RING POLINOMIAL

SKRIPSI

Diajukan Untuk Memenuhi Salah Satu Syarat
Memperoleh Gelar Sarjana Pendidikan
Program Studi Pendidikan
Matematika

Oleh :

PURWATININGSIH

N I M : 89 414 054
NIRM : 890052010501120034

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

1994

S k r i p s i

RING POLINOMIAL

Oleh

Purwatiningsih

NIM : 89 414 054

NIRM : 890052010501120034

telah disetujui oleh :

Pembimbing I

Dr.Frans Susilo, S.J tanggal 15-10-94

Pembimbing II

Dra. A. Linda Yuliastuti tanggal 15-10-94

S k r i p s i

RING POLINOMIAL

yang dipersiapkan dan disusun oleh

Purwatiningsih

Nim : 89 414 054

Nirm : 890052010501120034

telah dipertahankan di depan Panitia Penguji

pada tanggal 7 Oktober 1994

dan dinyatakan telah memenuhi syarat

Susunan Panitia Penguji

	Nama Lengkap	Tanda tangan
Ketua	Dr. St. Suwarsono	.....
Sekretaris	Dr. Y. Marpaung	.....
Anggota I	Dr. Frans. Susilo, S.J	.....
Anggota II	Dr. Y. Marpaung	.....
Anggota III	Dra. A. Linda Yuliastuti	.....

Yogyakarta, 10 Oktober 1994

Fakulktas Keguruan dan Ilmu Pendidikan

Universitas Sanata Dharma

Dekan FKIP

Priyono Marwan, S.J.

Dr. A. Priyono Marwan, S.J.

Kupersembahkan buat Bapak, Ibu, Adik,

dan Kekasihku tersayang

KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa atas berkat dan karuniaNya kepada penyusun, sehingga skripsi yang berjudul **RING POLINOMIAL** dapat terselesaikan.

Penyusunan skripsi ini dimaksudkan untuk memenuhi salah satu syarat memperoleh gelar sarjana pendidikan Program Studi Pendidikan Matematika di Jurusan Pendidikan Matematika dan Ilmu Pengetahuan Alam, Fakultas Keguruan dan Ilmu Pendidikan, Universitas Sanata Dharma, Yogyakarta.

Pada kesempatan ini, penyusun ingin mengucapkan terima kasih kepada :

- Romo Dr. Frans Susilo, S.J, selaku Pembimbing I yang dengan penuh kesabaran telah mencurahkan perhatiannya dalam membimbing penyusunan skripsi ini.
- Ibu Dra. A. Linda Yuliastuti, selaku pembimbing II yang telah dengan sabar dan teliti dalam membaca dan mengoreksi skripsi ini.
- Bapak Dr. St. Suwarsono, selaku Ketua Jurusan Pendidikan Matematika dan Ilmu Pengetahuan Alam, Universitas Sanata Dharma.
- Bapak Drs. T. Sugiarto, selaku Ketua Program Studi Pendidikan Matematika, Universitas Sanata Dharma.
- Bapak dan Ibu Dosen Universitas Sanata Dharma yang telah memberikan bimbingan selama penulis mengikuti kuliah di Universitas Sanata Dharma Yogyakarta.

- Bapak dan Ibu Karyawan Universitas Sanata Dharma yang memberikan dukungan moril dan pelayanan kepada penyusun.
- Kasihku Y.Hartono yang telah memberikan dorongan moril dan membantu terjemahan kepada penyusun sehingga skripsi ini dapat terselesaikan dengan baik.
- Rekan-rekan Mahasiswa di Universitas Sanata Dharma khususnya di Program Studi Pendidikan Matematika yang telah memberikan dukungan moril kepada penyusun.
- Semua pihak yang telah membantu penyusun dalam penyusunan skripsi ini.

Dalam penyusunan skripsi ini penyusun menyadari bahwa masih banyak terdapat kekurangan baik dari penguasaan materi maupun dari segi metodologi pembahasan, yang masih jauh dari sempurna. Oleh karena itu segala kritik dan saran yang membangun diharapkan demi sempurnanya skripsi ini. Penyusun berharap semoga skripsi ini dapat bermanfaat bagi pembaca.

Yogyakarta, September 1994

Penyusun

DAFTAR ISI

ABSTRAK

RING POLINOMIAL

Ring polinomial adalah ring yang elemen-elemennya adalah polinomial-polinomial dalam x atas suatu ring. Seperti halnya pada bilangan bulat, pada ring polinomial atas suatu field berlaku algoritma pembagian, dan dua polinomial atas suatu field yang tidak keduanya nol mempunyai faktor persekutuan terbesar. Setiap polinomial yang bukan konstanta di dalam ring polinomial atas field F dapat difaktorkan ke dalam perkalian polinomial-polinomial irreducible dengan tunggal tanpa memperhatikan urutan dan faktor-faktor unit dari F.

Ring polinomial atas daerah faktorisasi tunggal merupakan daerah faktorisasi tunggal.

Jika p(x) irreducible atas field F, maka F[x]/(p(x)) merupakan field yang memuat suatu subfield yang isomorfik dengan F.

Suatu polinomial dengan derajat positip atas field F pasti mempunyai akar di dalam suatu perluasan dari F.

BAB I

PENDAHULUAN

Dalam matematika dasar sudah diketahui bahwa persamaan $x^2-2=0$ tidak mempunyai penyelesaian di dalam field bilangan rasional, dan persamaan $x^2+1=0$ tidak mempunyai penyelesaian di dalam field bilangan real. Masalah tersebut dapat diatasi dengan memperluas fieldnya. Salah satu contoh dari perluasan field adalah ring faktor polinomial, yang akan dibahas dalam tulisan ini.

Tulisan ini akan diawali dengan membicarakan ring polinomial, yaitu ring yang elemen-elemennya adalah polinomial-polinomial dalam x atas suatu ring. Bila R adalah suatu ring, maka ring polinomial dalam x atas R, ditulis dengan notasi R[x], memuat semua ekspresi berbentuk $a_o+a_1x+\ldots+a_nx^n+\ldots$, di mana $a_i \in R$ dan $a_i=0$ untuk semua kecuali berhingga banyak i, dan i adalah bilangan bulat non-negatif. Ring R[x] merupakan daerah integral, jika R merupakan daerah integral. Ring ini akan dibahas dalam bab 2. Selain itu dibahas juga algoritma pembagian polinomial dan faktor persekutuan terbesar dari dua polinomial f(x) dan g(x) yang bukan keduanya polinomial nol.

Dalam bab 3 akan dibahas ring polinomial atas daerah faktorisasi tunggal. Dalam bab ini akan dibahas field pembagi dari daerah integral D, polinomial primitif, perkalian polinomial-polinomial primitif, dan content dari polinomial yang bukan konstanta di dalam D[x] (D daerah faktorisasi tunggal). Dalam bab ini akan dibuktikan pula

bahwa D[x] merupakan daerah faktorisasi tunggal, jika D adalah daerah faktorisasi tunggal.

Yang dibahas dalam bab 4 adalah ring faktor polinomial. Dalam bab ini dibuktikan bahwa setiap ideal dari ring polinomial F[x] adalah ideal utama. Selanjutnya ring faktor polinomial F[x]/(p(x)) adalah field bila dan hanya bila p(x) irreducible atas F, dan setiap elemen dari F[x]/(p(x)) dapat dinyatakan dengan tunggal dalam bentuk (p(x)) + (b_o + b_1x + ... + $b_{n-1}x^{n-1}$) dengan $b_o, b_1, \ldots, b_{n-1}$ di dalam F.

Dalam bab 5 akan dibahas perluasan field, yaitu suatu field yang memuat field semula sebagai subfieldnya, dan akan ditunjukkan bahwa suatu ring faktor polinomial dapat merupakan perluasan suatu field. Selain itu akan dibahas homomorfisme evaluasi, polinomial irreducible untuk α atas F, dan perluasan sederhana suatu field. Agar dapat memahami tulisan ini, pembaca diharapkan telah menguasai teori tentang field, grup, ring, dan teori tentang pemetaan.

Karena tulisan ini hanya merupakan hasil studi pustaka, maka dalam tulisan ini tidak ditemukan hal-hal yang baru.

BAB II

RING POLINOMIAL

Pada bagian ini akan dibahas suatu ring khusus yang disebut ring polinomial. Pembahasan ring polinomial ini akan dimulai dengan definisi dan sifat-sifat dasar dari polinomial.

2.1 Polinomial atas Suatu Ring.

Ring adalah himpunan R bersama dengan 2 operasi , misalkan penjumlahan (+) dan perkalian (.), sedemikian hingga aksioma-aksioma berikut dipenuhi :

1. Untuk setiap $a,b \in R$, $a+b \in R$.
2. Untuk setiap $a,b,c \in R$, $(a+b)+c=a+(b+c)$.
3. Ada elemen $0 \in R$ sedemikian hingga untuk setiap $a \in R$ berlaku $0+a=a+0=a$.
4. Untuk setiap $a \in R$, ada elemen $-a \in R$ sedemikian hingga $a+(-a) = -a+a = 0$.
5. Untuk setiap $a,b \in R$, $a+b=b+a$.
6. Untuk setiap $a,b \in R$, $ab \in R$.
7. Untuk setiap $a,b,c \in R$, $(ab)c=a(bc)$.
8. Untuk setiap $a,b,c \in R$,
   $a(b+c) = ab+ac$ dan $(a+b)c = ac+bc$.

Suatu ring R disebut **komutatif** jika $ab=ba$ untuk setiap $a,b \in R$.

Definisi 2.1.1

Misalkan R adalah ring. Suatu polinomial dalam variabel x dengan koefisien-koefisien di dalam R, dilambangkan dengan f(x), adalah suatu jumlahan yang dapat dinyatakan sebagai

$$\sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \ldots + a_n x^n + \ldots,$$

di mana $a_i \in R$ dan $a_i = 0$ untuk semua kecuali berhingga banyak i, dan i adalah bilangan bulat non-negatif. $a_i x^i$ disebut suku dari polinomial f(x). a_i disebut koefisien dari x^i dalam f(x). Nilai terbesar dari i sedemikian hingga $a_i \neq 0$ disebut derajat dari f(x), ditulis dengan d(f(x)).

Himpunan polinomial-polinomial dalam variabel x dengan koefisien-koefisien di dalam ring R dilambangkan dengan R[x], dan sering disebut secara singkat himpunan polinomial-polinomial dalam x atas ring R. Tanda "+" dan $a_i x^i$ pada definisi 2.1.1 adalah lambang yang tidak didefinisikan. Dalam penulisan akan digunakan a_0 untuk $a_0 x^0$, x untuk $1x^1$, x^i untuk $1x^i$ dan suku-suku dengan koefisien nol tidak dituliskan.

Jika $f(x) = a_0 + a_1 x + \ldots + a_n x^n + \ldots$ mempunyai $a_i = 0$ untuk $i > n$, maka ditulis $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. Polinomial f(x) sama dengan nol bila dan hanya bila $a_i = 0$ untuk setiap i.

Untuk membentuk ring dari himpunan polinomial-polinomial R[x], pertama-tama harus didefinisikan operasi penjumlah-

an dan perkalian pada R[x], dan selanjutnya dengan operasi tersebut dibuktikan bahwa R[x] adalah ring.

Definisi 2.1.2

Misalkan $f(x) = \sum_{i=0}^{\infty} a_i x^i$ dan $g(x) = \sum_{i=0}^{\infty} b_i x^i$ adalah polinomial-polinomial dalam x atas ring R. Maka

(1) $f(x) = g(x)$ bila dan hanya bila $a_i = b_i$ untuk setiap i,

(2) $f(x)+g(x) = \sum_{i=0}^{\infty} (a_i+b_i)x^i$,

(3) $f(x)\,g(x) = \sum_{i=0}^{\infty} d_i x^i$ dengan $d_i = \sum_{n=0}^{i} a_n b_{i-n}$.

