_i(x) | r_{i-1}(x)$, dan selanjutnya diperoleh $r_i(x) | r_{i-2}(x)$, $r_i(x) | r_{i-3}(x)$,.... $r_i(x) | g(x)$, $r_i(x) | f(x)$, sehingga $r_i(x)$ merupakan faktor persekutuan dari $f(x)$ dan $g(x)$.

Akan dibuktikan bahwa $r_i(x)$ merupakan FPB.

Andaikan $c(x) | f(x)$ dan $c(x) | g(x)$. Maka $c(x) | r_1(x)$ Tapi karena $c(x) | g(x)$ dan $c(x) | r_1(x)$, maka $c(x) | r_2(x)$. Demikian seterusnya sehingga pada akhirnya diperoleh :

$c(x) | r_1(x)$, $c(x) | r_2(x)$, ..., $c(x) | r_i(x)$.

Terbukti bahwa ada polinomial $h(x) = r_i(x)$ yang merupakan FPB dari $f(x)$ dan $g(x)$. ■

Teorema 2.4.17

Jika f(x) dan g(x) adalah polinomial-polinomial atas lapangan F yang bukan keduanya adalah polnomial nol dan h(x) adalah FPB dari f(x) dan g(x), maka ada polinomial u(x) dan v(x) atas F sedemikian sehingga h(x) = f(x).u(x) + g(x).v(x).

Bukti

Pada pembuktian teorema 2.4.16 diperoleh :

$r_{i-2}(x) = r_{i-1}(x).\, q_i(x) + r_i(x)$. Maka

$r_i(x) = r_{i-2}(x) - r_{i-1}(x).\, q_i(x)$ .....(1)

Sehingga $r_i(x)$ dapat dinyatakan sebagai jumlahan hasil kali suatu polinomial dengan $r_{i-1}(x)$ dan hasil suatu polinomial dengan $r_{i-2}(x)$.

$r_{i-9}(x) = r_{i-2}(x).q_{i-1}(x) + r_{i-1}(x)$.....(2)

Dari persamaan (1) dan (2) diperoleh :

$r_i(x) = r_{i-2}(x) - [r_{i-9}(x) - r_{i-2}(x)\, q_{i-1}(x)]q_i(x)$

$= r_{i-2}(x)\,[1 + q_{i-1}(x).q_i(x)] - r_{i-9}(x).q_i(x)$..(3)

Jadi $r_i(x)$ dapat dinyatakan sebagai jumlahan hasil kali suatu polinomial dengan $r_{i-2}(x)$ dan hasil kali suatu polinomial dengan $r_{i-9}(x)$.

$r_{i-4}(x) = r_{i-9}(x).q_{i-2}(x) + r_{i-2}(x)$.....(4)

Dari persamaan (3) dan (4) disimpulkan bahwa $r_i(x)$ dapat dinyatakan sebagai jumlahan hasil kali suatu polinomial dengan $r_{i-9}(x)$ dan hasil kali suatu polinomial dengan $r_{i-4}(x)$. Bila proses diteruskan, maka $r_i(x)$ dapat dinyatakan sebagai jumlahan hasil kali

suatu polinomial dengan $r_1(x)$ dan hasil kali suatu polinomial dengan g(x). Dan akhirnya $r_i(x)$ dapat dinyatakan sebagai jumlahan hasil kali suatu polinomial u(x) dengan f(x) dan hasil kali suatu polinomial v(x) dengan g(x), yaitu $r_i(x) = u(x).f(x) + v(x).g(x)$. Dalam hal ini FPB dari f(x) dan g(x) adalah $h(x) = r_i(x)$. Maka $h(x) = f(x).u(x) + g(x).v(x)$. ■

Teorema 2.4.18

Jika F lapangan, maka setiap ideal dari ring polinomial F[x] adalah ideal utama.

Bukti

Misalkan I adalah sebarang ideal dari F[x]. Jika $I = \{0\}$, maka I adalah ideal utama. Jika $I \neq \{0\}$, misalkan g(x) adalah polinomial dengan derajat paling kecil di antara polinomial-polinomial yang tidak sama dengan nol dalam I.

Akan dibuktikan $I = \langle g(x) \rangle$.

Jelas bahwa $\langle g(x) \rangle \subseteq I$.

Misalkan $f(x) \in I$. Maka menurut algoritma pembagian terdapat polinomial q(x) dan $r(x) \in F[x]$ sedemikian sehingga $f(x) = g(x).q(x) + r(x)$ dengan $r(x) = 0$ atau $d(r(x)) < d(g(x))$. Karena $f(x) \in I$ dan $g(x)q(x) \in I$, maka $r(x) = f(x) - g(x).q(x) \in I$.

Maka haruslah $r(x) = 0$, sebab tidak mungkin bahwa $d(r(x)) < d(g(x))$, mengingat bahwa g(x) adalah

polinomial dengan derajat paling kecil dalam I.

Jadi $f(x) = g(x).q(x) \in \langle g(x) \rangle$.

Jadi $I \subseteq \langle g(x) \rangle$, sehingga terbukti bahwa $I = \langle g(x) \rangle$. ■

Teorema 2.4.19

Bila F lapangan dan $p(x) \in F[x]$, maka ring faktor $F[x]/\langle p(x) \rangle$ adalah lapangan bila dan hanya bila p(x) adalah polinomial tak teredusir atas F.

Bukti

Andaikan I adalah ideal utama yang dibentuk oleh p(x) yaitu $I = \langle p(x) \rangle$.

1. ⇒

   Diketahui F[x]/I adalah lapangan, akan dibuktikan bahwa p(x) adalah polinomial tak teredusir atas F.

   Andaikan p(x) adalah polinomial teredusir. Maka ada polinomial a(x) dan $b(x) \in F[x]$ sedemikian sehingga $p(x) = a(x)b(x)$ dengan derajat a(x) dan b(x) tidak sama dengan nol dan kurang dari derajat p(x). Derajat polinomial yang tidak sama dengan nol dalam I paling sedikit harus sama dengan derajat p(x), maka $a(x) \notin I$ dan $b(x) \notin I$. Jadi $I + a(x)$ dan $I + b(x)$ keduanya bukan merupakan elemen nol (yaitu I) dari F[x]/I. Akan tetapi :

   $(I + a(x))(I + b(x)) = I + a(x)b(x) = I + p(x) = I$

   adalah elemen nol dari F[x]/I. Jadi F[x]/I memuat pembagi nol, sehingga F[x]/I bukan lapangan .

2. ←

Diketahui p(x) adalah polinomial tak teredusir atas F, akan dibuktikan bahwa F[x]/I adalah suatu lapangan.

a. F[x]/I merupakan ring komutatif dengan elemen satuan karena F lapangan.

b. Untuk setiap I+f(x) ≠ I di dalam F[x]/I, maka f(x) ∉ I, yang berarti f(x) bukan perkalian dari p(x) di dalam F[x]. Karena p(x) suatu polinomial yang tak teredusir, maka p(x) dan f(x) mempunyai FPB sama dengan e. Sehingga e = p(x).u(x) + f(x).v(x), untuk suatu u(x) dan v(x) di dalam F[x]. Maka I+e = I + (p(x).u(x) + f(x).v(x))

= (I + p(x).u(x)) + (I + f(x).v(x))

= I + f(x).v(x)

= (I+f(x)).(I+v(x))

Jadi terdapat I+v(x) di dalam F[x]/I sedemikian sehingga (I+f(x)).(I+v(x)) = I+e.

Jadi terbukti bahwa setiap I + f(x) ≠ I ∈ F[x]/I mempunyai invers.

Terbukti bahwa F[x]/I adalah lapangan. ■

Teorema 2.4.20

Andaikan F adalah lapangan, $p(x) = a_0+a_1x+a_2x^2+\ldots+a_nx^n$ adalah polinomial berderajat n atas F dan I adalah ideal <p(x)> dari F(x), maka setiap elemen dari F[x]/I

dapat dinyatakan secara tunggal dalam bentuk :

$I + (b_0+b_1x+b_2x^2+\ldots+b_{n-1}x^{n-1})$ dengan $b_0, b_1, b_2, \ldots, b_{n-1} \in F$

Dan juga bila p(x) polinomial tak teredusir, maka $\{I+b \mid b \in F\}$ adalah lapangan bagian dari F[x]/I yang isomorfik dengan F.