Teorema 2.1.1

Jika R adalah ring komutatif, maka R[x] adalah ring komutatif terhadap operasi yang didefinisikan pada definisi 2.1.2.

Bukti

Untuk setiap $f(x) = \sum_{i=0}^{\infty} a_i x^i$, $g(x) = \sum_{i=0}^{\infty} b_i x^i$, dan $h(x) = \sum_{i=0}^{\infty} c_i x^i$ di dalam R[x], berlaku :

1. $f(x)+g(x)$ di dalam R[x] karena a_i+b_i di dalam R untuk setiap a_i, b_i di dalam R.

2. $[f(x)+g(x)]+h(x)$
   $= [\sum_{i=0}^{\infty} (a_i+b_i)x^i] + \sum_{i=0}^{\infty} c_i x^i$

$$= \sum_{i=0}^{\infty} ((a_i+b_i)+c_i)\ x^i$$

$$= \sum_{i=0}^{\infty} (a_i+(b_i+c_i))\ x^i$$

$$= \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} (b_i+c_i)\ x^i$$

$$= \sum_{i=0}^{\infty} a_i x^i + [\sum_{i=0}^{\infty} b_i x^i + \sum_{i=0}^{\infty} c_i x^i\ ]$$

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

3. Terdapat $\sum_{i=0}^{\infty} 0x^i$ di dalam R[x] sedemikian hingga untuk setiap f(x) di dalam R[x], berlaku

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

dan

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} 0x^i = \sum_{i=0}^{\infty} (a_i+0)x^i = \sum_{i=0}^{\infty} a_i x^i .$$

4. Untuk setiap $f(x)=\sum_{i=0}^{\infty} a_i x^i \in R[x]$ terdapat $-f(x) = \sum_{i=0}^{\infty} (-a_i)x^i$ di dalam R[x] sedemikian hingga

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} (-a_i)x^i = \sum_{i=0}^{\infty} (a_i+(-a_i))x^i = \sum_{i=0}^{\infty} 0x^i,$$

dan

$$\sum_{i=0}^{\infty} (-a_i)x^i + \sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} (-a_i+a_i)x^i = \sum_{i=0}^{\infty} 0x^i.$$

5. $f(x)+g(x) = \sum_{i=0}^{\infty} (a_i+b_i)x^i$

$= \sum_{i=0}^{\infty} (b_i+a_i)x^i = g(x)+f(x).$

6. $f(x)g(x)$ di dalam $R[x]$ karena $a_n b_{i-n} \in R$ untuk setiap a_n, b_{i-n} di dalam R.

7. $[f(x)g(x)]\ h(x)$

$= [(\sum_{i=0}^{\infty} a_i x^i)\ (\sum_{j=0}^{\infty} b_j x^j)]\ (\sum_{k=0}^{\infty} c_k x^k)$

$= [\sum_{n=0}^{\infty} (\sum_{i=0}^{n} a_i b_{n-i})\ x^n\ ](\sum_{k=0}^{\infty} c_k x^k)$

$= \sum_{s=0}^{\infty} [\sum_{n=0}^{s} (\sum_{i=0}^{n} a_i b_{n-i})\ c_{s-n}]\ x^s$

$= \sum_{s=0}^{\infty} (\sum_{i+j+k=s} a_i b_j c_k)\ x^s$

$= \sum_{s=0}^{\infty} [\sum_{m=0}^{s} a_{s-m}\ (\sum_{j=0}^{m} b_j c_{m-j})\ ]\ x^s$

$= (\sum_{i=0}^{\infty} a_i x^i)\ [\sum_{m=0}^{\infty} (\sum_{j=0}^{m} b_j c_{m-j})\ x^m\ ]$

$= (\sum_{i=0}^{\infty} a_i x^i)\ [(\sum_{j=0}^{\infty} b_j x^j)\ (\sum_{k=0}^{\infty} c_k x^k)]$

$= f(x)\ [g(x)h(x)].$

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

$$= \left(\sum_{i=0}^{\infty} a_i x^i\right)\left[\sum_{i=0}^{\infty} (b_i+c_i)\, x^i\right]$$

$$= \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} (a_i(b_{n-i}+c_{n-i}))\right) x^n$$

$$= \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} (a_i b_{n-i} + a_i c_{n-i})\right) x^n$$

$$= \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} a_i b_{n-i}\right) x^n + \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} a_i c_{n-i}\right) x^n$$

$$= \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right) + \left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} c_i x^i\right)$$

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

9. $$f(x)g(x) = \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} a_i b_{n-i}\right) x^n$$

$$= \sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} b_{n-i} a_i\right) x^n$$

$$= \left(\sum_{i=0}^{\infty} b_i x^i\right)\left(\sum_{i=0}^{\infty} a_i x^i\right) = g(x)f(x).$$

Dari 1,2,...,9 terbukti bahwa R[x] ring komutatif ▓

Suatu elemen e dalam ring R disebut **elemen satuan** untuk ring R jika $ea=ae=a$ untuk setiap $a \in R$.

Teorema 2.1.2

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

Bukti

Untuk setiap $f(x) = \sum_{i=0}^{\infty} a_i x^i$ di dalam R[x], berlaku

$$(\sum_{i=0}^{\infty} a_i x^i)\,(ex^0) = \sum_{i=0}^{\infty} (a_i x^i)(e\,x^0) = \sum_{i=0}^{\infty} (\,a_i e\,)\,x^{i+0} = \sum_{i=0}^{\infty} a_i x^i,$$

dan

$$(ex^0)\,(\sum_{i=0}^{\infty} a_i x^i) = \sum_{i=0}^{\infty} (ex^0)(a_i x^i\,) = \sum_{i=0}^{\infty} (ea_i)\,x^{0+i} = \sum_{i=0}^{\infty} a_i x^i. \blacksquare$$

Suatu elemen $a \neq 0$ dalam ring komutatif R disebut **pembagi nol** dalam R jika terdapat $b \in R$, $b \neq 0$ sedemikian hingga $ab=0$.

Teorema 2.1.3

Jika R tidak mempunyai pembagi nol, maka R[x] tidak memuat pembagi nol.

Bukti

Andaikan R adalah ring yang tidak mempunyai pembagi nol. Misalkan $p(x) = \sum_{j=0}^{\infty} a_j x^j$ dan $q(x) = \sum_{j=0}^{\infty} b_j x^j$ di dalam R[x] $p(x) \neq 0$ dan $q(x) \neq 0$. Karena $p(x) \neq 0$, maka terdapat koefisien dari x^j yang tidak sama dengan nol , misalkan a_m adalah koefisien dengan indeks tertinggi yang tidak sama dengan nol. Karena $q(x) \neq 0$, maka terdapat koefisien dari x^j yang tidak sama dengan nol, misalkan b_n adalah koefisien dengan indeks tertinggi yang tidak sama dengan nol. Sehingga

$$p(x)q(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots + a_m b_n x^{m+n}.$$

Karena R tidak memuat pembagi nol, maka $a_m b_n \neq 0$. Sehingga $p(x)q(x) \neq 0$. Jadi R[x] tidak memuat pembagi nol. $\blacksquare$

2.2 Algoritma Pembagian pada Polinomial

Lemma 2.2.1

Jika p(x) dan q(x) adalah elemen-elemen yang tidak sama dengan nol dari F[x], di mana F Field, maka d(p(x)q(x)) = d(p(x)) + d(q(x)).

Bukti

Misalkan $p(x) = \sum_{i=0}^{\infty} a_i x^i$ dan $q(x) = \sum_{i=0}^{\infty} b_i x^i$ di dalam F[x], di mana d(p(x))=m dan d(q(x))=n. Dengan definisi 2.1.2,

$$p(x)q(x) = \sum_{i=0}^{\infty} d_i x^i \text{ dengan } d_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Maka $d_{m+n} = a_m b_n \neq 0$ karena $a_m \neq 0$ dan $b_n \neq 0$.

Selanjutnya akan diselidiki untuk $i>m+n$. Karena $i=j+(i-j)$, maka bila $i > m+n$, maka $j>m$ atau $(i-j)>n$. Karena $j>m$ atau $(i-j)>n$, maka $a_j=0$ atau $b_{i-j} = 0$. Sehingga $a_j b_{i-j}=0$.

Jadi $d_i = \sum_{j=0}^{i} a_j b_{i-j} = 0$ untuk $i>m+n$. Jadi koefisien tertinggi yang tidak sama dengan nol dari p(x)q(x) adalah $a_m b_n$, yaitu d(p(x)q(x)) = m+n = d(p(x)) + d(q(x)). ∎

Akibat 1

Jika p(x), q(x) adalah elemen-elemen yang tidak sama dengan nol dari F[x], di mana F Field, maka $d(p(x)) \leq d(p(x)q(x))$.

Bukti

d(p(x)q(x)) = d(p(x)) + d(q(x)). Karena d(q(x)) ≥ 0, maka d(p(x)q(x)) ≥ d(p(x)). ∎

Teorema 2.2.1 (Algoritma pembagian pada F[x])

Jika f(x) dan g(x) di dalam F[x] dengan F Field, dan $g(x) \neq 0$, maka terdapat dengan tunggal polinomial-polinomial q(x) dan r(x) atas F sedemikian hingga 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) berturut-turut disebut **hasil bagi** dan **sisa** dalam pembagian f(x) oleh g(x).

Bukti

1. Jika d(f(x)) < d(g(x)), maka diambil q(x)=0 dan r(x)=f(x), sehingga f(x) = g(x)q(x) + r(x) dengan d(r(x)) < d(g(x)).
2. Misalkan $f(x) = a_o + a_1x + \ldots + a_mx^m$, $a_m \neq 0$

   dan

   $g(x) = b_o + b_1x + \ldots + b_nx^n$, $b_n \neq 0$ dan $m \geq n$.

   Jika m=0, maka $f(x)=a_o$ dan $g(x)=b_o$. Dalam hal ini $a_o = b_o b_o^{-1} a_o + 0$. Sehingga diperoleh $q(x) = b_o^{-1}a_o$ dan r(x)=0.

   Untuk $m \neq 0$ dibuktikan dengan induksi matematik pada d(f(x)). Andaikan teorema benar untuk polinomial dengan derajat < m. Misalkan $f_1(x) = f(x) - (a_m b_n^{-1} x^{m-n}) g(x)$. Maka $d(f_1(x)) < d(f(x))$ karena

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

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

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

$$+ \ldots + a_m b_{n-1} b_n^{-1} x^{m-1} + a_m b_n b_n^{-1} x^m)$$

$$= (a_0 + a_1 x^1 + \ldots + a_m x^m) - (a_m b_0 b_n^{-1} x^{m-n} + a_m b_1 b_n^{-1} x^{m-n+1}$$

$$+ \ldots + a_m b_{n-1} b_n^{-1} x^{m-1} + (a_m e) x^m)$$

$$= (a_0 + a_1 x^1 + \ldots + a_m x^m) - (a_m b_0 b_n^{-1} x^{m-n} + a_m b_1 b_n^{-1} x^{m-n+1}$$

$$+ \ldots + a_m b_{n-1} b_n^{-1} x^{m-1} + a_m x^m)$$

$$= a_0 + a_1 x^1 + \ldots - a_m b_{n-1} b_n^{-1} x^{m-1}.$$

Jadi $d(f_1(x)) < d(f(x))$.

Sehingga menurut pengandaian terdapat polinomial $q_1(x)$ dan $r_1(x)$ sedemikian hingga

$f_1(x) = g(x)q_1(x) + r_1(x)$ dengan $r_1(x) = 0$ atau $d(r_1(x)) < d(g(x))$.

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

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

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

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

Maka $q(x) = q_1(x) + a_m b_n^{-1} x^{m-n}$ dan $r(x) = r_1(x)$. Ini membuktikan bahwa $q(x)$ dan $r(x)$ ada.