Bukti

Ambil sebarang elemen $I+f(x) \in F[x]/I$. Dengan algoritma pembagian diperoleh $f(x) = p(x).q(x)+r(x)$, untuk $q(x), r(x) \in F[x]$ dengan $d(r(x)) < d(p(x))$ atau $r(x) = 0$. Maka $f(x)-r(x) = p(x).q(x) \in I$ sehingga $I+f(x) = I+r(x)$. Jadi setiap elemen dari F[x]/I dapat dinyatakan paling sedikit dengan satu cara dalam bentuk $I + (b_0+b_1x+b_2x^2+\ldots+b_{n-1}x^{n-1})$ dengan $b_0, b_1, b_2, \ldots, b_{n-1} \in F$.Andaikan $I+f(x) \in F[x]/I$ dapat ditulis dengan cara lain misalnya

$I + (c_0+c_1x+c_2x^2+\ldots+c_{n-1}x^{n-1})$ dengan $c_0, c_1, c_2, \ldots, c_{n-1} \in F$. Maka

$I + (b_0+b_1x+b_2x^2+\ldots+b_{n-1}x^{n-1}) = I + (c_0+c_1x+c_2x^2+\ldots+c_{n-1}x^{n-1})$

sehingga $(b_0+b_1x+b_2x^2+\ldots+b_{n-1}x^{n-1}) + (-(c_0+c_1x+c_2x^2+\ldots+c_{n-1}x^{n-1}) \in I$, yaitu $(b_0-c_0)+(b_1-c_1)x+\ldots+(b_{n-1}-c_{n-1})x^{n-1} \in I$, berarti

$p(x) \mid (b_0-c_0)+(b_1-c_1)x+\ldots+(b_{n-1}-c_{n-1})x^{n-1}$.

Karena derajat $p(x) = n > n-1$, maka haruslah

$(b_0-c_0)+(b_1-c_1)x+\ldots+(b_{n-1}-c_{n-1})x^{n-1} = 0$, sehingga $b_i = c_i$ untuk $i = 0,1,\ldots,n-1$.

Jadi $I + f(x)$ dapat dinyatakan secara tunggal dalam

bentuk seperti di atas.

Selanjutnya akan dibuktikan bahwa $\{I + b \mid b \in F\}$ adalah lapangan bagian dari $F[x]/I$.

Andaikan $A = \{I + b \mid b \in F\}$. Jelas $A \subset F[x]/I$, karena setiap elemen $I + b \in A$ pasti di dalam $F[x]/I$.

1. A memuat elemen identitas dari $F[x]/I$, yaitu $I + 0 = I$ dan elemen satuan dari $F[x]/I$ yaitu $I + e$.
2. Jika $I + a$, $I + b$ di dalam A, maka $(I + a) + (I + b) = I + (a + b) \in A$ dan $(I + a)(I + b) = I + ab \in A$.
3. Jika $I + a \in A$, maka $I + (-a) \in A$.
4. Untuk semua $I + a \neq I$ di dalam A, maka $a \neq 0$ dan invers dari $I + a$, yaitu $I + a^{-1} \in A$ karena a^{-1} di dalam F.

Jadi terbukti bahwa A merupakan lapangan bagian dari ring faktor $F[x]/I$.

Andaikan θ adalah pemetaan dari F ke $A = \{I + b \mid b \in F\}$ yang didefinisikan dengan aturan $\theta(b) = I+b$, untuk semua $b \in F$. Definisi tersebut well-defined, sebab untuk setiap $a, b \in F$, bila $a = b$ maka $I + a = I + b$ sehingga $\theta(a) = \theta(b)$. Untuk setiap $a, b \in F$ berlaku :

$$\theta(a + b) = I + (a + b)$$
$$= (I + a)+(I + b)$$
$$= \theta(a) + \theta(b)$$

dan $\theta(a.b) = I + a.b$

$$= (I + a).(I + b)$$
$$= \theta(a).\theta(b)$$

Jadi θ adalah homomorfisma ring.

Ambil sebarang elemen $a,b \in F$ sedemikian sehingga $\theta(a)=\theta(b)$, maka $I+a = I+b$. Sehingga $a-b \in I$, yang berarti $a-b$ habis dibagi $p(x)$. Karena $d(p(x)) > d(a-b)$, maka haruslah $a-b = 0$, sehingga $a = b$ .Jadi θ injektif.

Ambil sebarang elemen $y \in A = \{ I+b \mid b \in F \}$. Maka $y = I + a$, untuk suatu $a \in F$. Jadi ada $a \in F$ sedemikian sehingga $\theta(a) = I + a = y$. Jadi θ surjektif.

Jadi terbukti bahwa A isomorfik dengan F. ■

BAB III
LAPANGAN PERLUASAN

Bab ini terdiri dari dua subbab. Subbab pertama membahas tentang ruang vektor, yang diperlukan dalam pembahasan tentang lapangan perluasan. Subbab ke dua membahas tentang lapangan perluasan.

1. Ruang Vektor

Definisi 3.1.1

Suatu *ruang vektor* atas lapangan F adalah suatu himpunan V bersama dengan suatu operasi jumlahan (+) di dalam V dan suatu pemetaan θ : FxV ——> V yang didefinisikan dengan $\theta(\alpha, v) = \alpha v$ dan memenuhi aksioma-aksioma berikut :

1. V adalah grup abel terhadap operasi jumlahan
2. $\alpha(v+w) = \alpha v + \alpha w$
3. $(\alpha+\beta)v = \alpha v + \beta v$
4. $(\alpha\beta)v = \alpha(\beta v)$
5. $ev = v$,

untuk setiap $\alpha, \beta \in F$ dan $v, w \in V$ dengan e adalah elemen satuan dari F.

Elemen-elemen di dalam V dinamakan *vektor-vektor*, elemen-elemen di dalam F dinamakan *skalar-skalar* dan α v

dinamakan *perkalian dengan skalar*, di mana $\alpha \in F$ dan $v \in V$.

Contoh 3.1.1

Jika V = F[x] adalah himpunan semua polinomial-polino - mial dalam x dengan koefisien-koefisiennya dalam lapangan F, maka V adalah ruang vektor atas lapangan F dengan operasi jumlahan dan perkalian dengan skalar seperti didefinisikan dalam definisi 2.4.6.

Bukti

1. Menurut teorema 2.4.8, F[x] merupakan grup abel ter- hadap operasi jumlahan.
2. Dengan memandang sebarang $\alpha, \beta \in F$ sebagai polinomial konstan dalam F[x], maka menurut teorema 2.4.8, aksioma-aksioma berikut dipenuhi yaitu :

   i) $\alpha(g(x)+h(x)) = \alpha g(x)+\alpha h(x)$

   ii) $(\alpha+\beta)g(x) = \alpha g(x) + \beta g(x)$

   iii) $(\alpha\beta)g(x) = \alpha(\beta(g(x))$.

   di mana g(x) dan h(x) adalah sebarang polinomial dalam F[x].
3. Ambil sebarang $g(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$. Bila e adalah elemen satuan dalam F, maka diperoleh :

$$eg(x) = e\sum_{i=0}^{n} a_i x^i$$
$$= \sum_{i=0}^{n} (ea_i)x^i$$
$$= \sum_{i=0}^{n} a_i x^i$$

$eg(x) = g(x)$

Terbukti bahwa F[x] merupakan ruang vektor atas lapangan F. ■

Teorema 3.1.1

Andaikan V ruang vektor atas lapangan F, maka berlakulah :

1. $\alpha 0 = 0, \forall\ \alpha \in F$ dan $0 \in V$.
2. $0x = 0, \forall\ x \in V$ dan $0 \in F$
3. $(-\alpha)x = \alpha\ (-x) = -(\alpha\ x), \forall\ \alpha \in F$ dan $\forall\ x \in V$

Bukti

1. Ambil sebarang elemen $\alpha \in F$ dan $0 \in V$, maka

   $\alpha\ x + \alpha\ 0 = \alpha\ (\ x + 0\ ) = \alpha\ x$

   $-(\alpha\ x) + \alpha\ x + \alpha\ 0 = -(\alpha\ x) + \alpha\ x$

   $\alpha\ 0 = 0$

2. Ambil sebarang $x \in V$ dan $0 \in F$, maka

   $\alpha\ x + 0\ x = (\ \alpha + 0\ )\ x = \alpha\ x$

   $-(\alpha\ x) + \alpha\ x + 0\ x = -(\alpha\ x) + \alpha\ x$

   $0\ x = 0$

3. Dari nomor 2 di atas diperoleh :

   $0 = 0\ x = [(-\alpha) + \alpha\ ]\ x = (-\alpha)\ x + \alpha\ x$

   Jadi $(-\alpha)\ x = -(\alpha x)$ .....i)

   Selanjutnya dari nomor 1 di atas diperoleh :

   $0 = \alpha\ 0 = \alpha\ [\ (-x) + x\ ] = \alpha\ (-x) + \alpha\ x$

   Jadi $\alpha\ (-x) = -\ (\alpha\ x)$.....ii)

Dari i) dan ii) diperoleh :

$(-\alpha)\ x = \alpha\ (-x) = -\ (\alpha\ x)$ ■

Definisi 3.1.2

Andaikan V adalah suatu ruang vektor atas lapangan F. Jika $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n \in F$ dan $v_1, v_2, v_3, \ldots, v_n \in V$, maka $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \ldots + \alpha_n v_n$ dinamakan *kombinasi linear* dari $v_1, v_2, v_3, \ldots, v_n$.