Tinggal membuktikan bahwa polinomial $q(x)$ dan $r(x)$ tunggal. Andaikan ada polinomial lain yaitu $q'(x)$ dan $r'(x)$ atas F , dan

$f(x)=g(x)q'(x)+r'(x)$ dengan $r'(x)=0$ atau $d(r'(x)) < d(g(x))$. Maka

$$g(x)q(x)+r(x) = g(x)q'(x)+r'(x),$$

sehingga

$$g(x)[q(x)-q'(x)] = r'(x)-r(x),$$

di mana $r'(x)-r(x) = 0$ atau $d(r'(x)-r(x)) < d(g(x))$. Demikian juga $g(x)[q(x)-q'(x)] = 0$ atau $d(g(x)[q(x)-q'(x)]) \geq d(g(x))$. Maka $g(x)[q(x)-q'(x)]=0$, sehingga $q(x)=q'(x)$ karena $g(x)\neq 0$. Jadi $r(x)-r'(x) = 0$, sehingga $r(x)=r'(x)$. ∎

Contoh 2.2.1

$f(x) = 2x^4+x^2-x+1$ dan $g(x) = 2x-1$ di dalam $R[x]$, di mana R adalah field bilangan real.

Maka

$$\begin{array}{r|l} & x^3+\frac{1}{2}x^2+\frac{3}{4}x+(-\frac{1}{8}) \\ \hline 2x-1 & 2x^4+x^2-x+1 \\ & \underline{2x^4-x^3} \\ & x^3+x^2-x+1 \\ & \underline{x^3-\frac{1}{2}x^2} \\ & \frac{3}{2}x^2-x+1 \\ & \underline{\frac{3}{2}x^2-\frac{3}{4}x} \\ & -\frac{1}{4}x+1 \\ & \underline{-\frac{1}{4}x+\frac{1}{8}} \\ & \frac{7}{8} \end{array}$$

Diperoleh $q(x) = x^3+\frac{1}{2}x^2+\frac{3}{4}x+(-\frac{1}{8})$ dan $r(x)=\frac{7}{8}$ sedemikian hingga $2x^4+x^2-x+1 = (x^3+\frac{1}{2}x^2+\frac{3}{4}x-\frac{1}{8})(2x-1)+\frac{7}{8}$.

Akibat 1

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

Bukti

Misalkan hasil bagi $f(x)$ oleh $x-c$ adalah $q(x) \in F[x]$ dan sisanya adalah r, yaitu

$$f(x) = (x-c)q(x) + r.$$

Substitusi c untuk x menghasilkan

$$\begin{aligned} f(c) &= (c-c)q(c) + r \\ &= 0\ q(c) + r \\ &= r. \end{aligned}$$

Jadi sisa pembagian $f(x)$ oleh $x-c$ adalah $r=f(c)$. ∎

Teorema ini dikenal sebagai **teorema sisa.**

Contoh 2.2.2

Pembagian $f(x)= x^3-2x^2+2$ di dalam $R[x]$ oleh $x-3$ di dalam $R[x]$.

$$\begin{array}{r|l} x-3 & x^2+x+3 \\ \hline & x^3-2x^2+2 \\ & x^3-3x^2 \quad - \\ \hline & \quad x^2+2 \\ & \quad x^2-3x \quad - \\ \hline & \quad\quad 3x+2 \\ & \quad\quad 3x-9 \quad - \\ \hline & \quad\quad\quad 11 \end{array}$$

$f(x) = (x-3)(x^2+x+3) + 11$. $f(3)=11$ = sisa pembagian x^3-2x^2+2 oleh $x-3$.

Jika $f(x), g(x) \in F[x]$, dengan $g(x) \neq 0$, maka $f(x)$ dikatakan **habis dibagi** oleh $g(x)$, jika $f(x) = g(x)q(x)$, untuk $q(x) \in F[x]$. Jika $f(x)$ habis dibagi $g(x)$, maka dikatakan $g(x)$ adalah **faktor** dari $f(x)$, atau $g(x)$ **membagi** $f(x)$, dan ditulis dengan notasi $g(x) | f(x)$.

Akibat 2

Jika $f(x) \in F[x]$ dan $c \in F$, maka $x-c$ adalah faktor dari $f(x)$ bila dan hanya bila $f(c)=0$.

Bukti

Menurut teorema sisa $f(x)=(x-c)q(x) + f(c)$. Jika $f(c)=0$, maka $f(x)=(x-c)q(x)$, berarti bahwa $(x-c)$ merupakan faktor dari $f(x)$.

Jika $x-c$ merupakan faktor dari $f(x)$, maka $f(x)=(x-c)q(x)$, dengan $q(x) \in F[x]$, sehingga $f(c) = (c-c)q(c) = 0$. Jadi $x-c$ adalah faktor dari $f(x)$ bila dan hanya bila $f(c)=0$. ∎

Teorema ini dikenal dengan **teorema faktor.**

Elemen $c \in F$ disebut **akar** dari polinomial $f(x) \in F[x]$ jika $f(c)=0$. Menurut teorema faktor, c adalah akar dari $f(x) \in F[x]$ bila dan hanya bila $x-c$ adalah faktor dari $f(x)$.

2.3 Faktorisasi Polinomial

Suatu polinomial atas field F disebut **monik** jika koefisien tertingginya adalah elemen satuan dari F.

Suatu elemen u di dalam daerah integral D disebut **unit** dari D jika u merupakan faktor dari elemen satuan e∈D.

Definisi 2.3.1

Misalkan a(x) dan b(x) adalah polinomial atas field F yang tidak keduanya polinomial nol. **Faktor persekutuan** dari a(x) dan b(x) adalah polinomial h(x) sedemikian hingga h(x)|a(x) dan h(x)|b(x).

Teorema 2.3.1

Jika a(x) dan b(x) adalah polinomial atas field F yang tidak keduanya polinomial nol, maka ada tunggal polinomial monik d(x) atas F sedemikian hingga :

(a) d(x)|a(x) dan d(x)|b(x), dan

(b) jika c(x) adalah polinomial sedemikian hingga c(x)|a(x) dan c(x)|b(x), maka c(x)|d(x).

Polinomial d(x) dalam teorema di atas disebut **faktor persekutuan terbesar**(FPB) dari a(x) dan b(x).

Bukti

Jika b(x)≠0, dengan algoritma pembagian diperoleh polinomial $q_1(x)$ dan $r_1(x)$ sedemikian hingga

$a(x)=b(x)q_1(x)+r_1(x)$, dengan $r_1(x)=0$ atau $d(r_1(x)) < d(b(x))$.

1. Jika $r_1(x)=0$, maka $b(x)|a(x)$, sehingga $d(x) = b(x)$ memenuhi (a) dan (b).
2. Jika $r_1(x)\neq 0$, dengan algoritma pembagian didapatkan $q_2(x)$

dan $r_2(x)$ sedemikian hingga

$b(x) = r_1(x)q_2(x) + r_2(x)$ dengan $d(r_2(x)) < d(r_1(x))$.

Algoritma pembagian tersebut diulangi terus sehingga diperoleh :

$a(x) = b(x)q_1(x)+r_1(x)$, dengan $d(r_1(x)) < d(b(x))$

$b(x) = r_1(x)q_2(x) + r_2(x)$ dengan $d(r_2(x)) < d(r_1(x))$

$r_1(x) = r_2(x)q_3(x) + r_3(x)$ dengan $d(r_3(x)) < d(r_2(x))$

:

:

$r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x)$ dengan $d(r_k(x)) < d(r_{k-1}(x))$

$r_{k-1}(x) = r_k(x)q_{k+1}(x)$.

Akhirnya didapatkan polinomial nol sebagai sisa karena $d(r_1(x)) > d(r_2(x)) > d(r_3(x)) > \ldots$

Andaikan $r_k(x)$ melambangkan sisa terakhir yang tidak nol; akan dibuktikan bahwa $r_k(x)$ memenuhi (a) dan (b).

Perhatikan bahwa $r_k(x)|r_{k-1}(x)$, karena $r_{k-1}(x) = r_k(x)q_{k+1}(x)$. Selanjutnya $r_k(x)|r_{k-2}(x)$, karena $r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x)$. Proses ini diteruskan sampai akhirnya diperoleh

$r_k(x)|r_{k-1}(x)$, $r_k(x)|r_{k-2}(x)$, $r_k(x)|r_{k-3}(x)$, ... , $r_k(x)|b(x)$, $r_k(x)|a(x)$. Jadi terbukti bahwa $r_k(x)$ merupakan faktor persekutuan $a(x)$ dan $b(x)$.

Untuk membuktikan (b), andaikan $c(x)|a(x)$ dan $c(x)|b(x)$. Maka $c(x)|r_1(x)$ karena $r_1(x)=a(x)-b(x)q_1(x)$. Tetapi jika $c(x)|b(x)$ dan $c(x)|r_1(x)$, maka $c(x)|r_2(x)$ karena

$r_2(x) = b(x) - r_1(x)q_2(x)$. Proses ini diteruskan sehingga akhirnya kita memperoleh

$$c(x)|r_1(x), c(x)|r_2(x), c(x)|r_3(x), \ldots, c(x)|r_k(x).$$

Jadi (b) terbukti.

Jika koefisien tertinggi $r_k(x)$ adalah r, maka $r^{-1}.r_k(x)$ adalah polinomial monik yang memenuhi (a) dan (b).

Jika $b(x)=0$ dan a_m adalah koefisien tertinggi dari $a(x)$, maka $a_m^{-1}.a(x)$ adalah polinomial monik yang memenuhi (a) dan (b).

Akan dibuktikan ketunggalan dari faktor persekutuan terbesar dari a(x) dan b(x). Andaikan $d_1(x)$ dan $d_2(x)$ faktor persekutuan terbesar monik dari a(x) dan b(x). Maka $d_1(x)$ memenuhi:

1. $d_1(x)|a(x)$ dan $d_1(x)|b(x)$, dan
2. jika c(x) adalah polinomial sedemikian hingga $c(x)|a(x)$ dan $c(x)|b(x)$, maka $c(x)|d_1(x)$. (1)

Demikian juga $d_2(x)$ memenuhi :

1. $d_2(x)|a(x)$ dan $d_2(x)|b(x)$, dan
2. jika c(x) adalah polinomial sedemikian hingga $c(x)|a(x)$ dan $c(x)|b(x)$, maka $c(x)|d_2(x)$. (2)

Karena $d_1(x)|a(x)$ dan $d_1(x)|b(x)$, maka $d_1(x)|d_2(x)$ (menurut 2).

Karena $d_2(x)|a(x)$ dan $d_2(x)|b(x)$, maka $d_2(x)|d_1(x)$ (menurut 1).

Karena $d_1(x)|d_2(x)$, maka $d_2(x) = h(x)d_1(x)$ untuk suatu $h(x) \in F[x]$ (3)

Karena $d_2(x)|d_1(x)$, maka $d_1(x) = g(x)d_2(x)$ untuk suatu

$g(x) \in F[x]$ (4).

Substitusi (4) ke (3) menghasilkan $d_2(x) = h(x)g(x)\ d_2(x)$. Sehingga $h(x)g(x) = e$. Jadi $h(x)$ dan $g(x)$ adalah unit dalam F. Maka $d_1(x) = g(x)d_2(x)$ di mana $g(x)$ adalah suatu unit di dalam F. Karena $d_1(x)$ dan $d_2(x)$ adalah monik, maka haruslah $g(x) = e$. Jadi $d_1(x) = d_2(x)$. ∎

Contoh 2.3.1

$a(x) = x^4-x^3-x^2+1$, dan $b(x)=x^3-1$ adalah polinomial atas field rasional, maka

$$x^4-x^3-x^2+1 = (x^3-1)\ (x-1) + (-x^2+x)$$

$$x^3-1 = (-x^2+x)\ (-x-1) + (x-1)$$

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

Jadi Faktor persekutuan terbesar dari $x^4-x^3-x^2+1$ dan x^3-1 adalah $x-1$.