Himpunan semua kombinasi linear dari $v_1, v_2, v_3, \ldots, v_n$ disebut *rentang* dari $v_1, v_2, v_3, \ldots, v_n$. Rentang dari $v_1, v_2, v_3, \ldots, v_n$ akan ditulis dengan $S(v_1, v_2, v_3, \ldots, v_n)$.

Definisi 3.1.3

Himpunan vektor-vektor $\{v_1, v_2, v_3, \ldots, v_n\}$ dikatakan *bebas linear* bila dan hanya bila jika $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \ldots + \alpha_n v_n = 0$, maka $\alpha_1 = \alpha_2 = \alpha_3 = \ldots = \alpha_n = 0$ untuk setiap $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n \in F$.

Himpunan vektor-vektor $\{v_1, v_2, v_3, \ldots, v_n\}$ dikatakan *tak bebas linear* bila dan hanya bila ada skalar-skalar $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ yang tidak semuanya nol sedemikian sehingga $\alpha_1 v_1 + \alpha_2 v_2 + \alpha_3 v_3 + \ldots + \alpha_n v_n = 0$.

Contoh 3.1.2

Andaikan V = F[x] yang merupakan ruang vektor atas

lapangan F . Maka $\{e, x, x^2, \ldots, x^n\}$ adalah himpunan bagian dari V yang bebas linear, sebab jika $\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n = 0$, maka haruslah $\alpha_1 = \alpha_2 = \alpha_3 = \ldots = \alpha_n = 0$. ■

Teorema 3.1.2

Jika suatu himpunan vektor-vektor $S = \{ v_1, v_2, \ldots, v_n \}$ adalah tak bebas linear, maka ada suatu vektor v_k dalam S yang dapat dinyatakan sebagai kombinasi linear dari n-1 vektor-vektor lainnya.

Bukti

Himpunan S adalah tak bebas linear, maka ada $\alpha_k \neq 0$, sedemikian sehingga $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_k v_k + \ldots + \alpha_n v_n = 0$.

Maka $v_k = \left(-\frac{\alpha_1}{\alpha_k}\right) v_1 + \left(-\frac{\alpha_2}{\alpha_k}\right) v_2 + \ldots + \left(-\frac{\alpha_{k-1}}{\alpha_k}\right) v_{k-1} + \left(-\frac{\alpha_{k+1}}{\alpha_k}\right) v_{k+1} + \ldots + \left(-\frac{\alpha_n}{\alpha_k}\right) v_n$. Jadi v_k dapat dinyatakan sebagai kombinasi linear dari (n-1) vektor-vektor lainnya. ■

Teorema 3.1.3

Jika vektor u dapat dinyatakan sebagai kombinasi linear dari himpunan vektor-vektor $\{ v_1, v_2, \ldots, v_n \}$, maka himpunan vektor-vektor $\{ v_1, v_2, \ldots, v_n, u \}$ adalah tak bebas linear.

Bukti

Andaikan $u = \alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n$, maka $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n - u = 0$. Jadi $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n + (-e)u = 0$, di mana $-e \neq 0$. Jadi himpunan vektor-vektor $\{v_1, v_2, \ldots, v_n, u\}$ adalah tak bebas linear. ■

Definisi 3.1.4

Himpunan bagian $B = \{v_1, v_2, v_3, \ldots, v_n\}$ dari ruang vektor V disebut *basis* dari ruang vektor V bila dan hanya bila

1. Vektor-vektor dalam B bebas linear.
2. Setiap vektor dari V dapat dinyatakan sebagai kombinasi linear dari vektor-vektor dalam B (dikatakan *B merentang V*).

Definisi 3.1.5

Ruang vektor V dikatakan *berdimensi berhinggga* jika ada himpunan berhingga vektor-vektor yang merentang V.
Bila tidak demikian, maka kita katakan ruang vektor V *berdimensi tak berhingga*.

Teorema 3.1.4

Andaikan V merupakan ruang vektor atas lapangan F yang berdimensi berhingga. Andaikan $v_1, v_2, \ldots, v_m$ adalah himpunan yang bebas linear dalam V, maka ada

vektor-vektor $v_{m+1}, v_{m+2}, \ldots, v_{m+p}$ dari V sedemikian sehingga $\{v_1, v_2, \ldots, v_m, v_{m+1}, v_{m+2}, \ldots, v_{m+p}\}$ merupakan basis.

Bukti

Andaikan $\{w_1, w_2, \ldots, w_n\}$ merupakan basis dari ruang vektor V. Perhatikan himpunan S = $\{v_1, v_2, \ldots, v_m, w_1, w_2, \ldots, w_n\}$. Himpunan tersebut merupakan himpunan yang tak bebas linear, karena semua v_i dapat dinyatakan sebagai kombinasi linear dari w_j. Jadi menurut teorema 3.1.2 ada vektor Z dalam S yang dapat dinyatakan sebagai kombinasi linear dari vektor-vektor lainnya. Karena v_i adalah bebas linear, maka $z \neq v_i$ untuk setiap i tetapi $z = w_i$ untuk suatu i. Selanjutnya perhatikan $\{v_1, v_2, \ldots, v_m, w_{i-1}, w_{i+1}, \ldots, w_n\}$. Setiap vektor dari V dapat dinyatakan sebagai kombinasi linear dari vektor-vektor tersebut. Jika vektor-vektor tersebut bebas linear, maka vektor-vektor tersebut merupakan basis. Jika tidak, maka proses diteruskan dengan cara yang sama yang pada akhirnya akan diperoleh suatu basis yang memuat $\{v_1, v_2, \ldots, v_m\}$. ■

Teorema 3.1.5

Andaikan $\{v_1, v_2, \ldots, v_m\}$ dan $\{w_1, w_2, \ldots, w_n\}$ merupakan basis dari ruang vektor V, maka m=n

Bukti

Andaikan m > n. Perhatikan himpunan $\{v_m, w_1, w_2, \ldots, w_n\}$,

yang tak bebas linear karena v_m dapat dinyatakan sebagai kombinasi linear dari vektor-vektor $w_1, w_2, \ldots, w_n$. Jadi ada w_i yang dapat dinyatakan sebagai kombinasi linear dari vektor-vektor lainnya. Dengan mengeluarkan w_i, maka diperoleh $\{v_m, w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_n\}$ yang merentang V.

Selanjutnya perhatikan bahwa v_{m-1} juga dapat dinyatakan sebagai kombinasi linear dari $\{v_m, w_1, \ldots, w_{i-1}, w_{i+1}, w_{i+1}, \ldots, w_n\}$. Jadi himpunan $\{v_{m-1}, v_m, w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_n\}$ merupakan himpunan yang tak bebas linear. Bila proses diteruskan, maka akan diperoleh himpunan $\{v_i, v_{i+1}, v_{i+2}, \ldots, v_m\}$ untuk suatu i yang tak bebas linear. Sehingga timbul kontradiksi bahwa $\{v_1, v_2, \ldots v_m\}$ merupakan basis dari V. Jadi $m \leq n$.

Dengan cara yang sama, tetapi diberlakukan terhadap basis yang lain, maka akan diperoleh $n \leq m$. Jadi $m=n$. ■

Definisi 3.1.6

Jika ruang vektor V mempunyai basis yang terdiri dari n vektor, maka kita katakan V mempunyai *dimensi n*.

Teorema 3.1.6

Andaikan V merupakan ruang vektor atas lapangan F yang berdimensi n, maka n+1 vektor-vektornya adalah tak bebas linear.

Bukti

Andaikan n+1 vektor-vektor adalah bebas linear, maka menurut teorema 3.1.4, maka n+1 vektor-vektor tersebut merupakan basis dari ruang vektor V. Sehingga timbul kontradiksi bahwa dimensi dari V adalah n. Jadi n+1 vektor-vektor tersebut tak bebas linear. ■

Teorema 3.1.7

Andaikan V adalah ruang vektor atas lapangan F dengan dimensi n>0, maka setiap n vektor yang bebas linear merentang V.

Bukti

Andaikan himpunan vektor-vektor bebas linear $\{v_1, v_2, \ldots, v_n\}$. Ambil elemen sebarang v dalam V. Menurut teorema 3.1.3 , $\{v_1, v_2, \ldots, v_n, v\}$ tak bebas linear. Jadi ada skalar α_i yang tidak semuanya nol sedemikian sehingga $\alpha_1 v_1 + \alpha_2 v_2 + \ldots + \alpha_n v_n + \alpha_{n+1} v_{n+1} = 0$. Karena α_{n+1} tidak nol,

maka $v = \left(\frac{-\alpha_1}{\alpha_{n+1}}\right) v_1 + \left(\frac{-\alpha_2}{\alpha_{n+1}}\right) v_2 + \ldots + \left(\frac{-\alpha_n}{\alpha_{n+1}}\right) v_n$.

Jadi $\{v_1, v_2, \ldots, v_n\}$ merentang V. ■

2. Lapangan Perluasan

Definisi 3.2.1

Lapangan E disebut *lapangan perluasan* dari lapangan F jika lapangan E memuat F sebagai lapangan bagiannya.

Definisi 3.2.2

Andaikan E adalah lapangan perluasan dari lapangan F, dan $\alpha \in E$. Andaikan $f(x) = a_o + a_1 x + \ldots + a_n x^n \in F[x]$. Jika $f(\alpha) = 0$, maka α dinamakan *elemen nul* dari $f(x)$.

Teorema 3.2.1

Jika F adalah suatu lapangan dan $p(x) \in F[x]$ adalah polinomial tak teredusir atas F, maka $F[x]/\langle p(x)\rangle$ adalah lapangan perluasan dari lapangan F dan $p(x)$ mempunyai suatu elemen nul dalam $F[x]/\langle p(x)\rangle$.

Bukti

Menurut teorema 2.4.19, maka $F[x]/\langle p(x)\rangle$ adalah lapangan. Dan menurut teorema 2.4.20, $F[x]/\langle p(x)\rangle$ memuat lapangan bagian yang isomorfik dengan lapangan F. Jadi $F[x]/\langle p(x)\rangle$ merupakan lapangan perluasan dari lapangan F. Andaikan $p(x) = a_o + a_1 x + a_2 x^2 + \ldots + a_n x^n$. Maka

$$p(\langle p(x)\rangle + x) = a_o + a_1(\langle p(x)\rangle + x) + a_2(\langle p(x)\rangle + x)^2 + \ldots + a_n(\langle p(x)\rangle + x)^n$$

$$= a_o + a_1(\langle p(x)\rangle + x) + a_2(\langle p(x)\rangle + x^2) + \ldots + a_n(\langle p(x)\rangle + x^n)$$

Menurut teorema 2.4.20 F isomorfis dengan $\{\langle p(x)\rangle + a \mid a \in F\}$, dengan isomorfisma dari $\theta(a) = \langle p(x)\rangle + a$, sehingga setiap $a \in F$ dapat diganti dengan $\langle p(x)\rangle + a$. Maka diperoleh

$$p(\langle p(x)\rangle + x) = (\langle p(x)\rangle + a_o) + (\langle p(x)\rangle + a_1)(\langle p(x)\rangle + x) + (\langle p(x)\rangle + a_2)(\langle p(x)\rangle + x^2) + \ldots + (\langle p(x)\rangle + a_n)(\langle p(x)\rangle + x^n)$$

$$p(\langle p(x)\rangle + x) = (\langle p(x)\rangle + a_0) + (\langle p(x)\rangle + a_1 x) + (\langle p(x)\rangle + a_2 x^2) + \ldots + (\langle p(x)\rangle + a_n x^n)$$

$$= \langle p(x)\rangle + (a_0 + a_1 x + \ldots + a_n x^n)$$

$$= \langle p(x)\rangle + p(x)$$

$$= \langle p(x)\rangle$$

Karena $\langle p(x)\rangle$ adalah elemen identitas dalam $F[x]/\langle p(x)\rangle$, maka terbukti bahwa $\langle p(x)\rangle + x$ merupakan elemen nul dari $p(x)$ dalam $F[x]/\langle p(x)\rangle$. ■

Berikut ini, akan dibahas teorema tentang homomorfisma yang penting dari F[x] ke lapangan perluasan E dari lapangan F yang akan disebut homomorfisma evaluasi.

Teorema 3.2.2

Andaikan E adalah lapangan perluasan dari suatu lapangan F. Andaikan α adalah sebarang elemen dari E. Didefinisikan suatu pemetaan $\theta_\alpha : F[x] \longrightarrow E$ dengan aturan $\theta_\alpha(a_0 + a_1 x + \ldots + a_n x^n) = a_0 + a_1\alpha + \ldots + a_n\alpha^n$. Maka θ_α adalah homomorfisma dari F[x] ke E. Selanjutnya $\theta_\alpha(x) = \alpha$, dan θ_α memetakan F ke F secara isomorfik sebagai pemetaan identitas, yaitu $\theta_\alpha(a) = a$ untuk $a \in F$. Homomorfisma θ_α disebut *evaluasi* pada α.

Bukti

Ambil sebarang $g(x), f(x) \in F[x]$, di mana $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ dan $g(x) = b_0 + b_1 x + \ldots + b_n x^n$ sedemikian sehingga $f(x) = g(x)$, maka $a_0 = b_0, a_1 = b_1, \ldots, a_n = b_n$ sehingga

$$a_o+a_1\alpha+\ldots+a_n\alpha^n = b_o+b_1\alpha+\ldots+b_n\alpha^n$$

$$\theta_\alpha(f(x) = \theta_\alpha(g(x))$$

Jadi θ_α well-defined.

Selanjutnya bila $f(x) = a_o+a_1x+\ldots+a_nx^n$ dan $g(x) = b_o+b_1x+\ldots+b_mx^m$ di mana $m > n$, maka

$$\begin{aligned}\theta_\alpha(f(x) + g(x)) &= \theta_\alpha((a_o+b_o)+(a_1+b_1)x+\ldots+(a_n+b_n)x^n + b_{n+1}x^{n+1} + \ldots + b_mx^m)) \\ &= (a_o+b_o)+(a_1+b_1)\alpha+\ldots+(a_n+b_n)\alpha^n + b_{n+1}\alpha^{n+1} + \ldots + b_m\alpha^m \\ &= (a_o+a_1\alpha+\ldots+a_n\alpha^n) + (b_o+b_1\alpha+\ldots+ b_n\alpha^n+\ldots+b_m\alpha^m) \\ &= \theta_\alpha(f(x)) + \theta_\alpha(g(x))\end{aligned}$$

Untuk $m = n$, $m < n$ dibuktikan dengan cara yang sama.

Selanjutnya $\theta_\alpha(f(x).g(x)) = \theta_\alpha(a_ob_o+(a_ob_1+a_1b_o)x+\ldots+ a_nb_mx^{n+m})$

$$\begin{aligned}&= a_ob_o+(a_ob_1+a_1b_o)\alpha+\ldots+a_nb_m\alpha^{n+m} \\ &= (a_o+a_1\alpha+\ldots+a_n\alpha^n)(b_o+b_1\alpha+\ldots+b_m\alpha^m) \\ &= \theta_\alpha(f(x))\theta_\alpha(g(x))\end{aligned}$$

Untuk setiap polinomial konstan $a \in F[x]$ diperoleh $\theta_\alpha(a) = a$. Jadi θ_α memetakan F ke F secara isomorfik sebagai pemetaan identitas. Dari definisi θ_α diperoleh $\theta_\alpha(x) = \theta_\alpha(ex) = e.\alpha = \alpha$. ■

Definisi 3.2.3

Suatu elemen α di dalam lapangan perluasan E dari lapangan F dikatakan *bersifat aljabar atas lapangan F*

jika $f(\alpha) = 0$, untuk suatu polinomial bukan nol $f(x) \in F[x]$. Jika α tidak bersifat aljabar atas F, maka α disebut *transendental atas F* .