Teorema 2.3.2

Jika a(x) dan b(x) adalah polinomial atas field F, yang tidak keduanya nol, dan d(x) adalah FPB-nya, maka ada polinomial-polinomial u(x) dan v(x) atas F sedemikian hingga $d(x) = a(x)u(x) + b(x)v(x)$.

Bukti

Dari bukti teorema 2.3.1 didapatkan

$$r_{k-2}(x) = r_{k-1}(x)q_k(x) + r_k(x),$$

sehingga $r_k(x)$ merupakan kombinasi linier dari $r_{k-1}(x)$ dan $r_{k-2}(x)$, yaitu

$$r_k(x) = r_{k-2}(x) - r_{k-1}(x)q_k(x). \qquad (1)$$

Dari bukti teorema 2.3.1 diperoleh juga

$$r_{k-3}(x) = r_{k-2}(x)\, q_{k-1}(x) + r_{k-1}(x). \quad (2)$$

Jika (2) disubstitusikan ke dalam persamaan (1) diperoleh $r_k(x)$ sebagai kombinasi linier dari $r_{k-2}(x)$ dan $r_{k-3}(x)$ yaitu

$$r_k(x) = r_{k-2}(x) - r_{k-1}(x)q_k(x)$$

$$= r_{k-2}(x) - [r_{k-3}(x) - r_{k-2}(x)q_{k-1}(x)]q_k(x)$$

$$= r_{k-2}(x)[1+q_{k-1}(x)q_k(x)] - r_{k-3}(x)q_k(x). \quad (3)$$

Dari bukti teorema 2.3.1 diperoleh

$$r_{k-4}(x) = r_{k-3}(x)\, q_{k-2}(x) + r_{k-2}(x). \quad (4)$$

Substitusi (4) ke dalam (3) menghasilkan $r_k(x)$ sebagai kombinasi linier dari $r_{k-3}(x)$ dan $r_{k-4}(x)$. Jika proses ini diteruskan, maka akan didapat $r_k(x)$ sebagai kombinasi linier dari $r_2(x)$ dan $r_1(x)$, $r_k(x)$ sebagai kombinasi linier dari $r_1(x)$ dan $b(x)$ dan akhirnya sebagai kombinasi linier dari $b(x)$ dan $a(x)$, yaitu $r_k(x) = u(x)a(x) + v(x)b(x)$. ∎

Contoh 2.3.2

Jika $a(x) = x^4-x^3-x^2+1$, $b(x)=x^3-1$ adalah polinomial atas field rasional, maka

$$x^4-x^3-x^2+1 = (x^3-1)(x-1) + (-x^2+x)$$

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

Dengan menggunakan contoh 2.3.1 baris keempat didapatkan

$$x-1 = (x^3-1) - (-x^2+x)(-x-1)$$
$$= (x^3-1) - [(x^4-x^3-x^2+1)-(x^3-1)(x-1)](-x-1)$$
$$= (x^4-x^3-x^2+1)(x+1) + (x^3-1)[1+(x-1)(-x-1)]$$
$$= (x^4-x^3-x^2+1)(x+1) + (x^3-1)(-x^2+2).$$

Jadi $d(x) = x-1 = a(x)u(x) + b(x)v(x)$ di mana $u(x) = x+1$ dan $v(x) = (-x^2+2)$.

Definisi 2.3.2

Suatu polinomial $f(x)$ yang bukan konstanta di dalam $F[x]$ dikatakan **irreducible** atas field F bila dan hanya bila jika $f(x)=a(x)b(x)$, maka $a(x)$ atau $b(x)$ mempunyai derajat nol.

Contoh 2.3.3

x^2-2 adalah irreducible atas field bilangan rasional, tetapi tidak atas field bilangan real karena $x^2-2 = (x+\sqrt{2})(x-\sqrt{2})$.

Teorema 2.3.3

Jika F adalah field, $a(x),b(x),p(x) \in F[x]$, $p(x)$ adalah polinomial irreducible atas F dan $p(x)|a(x)b(x)$, maka $p(x)|a(x)$ atau $p(x)|b(x)$.

Bukti

Jika $p(x)\nmid a(x)$, maka faktor persekutuan terbesar dari $p(x)$ dan $a(x)$ adalah e yaitu elemen satuan dari F. Maka menurut teorema 2.3.2 ada polinomial-polinomial $u(x)$ dan $v(x)$ sedemikian hingga

$$e = u(x)p(x) + v(x)a(x).$$

Jika kedua ruasnya dikalikan dengan $b(x)$, maka diperoleh

$$eb(x) = [u(x)p(x) + v(x)a(x)]b(x)$$

$$b(x) = u(x)p(x)b(x) + v(x)a(x)b(x).$$

Karena $p(x)|a(x)b(x)$, maka

$p(x)|[u(x)p(x)b(x) + v(x)a(x)b(x)]$. Jadi $p(x)|b(x)$.

Jadi jika $p(x)\nmid a(x)$, maka $p(x)|b(x)$. ∎

Akibat 1

Jika $p(x),a_1(x),a_2(x),\ldots,a_n(x)$ adalah polinomial-polinomial atas field F, dengan p(x) irreducible atas F dan $p(x)|a_1(x)a_2(x)\ldots a_n(x)$, maka $p(x)|a_i(x)$ untuk suatu i $(1\leq i\leq n)$.

Bukti

Dengan menggunakan induksi matematik. Teorema benar untuk i=2 yaitu jika $p(x)|a(x)b(x)$, maka $p(x)|a(x)$ atau $p(x)|b(x)$ (menurut teorema 2.3.3). Diasumsikan teorema benar untuk i=k-1, yaitu jika $p(x)|a_1(x)a_2(x)\ldots a_{k-1}(x)$, maka $p(x)|a_1(x)$ atau $p(x)|a_2(x)\ldots$ atau $p(x)|a_{k-1}(x)$. Dibuktikan teorema benar untuk i=k. Misalkan $g(x)=a_1(x)a_2(x)\ldots a_{k-1}(x)$. Maka

$$g(x)a_k(x) = a_1(x)a_2(x)a_3(x)\ldots a_k(x).$$

Jika $p(x)|g(x)a_k(x)$, maka $p(x)|g(x)$ atau $p(x)|a_k(x)$. Karena $g(x) = a_1(x)a_2(x)\ldots a_{k-1}(x)$, maka diperoleh $p(x)|a_1(x)$ atau $p(x)|a_2(x)$ ... atau $p(x)|a_{k-1}(x)$ atau $p(x)|a_k(x)$. ∎

Teorema 2.3.4

Jika F field, maka setiap polinomial f(x) yang bukan konstanta $\in$ F[x], dapat difaktorkan dalam F[x] sebagai perkalian polinomial-polinomial irreducible. Pemfaktoran tersebut adalah tunggal kecuali mungkin untuk urutan dan untuk faktor-faktor unit dari F.

Bukti

Misalkan $f(x) \in F[x]$ adalah polinomial yang bukan konstanta. Jika f(x) tak irreducible, maka $f(x) = g(x)h(x)$ dengan $d(g(x)) < d(f(x))$ dan $d(h(x)) < d(f(x))$. Jika g(x) dan h(x) keduanya irreducible, maka teorema terbukti. Jika tidak irreducible, maka difaktorkan kembali sehingga diperoleh polinomial-polinomial dengan derajat yang lebih rendah. Jika proses ini diteruskan akan diperoleh

$$f(x) = p_1(x)p_2(x)\ldots p_s(x)$$

di mana $p_i(x)$ $(1 \leq i \leq s)$ irreducible.

Selanjutnya, untuk membuktikan ketunggalan pemfaktoran itu andaikan

$$f(x) = p_1(x)p_2(x)\ldots p_s(x) = q_1(x)q_2(x)\ldots q_t(x) \qquad (1)$$

adalah faktorisasi f(x) ke dalam polinomial-polinomial irreducible $p_i(x)$ $(1 \leq i \leq s)$ dan $q_j(x)$ $(1 \leq j \leq t)$. Karena $p_1(x) \mid p_1(x)p_2(x)\ldots p_s(x)$ dan $p_1(x)p_2(x)\ldots p_s(x) = q_1(x)q_2(x)\ldots q_t(x)$, maka $p_1(x) \mid q_1(x)q_2(x)\ldots q_t(x)$.

Untuk $s \leq t$:

Dengan akibat 1 teorema 2.3.3, diperoleh $p_1(x) \mid q_j(x)$ untuk suatu j $(1 \leq j \leq t)$, misalkan $q_1(x)$. Karena $q_1(x)$ irreducible,

maka jika

$$q_1(x) = u(x)p_1(x),$$

maka $u(x)$ atau $p_1(x)$ berderajat nol. Padahal $p_1(x)$ irreducible, sehingga $u(x)$ harus berderajat nol di dalam $F[x]$, yaitu $u(x)$ unit di dalam F, misalkan $u(x)=u_1$, untuk u_1 unit dalam F. Dengan substitusi dan kanselasi pada persamaan (1), akan diperoleh

$$p_2(x)\ldots p_s(x) = u_1 q_2(x)\ldots q_t(x) .$$

Dengan cara yang analog, misalkan $q_2(x) = u_2\, p_2(x)$, sehingga akan diperoleh

$$p_3(x)\ldots p_s(x) = u_1 u_2 q_3(x)\ldots q_t(x).$$

Jika proses diteruskan akhirnya akan diperoleh

$$e = u_1 u_2 \ldots u_s q_{s+1}(x) \ldots q_t(x).$$

Jadi $q_i(x)$ $(s+1\le i\le t)$ adalah unit. Kontradiksi dengan asumsi bahwa $q_i(x)$ adalah irreducible. Jadi haruslah $s = t$.

Dengan cara yang analog dapat dibuktikan untuk $t<s$. Jadi $p_i(x)$ dan $q_j(x)$ adalah faktor-faktor irreducible yang sama kecuali mungkin untuk urutan dan faktor-faktor unit. ∎

BAB III

RING POLINOMIAL ATAS DAERAH FAKTORISASI TUNGGAL

3.1 Field Pembagi

Misalkan D daerah integral dan $D' = \{a \in D \mid a \neq 0\}$. Produk kartesian dari D dan D' adalah

$$D \times D' = \{(a,b) : a \in D, b \in D'\}.$$

Untuk setiap (a,b) dan (c,d) di dalam $D \times D'$ didefinisikan relasi $(a,b) \sim (c,d)$ bila dan hanya bila $ad = bc$.

Lemma 3.1.1

Relasi $\sim$ pada $D \times D'$ adalah relasi ekuivalensi.

Bukti

Untuk setiap (a,b),(c,d) dan (f,g) di dalam $D \times D'$ berlaku :

1. $(a,b) \sim (a,b)$ karena $ab=ba$.
2. Bila $(a,b) \sim (c,d)$, maka dengan definisi diperoleh $ad=bc$. Maka $cb=da$, yaitu $(c,d) \sim (a,b)$.
3. Jika $(a,b) \sim (c,d)$ dan $(c,d) \sim (f,g)$, maka $ad=bc$ dan $cg=df$. Sehingga $adg = bcg$ dan $bcg = bdf$. Maka $adg = bdf$, sehingga $(ag)d = (bf)d$. Karena D daerah integral dan $d \neq 0$, maka $ag=bf$ yaitu $(a,b) \sim (f,g)$. ∎

Jika $(a,b) \in D \times D'$, maka kelas ekuivalensi yang memuat (a,b) dilambangkan dengan [a,b], yaitu

$$[a,b] = \{(x,y) \in D \times D' \mid (a,b) \sim (x,y)\}.$$

Himpunan dari semua kelas ekuivalensi kita lambangkan dengan F_D.