Teorema 3.2.3

Andaikan E lapangan perluasan dari lapangan F dan $\alpha \in E$ di mana α bersifat aljabar atas F. Maka ada polinomial tak teredusir $p(x) \in F[x]$ sedemikian sehingga $p(\alpha) = 0$. Polinomial tak teredusir ini tertentu secara tunggal tanpa memperhatikan faktor konstan dalam F dan merupakan polinomial berderajat terendah di antara polinomial-polinomial f(x) dalam F[x] sedemikian sehingga $f(\alpha) = 0$ dan $d(f(x)) \geq 1$. Jika $f(\alpha) = 0$ untuk $f(x) \in F[x]$ dengan $f(x) \neq 0$, maka p(x) membagi f(x).

Bukti

Andaikan θ_α adalah homomorfisma evaluasi dari F[x] ke E. Menurut teorema 2.4.1 Kernel dari θ_α merupakan ideal dan dengan teorema 2.4.18 ideal itu merupakan ideal utama, yaitu ada suatu polinomial $p(x) \in F[x]$, sedemikian sehingga $\text{Ker}.\theta_\alpha = \langle p(x) \rangle$. Jadi $\langle p(x) \rangle$ terdiri dari elemen -elemen dari F[x] yang mempunyai α sebagai elemen nulnya. Sehingga jika $f(\alpha)=0$ untuk $f(x) \neq 0$, maka $f(x) \in \langle p(x) \rangle$. Jadi p(x) membagi f(x).

Jelaslah bahwa p(x) adalah polinomial berderajat terendah di antara polinomial-polinomial f(x) sehingga $f(\alpha) = 0$, dan $d(f(x)) \geq 1$. Polinomial lain yang berde-

rajat sama dengan p(x) haruslah berbentuk (a)p(x) untuk suatu a∈F. Selanjutnya andaikan p(x) teredusir yaitu p(x)=r(x)s(x) dengan d(r(x)) < d(p(x)) dan d(s(x)) < d(p(x)). Karena p(α)=0, maka r(α)s(α)=0. Karena E lapangan, maka r(α)=0 atau s(α) = 0. Sehingga timbul kontradiksi, karena p(x) adalah polinomial berderajat terendah diantara polinomial-polinomial f(x) sedemikian sehingga f(α) = 0. Jadi p(x) tak teredusir. ■

Kita dapat mengandaikan bahwa polinomial p(x) dalam teorema 3.2.3 di atas mempunyai koefisien utama sama dengan e (kalau perlu dengan mengalikan dengan elemen dari F yang sesuai). Polinomial semacam itu dinamakan *polinomial monik*.

Definisi 3.2.4

Andaikan E adalah lapangan perluasan dari lapangan F dan α ∈ E yang bersifat aljabar atas F. Polinomial monik p(x) dalam teorema 3.2.3 dinamakan *polinomial tak teredusir untuk α atas F*, dan akan dinotasikan dengan irr(α,F). Derajat dari irr(α,F) disebut *derajat dari α atas F*, yang akan dinotasikan dengan d(α,F).

Teorema 3.2.4

Andaikan E merupakan lapangan perluasan dari lapangan F dan α ∈ E bersifat aljabar atas F. Misalkan θ_α ada-

lah homomorfisma evaluasi dari F[x] ke E. Jika irr(α,F)= p(x), maka F[x]/<p(x)> $\approx \theta_\alpha$(F[x]). Selanjutnya θ_α(F[x]) merupakan lapangan bagian yang terkecil dari E yang memuat F dan α (yang dinyatakan dengan F(α)).

Bukti

Menurut bukti teorema 3.2.3 Ker.θ_α = <p(x)>. Karena θ_α merupakan homomorfisma dengan domain F[x] dan range θ_α(F[x]), maka menurut teorema fundamental homomorfisma ring diperoleh F[x]/<p(x)> $\approx \theta_\alpha$ (F[x]). Dari teorema 3.2.2 kita tahu bahwa θ_α (F[x]) memuat F dan α. Andaikan N sebarang lapangan bagian dari E yang memuat F dan α. Untuk setiap b $\in \theta_\alpha$(F[x]), maka terdapat $a_o+a_1x+\ldots+a_nx^n \in$ F[x] sedemikian sehingga b = $\theta_\alpha(a_o+a_1x+\ldots+a_nx^n) = a_o+a_1\alpha+\ldots+a_n\alpha^n$. Karena $a_o, a_1, \ldots, a_n$, $\alpha \in$ N, maka b $\in$ N. Sehingga θ_α(F[x]) $\subseteq$ N. Jadi θ_α(F[x]) merupakan lapangan bagian terkecil yang memuat F dan α. ■

Definisi 3.2.5

Jika E adalah lapangan perluasan dari lapangan F dan E= F(a) untuk suatu a $\in$ E, maka E dinamakan *perluasan sederhana dari F.*

Teorema 3.2.5

Andaikan E adalah perluasan sederhana F(α) dari lapangan F dan α bersifat aljabar atas F. Andaikan

derajat dari irr(α,F) adalah $n \geq 1$. Maka setiap elemen $\beta \in E = F(\alpha)$ dapat dinyatakan secara tunggal dalam bentuk $\beta = b_o + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$ dengan b_i dalam F.

Bukti

Andaikan θ_α homomorfisma evaluasi dari F[x] ke E. Maka setiap elemen dari $F(\alpha) = \theta_\alpha(F[x])$ pasti berbentuk $\theta_\alpha(f(x)) = f(\alpha)$ untuk suatu $f(x) \in F[x]$.

Andaikan irr(α,F) = $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_o$ di mana $p(\alpha) = 0$, yaitu $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_o = 0$, sehingga $\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_o$. Persamaan tersebut dapat digunakan untuk menyatakan setiap monomial α^m untuk $m \geq n$ ke dalam pangkat dari α yang lebih rendah daripada n. Sebagai contoh $\alpha^{n+1} = \alpha\alpha^n = -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - \ldots - a_o\alpha = a_{n-1}(-a_{n-1}\alpha^{n-1} - \ldots - a_o) - a_{n-2}\alpha^{n-1} - \ldots - a_o\alpha$.

Jika $\beta \in F(\alpha)$, maka β berbentuk $\theta_\alpha(f(x)) = f(\alpha)$ untuk suatu $f(x) \in F[x]$, yaitu $\beta = c_o + c_1\alpha + \ldots + c_k\alpha^k$ dengan $c_i \in F$. Karena setiap α^m, $m \geq n$, dapat dinyatakan dalam pangkat-pangkat yang lebih rendah daripada n, maka β dapat dinyatakan dalam bentuk $\beta = b_o + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$, dengan $b_i \in F$. Andaikan $\beta = b_o + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} \in F(\alpha)$ dapat ditulis dengan cara lain misalnya $b'_o + b'_1\alpha + \ldots + b'_{n-1}\alpha^{n-1}$, $b'_i \in F$. Maka $b_o + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} = b'_o + b'_1\alpha + \ldots + b'_{n-1}\alpha^{n-1}$. Sehingga $(b_o - b'_o) + (b_1 - b'_1)x + \ldots + (b_{n-1} - b'_{n-1})x^{n-1} = g(x)$ dalam F[x] dan $g(\alpha) = 0$, $d(g(x)) <$ d(irr(α,F)). Karena irr(α,F) adalah polinomial bukan nol dengan derajat terendah di antara polinomial

polinomial f(x) dalam F[x] dengan $f(\alpha) = 0$ maka haruslah $g(x) = 0$. Jadi $b_i - b_i' = 0$ yaitu $b_i = b_i'$, untuk setiap $i = 0,1,2,\ldots n-1$. ■

Contoh 3.2.1

Polinomial $p(x) = x^2+x+1$ adalah polinomial tak teredusir atas $\mathbb{Z}_2$. Dengan teorema 3.2.1, maka ada lapangan perluasan E dari $\mathbb{Z}_2$ yang memuat suatu elemen nul α dari x^2+x+1. Sehingga dengan teorema 3.2.5 di atas, elemen-elemen dari $\mathbb{Z}_2(\alpha)$ adalah $0+0\alpha$, $1+0\alpha$, $0+1\alpha$ dan $1+1\alpha$, yaitu $0, 1, \alpha$ dan $1+\alpha$.

Teorema 3.2.6

Jika E adalah suatu lapangan perluasan dari lapangan F, maka E adalah suatu ruang vektor atas F.