Definisi 3.1.1

Pada F_D didefinisikan operasi penjumlahan dan perkalian sebagai berikut :

(1) $[a,b] + [c,d] = [ad+bc, bd]$

(2) $[a,b] \cdot [c,d] = [ac, bd]$

untuk setiap $[a,b],[c,d] \in F_D$.

Kedua operasi yang didefinisikan di atas adalah well defined, yaitu jika

$$[a_1,b_1] = [a_2,b_2] \text{ dan } [c_1,d_1] = [c_2,d_2],$$

maka

$$[a_1d_1+b_1c_1, b_1d_1] = [a_2d_2+b_2c_2, b_2d_2]$$

dan

$$[a_1c_1, b_1d_1] = [a_2c_2, b_2d_2].$$

Bukti

Karena $[a_1,b_1] = [a_2,b_2]$, maka $(a_1,b_1) \sim (a_2,b_2)$, sehingga

$$a_1b_2 = b_1a_2. \qquad (1)$$

Dan karena $[c_1,d_1] = [c_2,d_2]$, maka $(c_1,d_1) \sim (c_2,d_2)$, sehingga

$$c_1d_2 = d_1c_2. \qquad (2)$$

Maka

$$\begin{aligned}(a_1d_1+b_1c_1)(b_2d_2) &= a_1d_1b_2d_2 + b_1c_1b_2d_2\\ &= a_1b_2d_1d_2 + b_1b_2c_1d_2\\ &= b_1a_2d_1d_2 + b_1b_2d_1c_2\\ &= b_1d_1a_2d_2 + b_1d_1b_2c_2\\ &= b_1d_1(a_2d_2 + b_2c_2).\end{aligned}$$

Jadi $[a_1d_1+b_1c_1, b_1d_1] = [a_2d_2+b_2c_2, b_2d_2]$.

Demikian pula $(a_1c_1)(b_2d_2) = a_1b_2c_1d_2$

$= b_1a_2d_1c_2$

$= b_1d_1a_2c_2$

$= (b_1d_1)(a_2c_2)$.

Jadi $[a_1c_1,b_1d_1] = [a_2c_2,b_2d_2]$.

Teorema 3.1.1

F_D dengan kedua operasi yang didefinisikan pada definisi 3.1.1 merupakan field.

Bukti

Untuk setiap $[a,b],[c,d]$ dan $[f,g]$ di dalam F_D, maka

1. $[a,b] + [c,d] = [ad+bc, bd]$ di dalam F_D karena $ad+bc \in D$ dan $bd \in D'$ untuk setiap $[a,b],[c,d]$ di dalam F_D.
2. $([a,b] + [c,d]) + [f,g] = [ad+bc, bd] + [f,g]$

   $= [(ad+bc)g + (bd)f, (bd)g]$

   $= [(ad)g + (bc)g +(bd)f , (bd)g]$

   $= [a(dg) + b(cg) +b(df) , b(dg)]$

   $= [a(dg) + b(cg+df), b(dg)]$

   $= [a,b] + [cg+df,dg]$

   $= [a,b] + ([c,d]+[f,g])$.
3. Terdapat $[0,d] \in F_D$ sedemikian hingga untuk setiap $[a,b] \in F_D$, berlaku

   $[a,b]+[0,d] = [ad+b0,bd] = [ad,bd] = [a,b]$,

   dan

   $[0,d]+[a,b] = [0b+da,db] = [da,db] = [a,b]$.
4. Untuk setiap $[a,b] \in F_D$, terdapat $[-a,b] \in F_D$ sedemikian hingga

$[a,b]+[-a,b] = [ab+(-ba),bb] = [0,bb] = [0,d]$ karena $(0,bb) \sim (0,d)$,

dan

$[-a,b]+[a,b] = [-ab+ba,bb] = [0,bb] = [0,d]$.

5. $[a,b]+[c,d] = [ad+bc,bd] = [da+cb,db] = [cb+da,db] = [c,d]+[a,b]$.

6. $[a,b]\,[c,d] = [ac,bd]$ di dalam F_D karena $ac \in D$ dan $bd \in D'$ untuk setiap $[a,b],[c,d]$ di dalam F_D.

7. $[a,b][c,d] = [ac,bd] = [ca,db] = [c,d][a,b]$.

8. $([a,b]\,[c,d])\,[f,g] = [ac,bd]\,[f,g] = [(ac)f,\ (bd)g] = [a(cf),b(dg)] = [a,b]\,[cf,dg] = [a,b]\,([c,d]\,[f,g])$.

9. $[a,b]\,([c,d] + [f,g]) = [a,b]\,[cg+df,dg]$
$= [a(cg+df),\ b(dg)]$
$= [acg+adf,\ bdg]$
$= [b(acg+adf),\ b(bdg)]$
$= [(ac)(bg)+(bd)(af),\ (bd)(bg)]$
$= [ac,bd] + [af,bg]$
$= [a,b][c,d] + [a,b][f,g]$.

10. Terdapat $[d,d] \in F_D$ sedemikian hingga untuk setiap $[a,b] \in F_D$, berlaku

$[a,b][d,d] = [ad,bd] = [a,b]$, dan

$[d,d][a,b] = [da,db] = [a,b]$.

11. Jika $[a,b] \in F_D$ dan $[a,b] \neq [0,d]$, maka $a \neq 0$ di dalam D, sehingga $[b,a] \in F_D$. Selanjutnya $[a,b][b,a] = [ab,ba] = [d,d]$ sebab $ab=ba$. Jadi $[b,a]$ di dalam F_D adalah invers dari $[a,b] \neq [0,d]$ dalam F_D.

Teorema 3.1.2

Jika $D_1 = \{[a,e] \mid a \in D\}$, maka D_1 adalah subdaerah integral dari F_D dan $D \approx D_1$.

Bukti

Misalkan $\Theta : D \longrightarrow F_D$ yang didefinisikan dengan $\Theta(a) = [a,e]$ untuk setiap $a \in D$. Maka jelas bahwa $\Theta(D) = D_1$.

Untuk setiap $a,b \in D$ berlaku

$\Theta(a+b) = [a+b,e] = [ae+eb,ee] = [a,e]+[b,e] = \Theta(a) + \Theta(b)$, dan

$\Theta(ab) = [ab,e] = [ab,ee] = [a,e][b,e] = \Theta(a)\,\Theta(b)$.

Untuk setiap $a,b \in D$, bila $\Theta(a)=\Theta(b)$, maka $[a,e]=[b,e]$. Jadi $(a,e) \sim (b,e)$, yang berarti $ae=eb$, yaitu $a=b$. Jadi $D \approx \Theta(D) = D_1$, dan D_1 adalah subdaerah integral dalam F_D. ▓

Dari Teorema 3.1.2 dapat disimpulkan bahwa sebarang daerah integral D dapat diperluas menjadi suatu field F_D yang memuat D. Field ini disebut **Field Pembagi** dari D.

3.2 Ring Polinomial atas Daerah Faktorisasi Tunggal

Definisi 3.2.1

Elemen a dan b di dalam daerah integral D dikatakan **bersekawan** jika $a|b$ dan $b|a$.

Teorema 3.2.1

Elemen a dan b di dalam daerah integral D adalah bersekawan bila dan hanya bila $a=bu$ untuk suatu unit u dari D.

Bukti

Bila a dan b bersekawan, maka $a|b$ yaitu $b=ac$ untuk suatu $c \in D$, dan $b|a$ yaitu $a=bu$ untuk suatu $u \in D$. Jadi $b = (bu)c = b(uc)$. Karena $b \neq 0$, dengan kanselasi kiri diperoleh $e = uc$ untuk suatu u di dalam D. Jadi u unit dari D.

Sebaliknya bila $a=bu$ untuk suatu unit u dari D, maka $e=um$ untuk suatu $m \in D$. Karena $ae = bu$, maka $a(um) = bu$, sehingga $(am)u = bu$. Dengan kanselasi kanan diperoleh $am = b$. Jadi $a|b$ dan $b|a$. ▓

Definisi 3.2.2

Suatu elemen p yang bukan nol dan bukan unit dari daerah integral D disebut **irreducible** dari D jika untuk sebarang faktorisasi $p=ab$ di dalam D, maka a atau b adalah unit.

Definisi 3.2.3

Suatu daerah integral D disebut **daerah faktorisasi tunggal** jika memenuhi aksioma berikut :

a. Jika $a \in D$, $a \neq 0$ dan a bukan unit, maka a dapat ditulis sebagai perkalian berhingga elemen-elemen irreducible dari D.

b. Jika $a \in D$ dan $a = p_1 \dots p_r = q_1 \dots q_s$, p_i $(1 \leq i \leq r)$, q_j $(1 \leq j \leq s)$ irreducible, maka $r=s$ dan setiap p_i bersekawan dengan suatu q_i.

Definisi 3.2.4

Jika D adalah daerah faktorisasi tunggal, maka suatu

polinomial yang bukan konstan $f(x) = a_o + a_1x + \ldots + a_nx^n$ di dalam D[x] disebut **primitif** bila dan hanya bila faktor-faktor persekutuan dari semua a_i hanyalah unit-unit dari D.

Contoh 3.2.1

Dalam Z[x], $4x^2+3x+2$ adalah primitif.

Lemma 3.2.1

Jika D adalah daerah faktorisasi tunggal, dan $f(x) \in D[x]$, f(x) bukan konstanta, maka $f(x) = c\ g(x)$, di mana $c \in D$, $g(x) \in D[x]$, dan g(x) primitif di dalam D[x]. Elemen c dan g(x) tersebut adalah tunggal tanpa memperhatikan faktor unit di dalam D. Elemen c itu disebut **content** dari f(x).

Bukti

Misalkan $f(x) \in D[x]$, di mana f(x) adalah polinomial yang bukan konstan. Karena D adalah daerah faktorisasi tunggal, maka setiap koefisien dari f(x) dapat difaktorkan menjadi perkalian berhingga elemen-elemen irreducible di dalam D secara tunggal, tanpa memperhatikan urutan dan sekawannya. Misalkan setiap koefisien dari f(x) difaktorkan demikian itu. Jika p adalah elemen irreducible yang membagi setiap koefisien dari f(x), gantilah setiap sekawan dari p dalam faktorisasi dari koefisien-koefisien tersebut dengan pu, di mana u suatu unit. Prosedur ini diteruskan untuk elemen irreducible lainnya q yang muncul dalam faktorisasi dari suatu koefisien f(x), dan seterusnya. Akhirnya akan

diperoleh faktorisasi dari koefisien-koefisien f(x), di mana setiap elemen irreducible p_i yang muncul dalam faktorisasi dari suatu koefisien dan yang membagi semua koefisien, juga akan muncul dalam faktorisasi dari semua koefisien, tetapi tidak satupun sekawan dari p_i yang muncul dalam faktorisasi dari koefisien manapun. Misalkan $c = \prod_i p_i^{v_i}$, yaitu perkalian dari semua elemen irreducible p_i yang muncul dalam faktorisasi dari semua koefisien tersebut, dan v_i adalah bilangan bulat terbesar sedemikian hingga $p_i^{v_i}$ membagi semua koefisien. Maka f(x) = c g(x), di mana $c \in D$, $g(x) \in D[x]$, dan g(x) adalah primitif.

Selanjutnya akan dibuktikan ketunggalan dari c dan g(x). Jika f(x) = d h(x) untuk $d \in D$, $h(x) \in D[x]$ dan h(x) primitif, maka setiap elemen irreducible yang merupakan faktor dari c harus membagi d dan sebaliknya. Karena c g(x) = d h(x) dan dengan mengkansel faktor-faktor irreducible dari c, akan diperoleh u g(x) = v h(x) di mana u dan v keduanya unit. Sehingga c adalah tunggal tanpa memperhatikan faktor unit. Karena f(x) = c g(x), maka polinomial primitif g(x) juga tunggal tanpa memperhatikan faktor-faktor unit. ■

Lemma 3.2.2

Jika D adalah daerah faktorisasi tunggal, maka perkalian dari dua polinomial primitif di dalam D[x] adalah primitif.

Bukti

Misalkan $f(x) = a_o + a_1x + \ldots + a_nx^n$,

dan

$g(x) = b_o + b_1x + \ldots + b_mx^m$ adalah primitif di dalam D[x]. Misalkan p adalah elemen irreducible di dalam D. Maka p bukan pembagi semua a_i dan p bukan pembagi semua b_j, sebab f(x) dan g(x) primitif. Misalkan a_r adalah koefisien pertama dari f(x) yang tidak dapat dibagi oleh p, yaitu $p|a_i$ untuk $i<r$, tetapi $p\nmid a_r$ (p bukan faktor a_r). Demikian pula, misalkan $p|b_j$ untuk $j<s$, tetapi $p\nmid b_s$. Koefisien dari x^{r+s} di dalam f(x)g(x) adalah

$$c_{r+s} = (a_ob_{r+s} + \ldots + a_{r-1}b_{s+1}) + a_rb_s + (a_{r+1}b_{s-1} + \ldots + a_{r+s}b_o).$$

Karena $p|a_i$ untuk $i<r$, maka

$$p|(a_ob_{r+s} + \ldots + a_{r-1}b_{s+1}),$$

dan karena $p|b_j$ untuk $j<s$, maka

$$p|(a_{r+1}b_{s-1} + \ldots + a_{r+s}b_o).$$

Karena p bukan faktor a_r atau b_s, maka p bukan faktor a_rb_s, sehingga p bukan faktor dari c_{r+s}. Hal ini menunjukkan bahwa untuk suatu elemen irreducible $p\in D$, terdapat koefisien dari f(x)g(x) yang tidak habis dibagi p. Jadi f(x)g(x) primitif.

Akibat

Jika D adalah daerah faktorisasi tunggal, maka perkalian berhingga banyak polinomial-polinomial primitif di dalam D[x] adalah primitif.

Bukti

Dengan menggunakan induksi matematik. Menurut lemma 3.2.2 perkalian dua polinomial primitif adalah primitif. Andaikan

perkalian n polinomial primitif adalah primitif. Misalkan $f_1(x),f_2(x),...,f_n(x),f_{n+1}(x)$ adalah polinomial-polinomial primitif di dalam D[x]. Maka $m(x) = f_1(x)f_2(x)...f_n(x)$ adalah primitif menurut hipotesis, sehingga $m(x)f_{n+1}(x)$ adalah primitif menurut lemma 3.2.2.

Lemma 3.2.3

Misalkan D adalah daerah faktorisasi tunggal dan F adalah field pembagi dari D. Misalkan $f(x) \in D[x]$, dengan $d(f(x)) > 0$. Jika f(x) irreducible dalam D[x], maka f(x) juga irreducible dalam F[x]. Selain itu, jika f(x) primitif dalam D[x] dan irreducible dalam F[x], maka f(x) irreducible dalam D[x].

Bukti

Misalkan f(x) polinomial bukan konstanta di dalam D[x], yang dapat difaktorkan menjadi polinomial-polinomial dengan derajat yang lebih rendah di dalam F[x]. Misalkan

$$f(x) = r(x)s(x)$$

untuk r(x),s(x) di dalam F[x]. Karena F adalah field pembagi D, maka setiap koefisien dari r(x) dan s(x) berbentuk [a,b] untuk a,b di dalam D, sehingga diperoleh

$$d\ f(x) = r_1(x)s_1(x)$$

untuk d di dalam D dan $r_1(x),s_1(x)$ di dalam D[x] dengan $d(r_1(x)) = d(r(x))$ dan $d(s_1(x)) = d(s(x))$. Dengan lemma 3.2.1, $f(x) = c\ g(x)$, $r_1(x) = c_1\ r_2(x)$ dan $s_1(x) = c_2\ s_2(x)$ untuk $g(x),r_2(x),s_2(x)$ primitif dan c,c_1,c_2 di dalam D. Sehingga

$$dc\ g(x) = c_1c_2\ r_2(x)s_2(x),$$

dan menurut lemma 3.2.2, polinomial $r_2(x)s_2(x)$ primitif. Dengan menggunakan sifat ketunggalan dari lemma 3.2.1, $c_1c_2=dcu$ untuk suatu unit u di dalam D, sehingga

$$dc\ g(x) = dcu\ r_2(x)s_2(x).$$

Karena $d\neq 0$ dan D daerah integral, maka berlaku kanselasi kiri. Jadi

$$f(x) = c\ g(x) = cu\ r_2(x)s_2(x).$$

Jadi jika f(x) dapat difaktorkan secara nontrivial dalam F[x], maka f(x) juga dapat difaktorkan secara nontrivial dalam polinomial-polinomial dengan derajat yang sama dalam D[x]. Jadi jika f(x) irreducible dalam D[x], maka ia juga irreducible dalam F[x].

Karena $D[x]\subseteq F[x]$, maka suatu polinomial bukan konstan $f(x) \in D[x]$, yang primitif di dalam D[x] dan irreducible dalam F[x] juga irreducible di dalam D[x].

Akibat

Jika D adalah daerah faktorisasi tunggal dan F adalah field pembagi dari D, maka polinomial bukan konstan $f(x)\in D[x]$ dapat difaktorkan menjadi perkalian dua polinomial dengan derajat yang lebih rendah dalam F[x] bila dan hanya bila f(x) mempunyai faktorisasi dalam polinomial-polinomial dengan derajat yang sama dalam D[x].

Bukti

Menurut bukti lemma 3.2.3, jika f(x) dapat difaktorkan menjadi perkalian dari dua polinomial dengan derajat lebih rendah dalam F[x], maka f(x) mempunyai faktorisasi dalam

polinomial-polinomial dengan derajat yang sama di dalam D[x].

Sebaliknya jelas, karena D[x]⊆ F[x].

Teorema 3.2.2

Jika D daerah faktorisasi tunggal, maka D[x] juga merupakan daerah faktorisasi tunggal.

Bukti

Misalkan f(x)∈D[x], di mana f(x) bukan nol dan bukan unit. Jika f(x) adalah konstanta, maka teorema terbukti. Misalkan d(f(x)) > 0. Kita pandang f(x) sebagai elemen dari F[x], di mana F adalah field pembagi dari D. Dengan teorema 2.3.4, $f(x) = p_1(x) \ldots p_r(x)$ di dalam F[x], di mana $p_i(x)$ adalah irreducible dalam F[x]. Karena F adalah field pembagi dari D, maka setiap koefisien dalam setiap $p_i(x)$ berbentuk [a,b] untuk a,b ∈ D. Maka

$$d\, f(x) = q_1(x) \ldots q_r(x),$$

di mana d∈D dan $q_i(x)$∈D[x]. Karena setiap $p_i(x)$ irreducible dalam F[x], maka $q_i(x)$, yang merupakan perkalian $p_i(x)$ dengan suatu unit dalam F, juga irreducible dalam F[x]. Dengan lemma 3.2.1, f(x) = c g(x) dan $q_i(x) = c_i\ q_i'(x)$ di dalam D[x] untuk g(x) dan $q_i'(x)$ primitif. Sehingga

$$dc\ g(x) = c_1 \ldots c_r\ q_1'(x) \ldots q_r'(x),$$

dengan akibat lemma 3.2.2 perkalian $q_1'(x), \ldots, q_r'(x)$ adalah primitif. Dengan sifat ketunggalan dari lemma 3.2,1, diperoleh

$$c_1 \ldots c_r = dcu$$

untuk suatu unit u di dalam D. Maka

$$dc\ g(x) = dcu\ q_1'(x) \ldots q_r'(x),$$

sehingga

$$f(x) = c\ g(x) = cu\ q_1'(x) \ldots q_r'(x).$$

Elemen cu dapat difaktorkan ke dalam elemen irreducible dalam D, sedangkan $q_1'(x), \ldots, q_r'(x)$ irreducible dalam D[x], sebab mereka primitif dan irreducible dalam F[x]. Jadi f(x) dapat difaktorkan ke dalam perkalian elemen-elemen irreducible dalam D[x].

Ketunggalan faktorisasi dari $f(x) \in D[x]$ adalah jelas untuk $f(x) \in D$ yang bukan nol dan bukan unit. Jika $d(f(x)) > 0$, tiap faktorisasi dari f(x) ke dalam elemen-elemen irreducible dalam D[x] dapat dipandang sebagai faktorisasi dalam F[x] ke dalam unit-unit (yaitu faktor-faktor dalam D) dan polinomial-polinomial irreducible dalam F[x] (dengan lemma 3.2.3). Dengan teorema 2.3.4 polinomial-polinomial ini adalah tunggal kecuali mungkin untuk faktor-faktor konstan dalam F. Tetapi sebagai elemen irreducible dalam D[x], setiap polinomial dengan derajat > 0 yang muncul dalam faktorisasi dari f(x) dalam D[x] adalah primitif. Dengan sifat ketunggalan dari lemma 3.2.1, hal ini menunjukkan bahwa polinomial-polinomial ini adalah tunggal dalam D[x] tanpa memperhatikan faktor-faktor unit, yaitu sekawannya. Perkalian elemen-elemen irreducible dalam D dalam faktorisasi dari f(x) adalah content dari f(x), yang juga tunggal tanpa memperhatikan faktor-faktor unit (dengan lemma 3.2.1). Jadi semua elemen irreducible dalam D[x] yang muncul

dalam faktorisasi itu adalah tunggal tanpa memperhatikan urutan dan sekawannya.

BAB IV

RING FAKTOR POLINOMIAL

Dalam teori ring telah dibuktikan bahwa jika R adalah ring, I ideal dari R dan R/I adalah himpunan semua koset kanan dari I yaitu $\{I+a \mid a \in R\}$, dan pada R/I didefinisikan operasi jumlahan dan perkalian sebagai berikut :

1. $(I+a) + (I+b) = I + (a+b)$
2. $(I+a)(I+b) = I + ab$,

untuk setiap I+a, I+b di dalam R/I , maka dengan kedua operasi tersebut R/I merupakan ring, yang disebut ring faktor.

Teorema 4.1

Jika F adalah field, 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 (0). 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 $I=(g(x))$. Jelas bahwa $(g(x)) \subseteq I$.

Misalkan $f(x) \in I$, maka dengan algoritma pembagian terdapat polinomial $q(x), r(x) \in F[x]$ sedemikian hingga

$f(x) = g(x)q(x)+r(x)$ 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 derajat

r(x)<derajat g(x) mengingat bahwa g(x) adalah polinomial dengan derajat paling kecil dalam I. Jadi f(x) = g(x)q(x) ∈ (g(x)). Jadi I=(g(x)). ∎

Teorema 4.2

Andaikan bahwa F adalah field dan p(x) ∈ F[x], maka ring faktor F[x]/(p(x)) adalah field bila dan hanya bila p(x) irreducible atas F.

Bukti

Misalkan I adalah ideal utama yang dibentuk oleh p(x) yaitu I=(p(x)).

1. Jika F[x]/I adalah field, maka p(x) irreducible atas F.
   Andaikan p(x) tidak irreducible atas F. Maka p(x)=a(x)b(x) dengan derajat a(x) maupun b(x) 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) ∉ I dan b(x) ∉ I. Jadi I+a(x) dan I+b(x) keduanya bukan merupakan elemen nol (yaitu I) dari F[x]/I. 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 mempunyai pembagi nol, maka F[x]/I bukan field.