Bukti

1. Karena E adalah lapangan, maka E merupakan grup abel terhadap operasi jumlahan .
2. Karena F lapangan bagian dari lapangan E, maka
   i). Jika $\alpha \in F$ dan $x,y \in E$, maka $\alpha(x+y) = \alpha x + \alpha y$
   ii). Jika $\alpha, \beta \in F$ dan $x \in E$, maka $(\alpha+\beta)x = \alpha x + \beta x$
   iii). Jika $\alpha, \beta \in F$ dan $x \in E$, maka $(\alpha\beta)x = \alpha(\beta x)$
   iv). $e\,x = x$, untuk semua $x \in E$ (di mana e adalah elemen satuan dalam F)

Jadi E adalah suatu ruang vektor atas F. ■

Teorema 3.2.7

Misalkan E adalah lapangan perluasan dari lapangan F dan misalkan $\alpha \in E$ bersifat aljabar atas F. Jika $d(\alpha,F) = n$, maka $F(\alpha)$ adalah ruang vektor berdimensi n atas F dengan $\{e,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$ sebagai basis. Selanjutnya setiap elemen β dari $F(\alpha)$ bersifat aljabar atas F dan $d(\beta,F) \leq d(\alpha,F)$.

Bukti

E adalah lapangan perluasan dari lapangan F dan $\alpha \in E$ bersifat aljabar atas F. Karena $F(\alpha)$ merupakan lapangan perluasan dari F, maka dengan teorema 3.2.6, $F(\alpha)$ merupakan ruang vektor atas F dan menurut teorema 3.2.5, setiap elemen dari $F(\alpha)$ dapat dinyatakan dengan tunggal dalam bentuk $b_o+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1}$ di mana $b_i \in F$ dan $n=d(\alpha,F)$. Jadi setiap elemen dari $F(\alpha)$ dapat dinyatakan sebagai kombinasi linear dari $\{e,\alpha,\ldots,\alpha^{n-1}\}$. Himpunan vektor-vektor $\{e,\alpha,\ldots,\alpha^{n-1}\}$ adalah bebas linear sebab $b_o+b_1\alpha+\ldots+b_{n-1}\alpha^{n-1} = 0$ hanya bila $b_o=b_1=\ldots=b_{n-1}=0$. Jadi himpunan vektor-vektor $\{e,\alpha,\ldots,\alpha^{n-1}\}$ merupakan basis dari $F(\alpha)$, yang berarti dimensi $F(\alpha)$ sama dengan n. Selanjutnya, misalkan $\beta \in F(\alpha)$ di mana α bersifat aljabar atas F dengan $d(\alpha,F) = n$. Perhatikan himpunan $\{e,\beta,\ldots\beta^n\}$. Kalau semua elemen dalam himpunan tersebut berlainan, maka menurut teorema 3.1.6 himpunan dengan n+1 elemen tersebut tak bebas linear sebab $F(\alpha)$ merupakan ruang vektor yang berdimensi n. Kalau ada

elemen yang sama dalam himpunan tersebut, misalnya $\beta^i=\beta^j$, maka $\beta^i-\beta^j=0$. Jadi bagaimanapun pasti ada $b_i \in F$ $(i=0,1,2,\ldots,n)$ yang tidak semuanya nol, sedemikian sehingga $b_o+b_1\beta+\ldots+b_n\beta^n = 0$. Maka $f(x) = b_nx^n+\ldots+b_1x+b_o$ adalah polinomial tak nol dalam F[x] sedemikian sehingga $f(\beta) = 0$. Jadi β bersifat aljabar atas F dan $d(\beta,F) \leq n$. ■

Definisi 3.2.6

Suatu lapangan perluasan E dari lapangan F disebut *perluasan aljabar dari F* jika setiap elemen dalam E bersifat aljabar atas F.

Definisi 3.2.7

Lapangan perluasan E dari lapangan F disebut *perluasan berhingga dari F* bila dimensi dari E sebagai ruang vektor atas F adalah berhingga.

Dimensi E sebagai suatu ruang vektor atas F akan ditulis dengan lambang [E:F] .

[E:F] = 1 bila dan hanya bila E=F.

Sebab:

Bila [E:F] = 1, maka menurut teorema 3.1.7 himpunan bebas linear {e} merupakan basis. Jadi setiap elemen dari E dapat dinyatakan sebagai ae untuk suatu $a \in F$.

Karena ae = a dalam F, maka $E \subseteq F$. Jadi E=F.

Selanjutnya andaikan E=F. Maka [E:F]=[F:F]. Setiap elemen a∈F dapat dinyatakan sebagai ae dengan e elemen satuan dalam F. Karena himpunan {e} bebas linear dan merentang F, maka {e} merupakan basis untuk ruang vektor F atas F, yaitu [F:F] = 1. Jadi [E:F] = 1 ■

Teorema 3.2.8

Suatu lapangan perluasan berhingga E dari lapangan F merupakan perluasan aljabar dari F.

Bukti

Andaikan [E:F] = n, dan $\alpha \in E$, maka $e,\alpha,\alpha^2,\ldots,\alpha^n$ adalah (n+1) elemen yang tidak bebas linear dalam E. Jadi ada $a_i \in F$ yang tidak semuanya nol sedemikian sehingga $a_n\alpha^n+a_{n-1}\alpha^{n-1}+\ldots+a_1\alpha+a_o=0$. Jadi ada polinomial bukan nol $f(x) = a_nx^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_o$ dalam F[x] dengan $f(\alpha)=0$. Jadi α bersifat aljabar atas F. ■

Teorema 3.2.9

Bila L suatu lapangan perluasan berhingga dari lapangan K, dan K lapangan perluasan berhingga dari lapangan F, maka L adalah lapangan perluasan berhingga dari lapangan F, dan [L:F] = [L:K][K:F].

Bukti

Andaikan [L:K]=m dan $\{u_1,u_2,\ldots,u_m\}$ adalah basis untuk L atas K. Andaikan [K:F]=n dan $\{v_1,v_2,\ldots,v_n\}$ adalah basis untuk K atas F. Akan ditunjukkan bahwa $B=\{v_ju_i|$

$i=1,2,\ldots,m$, $j=1,2,\ldots,n\}$ adalah basis untuk L atas F. Jika $x\in L$, maka $x=\sum_{i=1}^{m}\lambda_i u_i$ dengan $\lambda_i\in K$. Karena $\{v_1,v_2,\ldots,v_n\}$ merupakan basis untuk K atas F, maka tiap elemen λ_i dapat ditulis sebagai $\lambda_i=\sum_{j=1}^{n}\mu_{ij}v_j$ dengan $\mu_{ij}\in$ F. Jadi $x=\sum_{i=1}^{m}\sum_{j=1}^{n}\mu_{ij}v_j u_i$. Terbukti B merentang L atas F.

Andaikan $\sum_{i=1}^{m}\sum_{j=1}^{n}\mu_{ij}v_j u_i=0$ dengan $\mu_{ij}\in$ F. Maka $\sum_{i=1}^{m}\left(\sum_{j=1}^{n}\mu_{ij}v_j\right)u_i=0$. Karena $u_1,u_2,\ldots,u_m$ adalah bebas linear atas K, maka untuk setiap $i=1,2,\ldots,m$, $\sum_{=1}^{n}\mu_{ij}v_j=$ 0. Selanjutnya $v_1,v_2,\ldots,v_n$ adalah bebas linear atas F, sehingga untuk setiap i dan j , $\mu_{ij}=0$. Jadi B adalah bebas linear, sehingga B adalah basis untuk L atas F, dan $[L:F]=mn=[L:K][K:F]$. ■

Akibat 1

Jika F_i adalah lapangan untuk $i=1,2,\ldots,r$ dan F_{i+1} adalah lapangan perluasan berhingga dari F_i, maka F_r adalah lapangan perluasan berhingga dari F_1, dan

$[F_r:F_1]=[F_r:F_{r-1}][F_{r-1}:F_{r-2}]\ldots[F_2:F_1]$.

Bukti

Akan dibuktikan dengan induksi matematik.

1. Untuk r=3, menurut teorema 3.2.9, diperoleh F_3 adalah lapangan perluasan berhingga dari F_1,

dan $[F_3:F_1]=[F_3:F_2][F_2:F_1]$.

2. Andaikan teorema benar untuk r=n-1, yaitu F_{n-1} adalah lapangan perluasan berhingga dari F_1 dan $[F_{n-1}:F_1]=[F_{n-1}:F_{n-2}][F_{n-2}:F_{n-3}]\ldots[F_2:F_1]$.

   Akan dibuktikan teorema benar untuk r=n.

   Karena F_n adalah lapangan perluasan berhingga dari F_{n-1}, dan F_{n-1} adalah lapangan perluasan berhingga dari F_1, maka F_n adalah lapangan perluasan berhingga dari F_1, dan $[F_n:F_1] = [F_n:F_{n-1}][F_{n-1}:F_1]= [F_n:F_{n-1}][F_{n-1}:F_{n-2}][F_{n-2}:F_{n-3}]\ldots[[F_2:F_1]$.

   Jadi teorema benar untuk r=n. ■

Akibat 2

Jika E adalah lapangan perluasan dari F, $\alpha\in E$ bersifat aljabar atas F dan $\beta\in F(\alpha)$, maka $d(\beta,F)$ membagi $d(\alpha,F)$.

Bukti

Menurut teorema 3.2.7, $d(\alpha,F) = [F(\alpha):F]$ dan $d(\beta,F) = [F(\beta):F]$. Karena $F(\beta)$ merupakan lapangan perluasan berhingga dari lapangan F dan $F(\alpha)$ merupakan lapangan perluasan berhingga dari lapangan $F(\beta)$, maka menurut teorema 3.2.9, $[F(\alpha):F]=[F(\alpha):F(\beta)][F(\beta):F]$. Jadi $[F(\beta):F]$ membagi $[F(\alpha):F]$, yaitu $d(\beta,F)$ membagi $d(\alpha,F)$.■

Definisi 3.2.8

Andaikan E adalah lapangan perluasan dari lapangan F dan $\alpha_1,\alpha_2,\ldots,\alpha_n \in E$. Maka lapangan bagian terkecil da-

ri E yang memuat F dan $\alpha_1,\alpha_2,\ldots,\alpha_n$ akan disajikan dengan lambang $F(\alpha_1,\alpha_2,\ldots,\alpha_n)$.

Teorema 3.2.10

Misalkan E adalah perluasan aljabar dari lapangan F. Maka terdapat elemen-elemen $\alpha_1,\alpha_2,\ldots,\alpha_n$ dalam E sedemikian sehingga $E = F(\alpha_1,\alpha_2,\ldots,\alpha_n)$ bila dan hanya bila E merupakan ruang vektor berdimensi berhingga atas F, yaitu bila dan hanya bila E merupakan perluasan berhingga dari F.

Bukti

1. $\Rightarrow$

   Andaikan $E=F(\alpha_1,\alpha_2,\ldots,\alpha_n)$. Karena E merupakan perluasan aljabar dari F, maka tiap α_i bersifat aljabar atas F, sehingga setiap α_i bersifat aljabar atas setiap lapangan perluasan dari F dalam E. Jadi $F(\alpha_1)$ merupakan perluasan aljabar atas F, dan secara umum $F(\alpha_1,\alpha_2,\ldots,\alpha_j)$ merupakan perluasan aljabar atas $F(\alpha_1,\alpha_2,\ldots,\alpha_{j-1})$ untuk $j = 2,3,\ldots,n$. Menurut akibat 1 dari teorema 3.2.9 yang diberlakukan untuk perluasan-perluasan berhingga $F, F(\alpha_1), F(\alpha_1,\alpha_2),\ldots, F(\alpha_1,\alpha_2,\ldots,\alpha_n)= E$, maka E adalah perluasan berhingga dari F.

2. $\Leftarrow$

   Andaikan E adalah lapangan perluasan berhingga dari

lapangan F. Jika [E:F]=1, maka E = F dan bukti selesai.

Jika $E \neq F$, misalkan $\alpha_1 \in E$ tetapi $\alpha_1 \notin F$. Maka $[F(\alpha_1):F] > 1$. Jika $F(\alpha_1)=E$, maka bukti selesai.

Jika tidak demikian, misalkan $\alpha_2 \in E$ dengan $\alpha_2 \notin F(\alpha_1)$.

Bila proses ini diteruskan, karena [E:F] berhingga, maka menurut teorema 3.2.9, kita akan memperoleh α_n sedemikian sehingga $F(\alpha_1,\alpha_2,\ldots,\alpha_n) = E$. ■

Teorema 3.2.11

Misalkan E adalah lapangan perluasan dari F. Maka $\overline{F}_E$ = { $\alpha \in E$| α bersifat aljabar atas F } adalah lapangan bagian dari E, dan disebut *tutupan aljabar dari F dalam E.*

Bukti

Misalkan $\alpha, \beta \in \overline{F}_E$. Maka menurut teorema 3.2.10, $F(\alpha,\beta)$ merupakan perluasan berhingga dari F. Dan menurut teorema 3.2.8 , maka setiap elemen dari $F(\alpha,\beta)$ bersifat aljabar atas F, yaitu $F(\alpha,\beta) \subseteq \overline{F}_E$. Jadi $\overline{F}_E$ memuat $\alpha+\beta$, $\alpha\beta$, $\alpha-\beta$, dan juga $\alpha\beta^{-1}$ untuk $\beta \neq 0$. Maka $\overline{F}_E$ merupakan lapangan bagian dari E. ■

Definisi 3.2.9

Suatu lapangan F disebut *tertutup secara aljabar*, jika setiap polinomial yang bukan polinomial konstan dalam

F[x] mempunyai akar dalam F.

Teorema 3.2.12

Lapangan F tertutup secara aljabar bila dan hanya bila setiap polinomial yang bukan polinomial konstan dalam F[x] dapat difaktorkan menjadi faktor-faktor linear dalam F[x].

Bukti

1. ⇒

Andaikan F tertutup secara aljabar, maka menurut definisi 3.2.9 polinomial f(x) yang bukan konstan dalam F[x], mempunyai akar a∈F. Menurut teorema 2.4.14, x-a adalah faktor dari f(x), sehingga f(x) =(x-a)g(x) untuk suatu g(x) ∈ F[x]. Jika g(x) adalah polinomial yang bukan konstan, maka g(x) mempunyai akar b∈F, dan f(x) = (x-a)(x-b)h(x) untuk suatu h(x) ∈ F[x]. Bila proses diteruskan, maka akhirnya akan didapat faktorisasi f(x) dalam faktor-faktor linear dalam F[x].

2. ⇐

Andaikan bahwa setiap polinomial yang bukan konstan dalam F[x] dapat difaktorkan dalam faktor-faktor linear. Jika ax-b adalah suatu faktor linear dari f(x), maka $ba^{-1} \in F$ adalah akar dari f(x). Jadi F tertutup secara aljabar. ■

Akibat 1

Lapangan tertutup secara aljabar F tidak mempunyai perluasan aljabar sejati, yaitu tidak ada perluasan aljabar E dari F dengan $F \subset E$ dan $F \neq E$.

Bukti

Andaikan E adalah suatu perluasan aljabar dari F. Karena F tertutup secara aljabar, maka menurut teorema 3.2.12, jika $\alpha \in E$ akan diperoleh $irr(\alpha, F) = x-\alpha$.

Sehingga $\alpha \in F$. Jadi F=E. ■

BAB IV
LAPANGAN BERHINGGA

Bab ini membahas struktur lapangan berhingga. Kita akan menunjukkan bahwa untuk setiap bilangan prima p dan bilangan bulat positif n, ada lapangan berhingga dengan p^n elemen, yang akan disebut *lapangan Galois dengan ordo* p^n dan dilambangkan dengan $GF(p^n)$.

Teorema 4.1

Andaikan E adalah lapangan perluasan berhingga dari lapangan F, dan [E:F] = n. Jika F mempunyai q elemen, maka E mempunyai q^n elemen.

Bukti

Andaikan $\{\alpha_1,\alpha_2,\ldots,\alpha_n\}$ adalah basis untuk E sebagai ruang vektor atas F. Maka tiap $\beta\in E$ dapat dinyatakan secara tunggal sebagai $\beta = b_1\alpha_1+b_2\alpha_2+\ldots+b_n\alpha_n$ dengan $b_i\in F$. Karena tiap b_i adalah salah satu dari q elemen dalam F, maka jumlah total kombinasi linear dari α_i, yaitu jumlah elemen dari E, adalah q^n elemen. ■

Akibat

Jika E adalah lapangan berhingga dengan karakteristik p, maka E memuat tepat p^n elemen untuk suatu bilangan bulat positif n.

Bukti

Karena karakteristik dari E adalah p, maka E memuat lapangan bagian yang isomorfis dengan $\mathbb{Z}_p$. Andaikan $[E:\mathbb{Z}_p] = n$. Maka menurut teorema 4.1, E memuat p^n elemen. ■

Teorema 4.2

Jika E adalah lapangan berhingga E dengan p^n elemen, yang termuat dalam tutupan aljabar $\bar{\mathbb{Z}}_p$ dari $\mathbb{Z}_p$, maka elemen-elemen dari E adalah tepat sama dengan elemen-elemen nul dalam $\bar{\mathbb{Z}}_p$ dari polinomial $x^{p^n}-x \in \mathbb{Z}_p[x]$.