2. Jika p(x) irreducible, maka F[x]/I adalah field.
   a. F[x]/I merupakan ring.
   b. Untuk setiap I+a(x), I+b(x) di dalam F[x]/I, maka

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

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

c. Terdapat $I+e$ di dalam $F[x]/I$, di mana e elemen satuan dari F sedemikian hingga untuk setiap $I+a(x) \in F[x]/I$ berlaku

$(I+a(x))(I+e) = I + a(x)e = I+a(x)$,

dan

$(I+e)(I+a(x)) = I + ea(x) = I+a(x)$.

d. Untuk setiap $I+f(x) \neq I$ di dalam $F[x]/I$ maka $f(x) \notin I$, yang berarti $f(x)$ bukan perkalian dari $p(x)$ di dalam $F[x]$. Karena $p(x)$ irreducible, maka $p(x)$ dan $f(x)$ mempunyai FPB e, sehingga $e = p(x)u(x)+f(x)v(x)$ untuk suatu $u(x),v(x)$ 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 hingga $(I+f(x))(I+v(x)) = I+e$, yang berarti $I+v(x)$ adalah invers dari $I+f(x)$. ∎

Teorema 4.3

Andaikan F adalah field, $p(x)= a_0 + a_1x + \ldots + a_nx^n$, 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:

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

Lagi pula jika p(x) irreducible, maka {I+b|b∈F} adalah subfield dari F[x]/I yang isomorfik dengan F.

Bukti

Ambil sebarang elemen I+f(x) ∈ F[x]/I. Dengan algoritma pembagian diperoleh f(x)=p(x)q(x)+r(x), untuk suatu q(x),r(x) ∈ F[x] dengan d(r(x)) < d(p(x)) atau r(x)=0. Maka f(x)-r(x) = p(x)q(x)∈I, sehingga I+f(x) = I+r(x).

Jadi setiap elemen dari F[x]/I dapat dinyatakan paling sedikit dengan satu cara dalam bentuk

$$I + (b_0+b_1x+\ldots+b_{n-1}x^{n-1})$$

dengan $b_0,b_1,\ldots,b_{n-1}\in F$. Andaikan I+f(x) ∈ F[x]/I dapat ditulis dengan cara lain, misalnya

$$I + (c_0+c_1x+\ldots+c_{n-1}x^{n-1})$$

dengan $c_0,c_1,\ldots,c_{n-1}\in F$. Maka

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

Sehingga

$$(b_0+b_1x+\ldots+b_{n-1}x^{n-1})+(-(c_0+c_1x+\ldots+c_{n-1}x^{n-1})) \in I,$$

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 $b_0-c_0 = 0$, maka $b_0= c_0$

$b_1-c_1 = 0$, maka $b_1= c_1$

⋮

$b_{n-1}-c_{n-1}=0$, maka $b_{n-1}= c_{n-1}$

Jadi I+f(x) dapat dinyatakan secara tunggal dalam bentuk tersebut.

Selanjutnya akan dibuktikan {I+b|b∈F} adalah subfield dari F[x]/I. Misalkan A = {I+b|b∈F}. Jelas bahwa A ⊂ F[x]/I karena setiap elemen I+a ∈ A pasti di dalam F[x]/I. Selanjutnya

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) ∈ A, dan (I+a) (I+b) = I + ab ∈ A.
3. Jika I+a ∈ A, maka I+(-a) ∈ A.
4. Untuk setiap I+a ≠ I di dalam A, maka invers dari I+a, yaitu $I+a^{-1}\in$ A karena a^{-1} di dalam F. $I+a^{-1}$ invers dari I+a terhadap perkalian karena $(I+a)(I+a^{-1}) = I+aa^{-1} =$ I+e.

Jadi A adalah subfield dari F[x]/I.

Misalkan α adalah pemetaan dari F ke {I+b|b∈F} yang didefinisikan dengan α(b) = I+b untuk setiap b∈F. Definisi tersebut well defined, sebab untuk setiap a,b∈F, bila a=b, maka I+a=I+b, sehingga α(a)=α(b).

Untuk setiap a,b di dalam F, berlaku

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

dan

$$\alpha(ab) = I+ab$$

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

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

Jadi α merupakan homomorfisme ring.

Ambil sebarang elemen $a,b \in F$ sedemikian hingga $\alpha(a)=\alpha(b)$. Maka $I+a=I+b$, sehingga $a-b \in I$ yang berarti $a-b$ habis dibagi oleh $p(x)$. Hal ini terjadi bila dan hanya bila $a-b=0$ (karena derajat $p(x)$ > derajat $(a-b)$), sehingga $a-b=0$. Jadi $a=b$.

Untuk setiap y di dalam $\{I+b \mid b \in F\}$, maka $y = I+a$ untuk $a \in F$. Jadi pasti terdapat $a \in F$ sedemikian hingga $\alpha(a) = I+a = y$. Jadi $F \approx \{I+b \mid b \in F\}$. ▓

Contoh 4.1

Misalkan R adalah field bilangan real dan $p(x) = 1+x^2 \in R[x]$ adalah irreducible atas R. Bila $I = (1+x^2)$, maka dengan teorema 4.2 $R[x]/I$ merupakan field. Buktikan bahwa $R[x]/I \approx C$ (field bilangan kompleks).

Bukti

Setiap elemen dari $R[x]/I$ dapat ditulis dengan tunggal sebagai $I+(a+bx)$ dengan $a,b \in R$. Misalkan β pemetaan dari $R[x]/I$ ke C yang didefinisikan dengan $\beta(I+(a+bx)) = a+bi$ untuk setiap $I+(a+bx)$ di dalam $R[x]/I$.

Misalkan $I+(a+bx)$, $I+(c+dx)$ sebarang elemen dari $R[x]/I$. Maka

$$\beta\,[(I+(a+bx)) + (I+(c+dx))] = \beta\,[I+((a+bx)+(c+dx))]$$
$$= \beta\,[I+ ((a+c) + (b+d)x)]$$
$$= (a+c) + (b+d)i$$

$= (a+c) + (bi+di)$

$= (a+bi) + (c+di)$

$= \beta(I+(a+bx)) + \beta(I+(c+dx))$

dan

$\beta\,[(I+(a+bx))\,(I+(c+dx))] = \beta\,[I+(ac + (ad+bc)x + bdx^2)]$.

Pembagian $ac + (ad+bc)x + bdx^2$ oleh $1+x^2$ menghasilkan

$ac + (ad+bc)x + bdx^2 = (1+x^2)bd + (ac-bd) + (ad+bc)x$.

Jadi

$(ac + (ad+bc)x + bdx^2) - ((ac-bd) + (ad+bc)x) = (1+x^2)bd \in I$,

sehingga

$I + (ac + (ad+bc)x + bdx^2) = I + (ac-bd) + (ad+bc)x)$.

Jadi $\beta\,[(I+(a+bx))\,(I+(c+dx))] = \beta\,[I+((ac-bd) + (ad+bc)x)]$

$= (ac-bd) + (ad+bc)i$

$= (a+bi)\,(c+di)$

$= \beta\,(I+(a+bx))\,\beta(I+(c+dx))$.

Jadi β merupakan homomorfisme ring.

Bila $a+bi, c+di \in C$ sedemikian hingga $a+bi=c+di$, maka $a=c$ dan $b=d$, sehingga $a+bx = c+dx$, dan akibatnya $I+(a+bx) = I+(c+dx)$.

Untuk setiap $a+bi \in C$, maka terdapat $a,b \in R$, sehingga $a+bx \in R[x]$, dan $I+(a+bx) \in R[x]/I$ sedemikian hingga $\beta(I+(a+bx)) = a+bi$. Jadi terbukti bahwa $R[x]/I \approx C$.

BAB V

PERLUASAN FIELD

5.1 Susunan Perluasan Field.

Definisi 5.1.1

Misalkan F adalah field. Field E disebut perluasan field (extension field) F jika E memuat F sebagai subfieldnya.

Contoh 5.1.1

Field bilangan rasional Q merupakan subfield dari field bilangan real R sehingga R merupakan perluasan Q.

Contoh 5.1.2

Misalkan F adalah field dan $p(x) \in F[x]$ irreducible atas F, maka $F[x]/(p(x))$ adalah perluasan field F, karena menurut teorema 4.3, $F[x]/(p(x))$ memuat F sebagai subfieldnya.

Definisi 5.1.2

Misalkan E perluasan field F. Jika $f(x) = a_0 + a_1x + \ldots + a_nx^n$ di dalam F[x], maka yang dimaksud f(c) untuk sebarang $c \in E$ adalah $a_0 + a_1c + \ldots + a_nc^n \in E$ yang merupakan nilai f(x) untuk x=c.

Teorema 5.1.1

Misalkan F adalah field dan $p(x) \in F[x]$ irreducible atas F, maka p(x) mempunyai akar di dalam suatu perluasan dari field

F, yaitu F[x]/(p(x)).

Bukti

Misalkan $p(x) = a_o + a_1x + \ldots + a_nx^n$ dan $(p(x))=I$.

Misalkan α melambangkan elemen $I+x \in F[x]/I$. Maka

$$p(\alpha) = a_o + a_1\alpha + \ldots + a_n\alpha^n$$

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

$$= a_o + a_1(I+x) + \ldots + a_n(I+x^n),$$

karena $F \approx \{I+a_i \mid a_i \in F\}$, maka dengan identifikasi setiap elemen $a_i \in F$ dengan $I+a_i \in \{I+a_i \mid a_i \in F\}$, akan diperoleh

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

$$= (I+a_o) + (I+a_1x) + \ldots + (I+a_nx^n)$$

$$= I + (a_o + a_1x + \ldots + a_nx^n)$$

$$= I + p(x)$$

$$= I.$$

Tetapi I adalah elemen nol dari F[x]/I, maka α adalah akar dari p(x) dalam F[x]/I. ∎

Akibat 1

Jika F adalah field dan f(x) adalah polinomial dengan derajat positip atas F, maka f(x) pasti mempunyai akar di dalam suatu perluasan F.

Bukti

Jika f(x) irreducible atas F, maka f(x) mempunyai akar di dalam suatu perluasan F (menurut teorema 5.1.1). Jika f(x) tidak irreducible, maka menurut teorema 2.3.4, f(x)

mempunyai faktor p(x) yang irreducible di dalam F[x]. Maka $f(x)=p(x)q(x)$ untuk suatu $q(x)\in F[x]$. Menurut teorema 5.1.1, maka p(x) mempunyai akar α di dalam F[x]/(p(x)), sehingga α juga merupakan akar untuk f(x) karena $f(\alpha) = p(\alpha)q(\alpha) = 0.q(\alpha) = 0$. ▓

Contoh 5.1.3

Misalkan F adalah field bilangan real dan $p(x) = x^2+1$ di dalam F[x]. Karena p(x) irreducible di dalam F[x], maka F[x]/(p(x)) merupakan field. Misalkan $I=(p(x))$ dan $\alpha = I+x$, maka

$$\begin{aligned} p(\alpha) &= \alpha^2 + 1 \\ &= (I+x)^2 + 1 \\ &= I + x^2 + 1 \\ &= I \end{aligned}$$

yaitu elemen nol dari F[x]/(p(x)). Jadi α adalah akar dari p(x) di dalam F[x]/(p(x)).

Teorema 5.1.2

Andaikan F field, E perluasan field F dan $a\in E$. Bila

$R = \{ M \mid M$ subfield dari E yang memuat a dan F$\}$,

dan $F(a) = \cap \{ M \mid M\in R \}$, maka F(a) merupakan subfield terkecil dari E yang memuat a dan F.

Bukti

R tidak kosong karena $E \in R$, sehingga $F(a)\neq\emptyset$. Untuk setiap v,w sebarang elemen F(a), maka v,w di dalam M untuk setiap $M\in R$. Karena M subfield dari E yang memuat a dan F, maka v+w,vw,-v di dalam M untuk setiap $M\in R$. Dan untuk setiap

$v \neq 0$, maka v^{-1} di dalam M untuk setiap $M \in R$. Sehingga $v+w, vw, -v$ di dalam $\cap\{M \mid M \in R\} = F(a)$, dan untuk setiap $v \neq 0$, maka v^{-1} di dalam $\cap\{M \mid M \in R\} = F(a)$. Jadi F(a) merupakan subfield dari E yang memuat a dan F .