Bukti

Himpunan E^* yang terdiri dari elemen -elemen yang tidak sama dengan nol dari E membentuk grup terhadap operasi perkalian dengan ordo p^n-1. Ordo dari sebarang elemen $\alpha \in E^*$ membagi habis ordo dari grup E^*. Jadi untuk $\alpha \in E^*$, $\alpha^{p^n-1} = e$, yaitu $\alpha^{p^n} = \alpha$. Jadi setiap elemen dalam E merupakan elemen nul dari polinomial $x^{p^n}-x$. Karena polinomial $x^{p^n}-x$ mempunyai paling banyak p^n elemen nul, maka terbuktilah bahwa elemen-elemen dari E adalah tepat sama dengan elemen-elemen nul dalam $\bar{\mathbb{Z}}_p$ dari polinomial $x^{p^n}-x$. ■

Definisi 4.1

Suatu elemen α dalam tutupan aljabar $\bar{F}$ dari F disebut elemen nul dari $f(x) \in F[x]$ dengan *multiplisitas v*, jika v adalah bilangan bulat terbesar sedemikian sehingga $(x-\alpha)^v$ merupakan faktor dari f(x) dalam $\bar{F}[x]$.

Lemma 4.a

Jika F adalah lapangan berhingga berkarakteristik p dengan tutupan aljabar $\bar{F}$, maka polinomial $x^{p^n}-x$ mempunyai p^n elemen nul yang berbeda dalam $\bar{F}$.

Bukti

Jelaslah bahwa 0 merupakan elemen nul dari polinomial $x^{p^n}-x$ dengan multiplisitas 1. Andaikan $\alpha \neq 0$ adalah elemen nul dari polinomial $x^{p^n}-x$. Maka α merupakan elemen nul dari $f(x) = x^{p^n-1}-e$. Jadi $x-\alpha$ adalah faktor dari $f(x) \in \bar{F}[x]$, yaitu $f(x) = (x-\alpha)g(x)$, di mana

$g(x) = x^{p^n-2}+\alpha x^{p^n-3}+\alpha^2 x^{p^n-4}+\alpha^3 x^{p^n-5}+\ldots+\alpha^{p^n-3}x+\alpha^{p^n-2}$ yang terdiri dari p^n-1 suku. Masing-masing suku dari $g(\alpha)$ adalah $\alpha^{p^n-2} = \alpha^{p^n-1}\alpha^{-1} = e\alpha^{-1} = \alpha^{-1}$ sehingga $g(\alpha) = (p^n-1)\alpha^{-1} = p^n\alpha^{-1}-\alpha^{-1} = \alpha^{-1}$ sebab karakteristik dari F adalah p. Jadi $g(\alpha) \neq 0$, maka α adalah elemen nul dari f(x) dengan multiplisitas 1. Sehingga polinomial $x^{p^n}-x$ mempunyai p^n elemen nul yang berbeda. ■

Berikut ini akan dibahas lemma yang digunakan dalam pembuktian teorema berikutnya. Dalam pembuktian lemma ini akan digunakan teorema binomial yang tidak dibahas disini.

Lemma 4.b

Jika α, β elemen dalam suatu ring dengan karakteristik p, di mana p adalah suatu bilangan prima, maka $(\alpha+\beta)^{p^n} = \alpha^{p^n} + \beta^{p^n}$ untuk suatu bilangan bulat positif n.

Bukti

Akan dibuktikan dengan induksi matematik.

1. Untuk n=1, dengan teorema binomial diperoleh bahwa

$$(\alpha+\beta)^p = \binom{p}{0}\alpha^p+\binom{p}{1}\alpha^{p-1}\beta+\binom{p}{2}\alpha^{p-2}\beta^2+\ldots+\binom{p}{k}\alpha^{p-k}\beta^k +\ldots+\binom{p}{p}\beta^p$$

$$= \left(\frac{p!}{p!0!}\right)\alpha^p+\left(\frac{p!}{(p-1)!1!}\right)\alpha^{p-1}\beta+\left(\frac{p!}{(p-2)!2!}\right)\alpha^{p-2}\beta^2 +\ldots+\left(\frac{p!}{(p-k)!k!}\right)\alpha^{p-k}\beta^k+\ldots+\left(\frac{p!}{p!0!}\right)\beta^p$$

Karena karakteristik ring tersebut sama dengan p, maka diperoleh $(\alpha+\beta)^p = \alpha^p+\beta^p$. ■

2. Andaikan lemma benar untuk n = m.

Akan dibuktikan lemma benar untuk n = m+1

$$(\alpha+\beta)^{p^{m+1}} = ((\alpha+\beta)^p)^{p^m}$$

$$= (\alpha^p+\beta^p)^{p^m}$$

$$= \alpha^{p^{m+1}}+\beta^{p^{m+1}}$$

■

Teorema 4.3

Untuk setiap bilangan prima p dan bilangan bulat positif n terdapat lapangan berhingga dengan p^n elemen, yang disajikan dengan $GF(p^n)$.

Bukti

Andaikan $\bar{Z}_p$ tutupan aljabar dari lapangan berhingga Z_p, yang berkarakteristik p, dan K himpunan bagian dari $\bar{Z}_p$ yang terdiri dari semua elemen nul dari polinomial $x^{p^n}-x$ dalam $\bar{Z}_p$. Jelas $K\neq\emptyset$ sebab 0 dan e berada dalam K. Ambil sebarang

elemen $\alpha, \beta \in K$, maka $(\alpha \pm \beta)^{p^n} = \alpha^{p^n} \pm \beta^{p^n} = \alpha \pm \beta$ $(\alpha\beta)^{p^n} = \alpha^{p^n} \beta^{p^n} = \alpha\beta$. Jadi K tertutup terhadap jumlahan, pengurangan dan perkalian. Untuk $\alpha \in K$ dan $\alpha \neq 0$, maka $\alpha^{p^n} = \alpha$ sehingga diperoleh $(\alpha^{-1})^{p^n} = \alpha^{-1}$, yang berarti $\alpha^{-1} \in K$. Jadi K merupakan lapangan bagian dari $\bar{Z}_p$ yang memuat Z_p. Menurut lemma 4.a, maka K memuat p^n elemen yang berbeda. ■

BAB V

KESIMPULAN

Berdasarkan uraian bab-bab sebelumnya dapat disimpulkan bahwa :

1. Lapangan E disebut lapangan perluasan dari lapangan F jika lapangan E memuat F sebagai lapangan bagiannya.
2. Suatu polinomial $p(x) \in F[x]$ yang tak teredusir atas lapangan F mempunyai elemen nul dalam suatu lapangan perluasan dari F.
3. Suatu elemen α di dalam lapangan perluasan E dari lapangan F dikatakan bersifat aljabar atas lapangan F jika $f(\alpha) = 0$ untuk suatu polinomial tak nol $f(x) \in F[x]$.
4. Suatu lapangan perluasan E dari lapangan F merupakan suatu ruang vektor atas F.
5. Suatu lapangan perluasan E dari lapangan F disebut perluasan aljabar dari F jika setiap elemen dalam E bersifat aljabar atas F.
6. Suatu lapangan perluasan E dari lapangan F disebut perluasan berhingga dari F bila dimensi dari E sebagai ruang vektor atas F adalah berhingga.
7. Suatu lapangan perluasan berhingga E dari lapangan F merupakan perluasan aljabar dari F.
8. Jika E adalah suatu lapangan perluasan dari lapangan F, maka $\overline{F}_E = \{\alpha \in E \mid \alpha$ bersifat aljabar atas $F\}$ merupakan

lapangan bagian dari E.

9. Untuk setiap bilangan prima p dan bilangan bulat positif n, terdapat lapangan berhingga dengan ordo p^n.

DAFTAR PUSTAKA

1. Chauduri, N.P. 1983. *Abstract ALgebra*. New Dehli : Tata Mc Graw - Hill Publishing Company Limited.
2. Durbin, John R. 1985. *Modern Algebra. An Introduction.* New York : John Wiley and Sons.
3. Fraleigh, John B. 1989. *A First Course in Abstract Algebra*. Reading, Massachusetts : Addison Wesley Publishing Company Inc.
4. Gilbert, William J. 1976. *Modern Algebra with Applications*. New York : John Wiley and Sons.
5. Mc Coy, N.H. 1987. *Introduction to Modern Algebra*. Boston : Allyn and Bacon Inc.
6. Narayan, Shanti and Sat Pal. 1979. *A Text Book of Modern Abstract Algebra*. New Dehli : S. Chand and Company Ltd.