Misalkan N sebarang subfield dari E yang memuat a dan F, maka $N \supseteq \cap \{M \mid M \in R\} = F(a)$. Jadi F(a) merupakan subfield terkecil yang memuat a dan F.

Definisi 5.1.3

Misalkan F field dan E perluasan field F. Elemen $\alpha \in E$ dikatakan **bersifat aljabar** (algebraic) atas F jika terdapat polinomial $f(x) \in F[x]$, $f(x) \neq 0$, sedemikian hingga $f(\alpha)=0$.

Teorema 5.1.3

Misalkan F field, E perluasan field F dan $a \in E$ bersifat aljabar atas F. Jika $p(x) \in F[x]$, $p(x) \neq 0$, adalah polinomial dengan derajat positip terendah sedemikian hingga $p(a)=0$, maka

1. p(x) irreducible atas F , dan
2. jika p(x) monik, maka p(x) tunggal.

Bukti

Perhatikan himpunan $I = \{f(x) \in F[x] \mid f(a)=0\}$. Karena $a \in E$ bersifat aljabar atas F, maka terdapat $f(x) \in F[x]$, $f(x) \neq 0$, sedemikian hingga $f(a)=0$. Jadi $I \neq \emptyset$.

Untuk setiap $g(x), h(x) \in I$, maka $g(x) \pm h(x) \in I$. Untuk setiap $k(x) \in F[x]$, maka $g(x)k(x) \in I$ dan $k(x)g(x) \in I$. Jadi I merupakan ideal di dalam F[x].

Misalkan $p(x)\in I$, $p(x)\neq 0$, adalah polinomial dengan derajat terendah. Dengan algoritma pembagian, untuk setiap $g(x)\in I$, terdapat $q(x),r(x)\in F[x]$ sedemikian hingga $g(x) = q(x)p(x)+r(x)$ dengan $r(x)=0$ atau $d(r(x)) < d(p(x))$. Karena $g(x)\in I$, maka $0 = g(a) = q(a)p(a)+r(a)$.

$$= q(a)\ 0\ +r(a)$$

$$= r(a).$$

Jadi $r(x)\in I$. Karena $p(x)$ berderajat terendah, maka haruslah $r(x)=0$. Sehingga untuk setiap $g(x)\in I$, $g(x)=q(x)p(x)$ untuk suatu $q(x)\in F[x]$. Jadi $I=(p(x))$.

Misalkan $p(x)=q(x)r(x)$ untuk suatu $q(x),r(x)\in F[x]$. Karena $q(x),r(x)$ faktor dari $p(x)$, maka $d(q(x)) \leq d(p(x))$ dan $d(r(x)) \leq d(p(x))$. Karena $q(a)r(a)=p(a)=0$ dan $q(a),r(a)\in E$, maka $q(a)=0$ atau $r(a)=0$. Misalkan $q(a)=0$, maka $q(x)\in I$. Mengingat pemilihan $p(x)$, maka $d(q(x))=d(p(x))$, sehingga $d(r(x))=0$ yaitu $r(x)\in F$. Dengan cara yang sama jika $r(a)=0$, maka $q(x)\in F$. Jadi $p(x)$ irreducible atas F.

Selanjutnya, misalkan $p(x)$ polinomial monik. Andaikan $q(x)$ juga polinomial monik dengan derajat positip terendah sedemikian hingga $q(a) = 0$. Maka $q(x) \in I$. Karena $p(x)$ mempunyai derajat positip terendah, maka $d(q(x)) = d(p(x))$. Misalkan $p(x) = a_o + a_1x +\ldots+ ex^n$ dan $q(x) = b_o + b_1x +\ldots+ ex^n$, maka

$$p(x)-q(x) = (a_o-b_o) + (a_1-b_1)x +\ldots+ (a_{n-1}-b_{n-1})x^{n-1}.$$

Karena $p(a)-q(a) = 0$, maka $p(x)-q(x) \in I$. Karena $d(\ p(x)-q(x)\ ) < d(p(x))$ dan karena pemilihan $p(x)$, maka

$p(x)-q(x) = 0$. Jadi $p(x) = q(x)$. Jadi jika $p(x)$ monik, maka $p(x)$ tunggal.

5.2 Homomorfisme Evaluasi

Misalkan E dan F field, dengan F subfield dari E. Teorema berikut menegaskan adanya homomorfisme yang sangat penting dari F[x] ke E.

Teorema 5.2.1

Misalkan F adalah subfield dari field E dan α elemen dari E. Maka pemetaan $\phi_\alpha : F[x] \longrightarrow E$, didefinisikan dengan

$$\phi_\alpha(a_o + a_1x + \ldots + a_nx^n) = a_o + a_1\alpha + \ldots + a_n\alpha^n$$

untuk setiap $a_o + a_1x + \ldots + a_nx^n \in F[x]$ adalah homomorfisme dari F[x] ke E. Selanjutnya $\phi_\alpha(x)=\alpha$, dan ϕ_α memetakan F ke F secara isomorfik sebagai pemetaan identitas, yaitu $\phi_\alpha(a)=a$, untuk $a \in F$. Homomorfisme ϕ_α tersebut disebut **evaluasi** pada α.

Bukti :

Pemetaan ϕ_α jelas well defined, karena untuk setiap $f(x) = a_o + a_1x + \ldots + a_nx^n$, dan $g(x) = b_o + b_1x + \ldots + b_mx^m$, bila $f(x)=g(x)$ yaitu

$$a_o + a_1x + \ldots + a_nx^n = b_o + b_1x + \ldots + b_mx^m,$$

maka

$$a_o + a_1\alpha + \ldots + a_n\alpha^n = b_o + b_1\alpha + \ldots + b_m\alpha^m,$$

yaitu

$$\phi_\alpha(a_o + a_1x + \ldots + a_nx^n) = \phi_\alpha(b_o + b_1x + \ldots + b_mx^m).$$

Selanjutnya

$$\phi_\alpha (f(x)+g(x)) = \phi_\alpha((a_o+b_o) + (a_1+b_1)x + \ldots + (a_n+b_n)x^n + b_{n+1}x^{n+1} + \ldots + b_m x^m) \text{ untuk } m>n.$$

$$= (a_o+b_o) + (a_1+b_1)\alpha + \ldots + (a_n+b_n)\alpha^n + b_{n+1}\alpha^{n+1} + \ldots + b_m\alpha^m$$

$$= (a_o + a_1\alpha + \ldots + a_n\alpha^n)+(b_o + b_1\alpha + \ldots + b_m\alpha^m)$$

$$= \phi_\alpha(f(x)) + \phi_\alpha(g(x)).$$

Dengan cara yang analog dapat dibuktikan untuk m=n dan m<n.

Demikian pula

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

$$= a_o b_o + (a_o b_1+a_1 b_o)\alpha + \ldots + a_n b_m \alpha^{n+m}$$

$$= (a_o + a_1\alpha + \ldots + a_n\alpha^n)(b_o + b_1\alpha + \ldots + b_m\alpha^m)$$

$$= \phi_\alpha(f(x))\ \phi_\alpha(g(x)).$$

Jadi ϕ_α homomorfisme.

Jika definisi dari ϕ_α diterapkan pada polinomial $a \in F[x]$, dengan $a \in F$, yaitu $\phi_\alpha(a)=a$. Jadi ϕ_α memetakan F ke F secara isomorfik sebagai pemetaan identitas. Dengan definisi ϕ_α diperoleh juga $\phi_\alpha(x) = \phi_\alpha(ex) = e\alpha = \alpha$. ∎

Teorema 5.2.2

Misalkan E adalah perluasan field F, dan $\alpha \in E$ bersifat aljabar atas F. Maka terdapat polinomial irreducible $p(x) \in F[x]$ sedemikian hingga $p(\alpha)=0$. Polinomial p(x) tersebut adalah tunggal tanpa memperhatikan faktor-faktor konstan di dalam F dan merupakan polinomial dengan derajat terendah ≥ 1 di dalam F[x] yang mempunyai α sebagai akar. Jika $f(\alpha)=0$ untuk $f(x) \in F[x]$, dengan $f(x) \neq 0$, maka p(x) merupakan faktor

dari f(x).

Bukti :

Misalkan ϕ_α adalah homomorfisme evaluasi dari F[x] ke E. Menurut teorema 4.1 kernel ϕ_α adalah ideal utama, yang dibentuk oleh suatu polinomial $p(x) \in F[x]$. Jadi $(p(x))$ terdiri dari semua polinomial dalam F[x] yang memunyai akar α. Jika $f(\alpha)=0$ untuk $f(x) \neq 0$, maka $f(x) \in (p(x))$, sehingga $p(x) | f(x)$. Kemudian, jelas bahwa p(x) adalah polinomial dengan derajat terendah ≥ 1 yang mempunyai akar α, dan polinomial lain yang mempunyai derajat yang sama dengan derajat p(x) pasti berbentuk a p(x) untuk $a \in F$. Menurut teorema 5.1.3, polinomial p(x) adalah irreducible. Polinomial p(x) tersebut dapat dipilih polinomial yang monik. Dan menurut teorema 5.1.3, jika p(x) monik, maka p(x) tunggal. ∎

Definisi 5.2.1

Misalkan E perluasan field dari field F, dan $\alpha \in E$ bersifat aljabar atas F. Polinomial monik p(x) di dalam teorema 5.2.2 disebut **polinomial irreducible untuk α atas F**, dan dilambangkan dengan irr(α,F). Yang disebut **derajat untuk α atas F**, dilambangkan dengan d(α,F), ialah derajat dari irr(α,F).

Contoh 5.2.1

Misalkan Q field bilangan rasional dan R field bilangan real. Bilangan $\sqrt{2} \in R$ bersifat aljabar atas Q dengan irr($\sqrt{2}$,Q)

$= x^2-2$ dan $d(\sqrt{2},Q)=2$.

5.3 Perluasan Sederhana Field

Teorema 5.3.1

Misalkan F field, E perluasan field F dan $\alpha \in E$ bersifat aljabar atas F. Misalkan ϕ_α adalah homomorfime evaluasi dari F[x] ke E. Jika $irr(\alpha,F) = p(x)$, maka $F[x]/(p(x)) \approx \phi_\alpha(F[x])$. Lagi pula $\phi_\alpha(F[x])$ merupakan subfield terkecil dari E yang memuat F dan α, yang akan dilambangkan dengan $F(\alpha)$.

Bukti:

Karena α bersifat aljabar atas F dengan $irr(\alpha,F) = p(x)$, maka menurut teorema 5.2.2 $\ker \phi_\alpha = (p(x))$. Karena ϕ_α merupakan homomorfisme dengan domain F[x], range $\phi_\alpha(F[x])$ dan $\ker \phi_\alpha = (p(x))$, maka dengan teorema fundamental homomorfisme ring diperoleh bahwa $F[x]/(p(x)) \approx \phi_\alpha(F[x])$.

Andaikan N sebarang subfield dari E yang memuat F dan α. Untuk setiap $b \in \phi_\alpha(F[x])$, maka terdapat $a_o+a_1x+\ldots+a_nx^n \in F[x]$ sedemikian hingga $b = \phi_\alpha(a_o+a_1x+\ldots+a_nx^n) = a_o+a_1\alpha+\ldots+a_n\alpha^n$. Karena $a_o, a_1, \ldots, a_n, \alpha$ di dalam N, maka $b \in N$. Sehingga $\phi_\alpha(F[x]) \subseteq N$. Jadi $\phi_\alpha(F[x])$ merupakan subfield terkecil dari E yang memuat F dan α.

Definisi 5.3.1

Misalkan F field dan E adalah perluasan dari field F. Field E disebut perluasan sederhana dari field F jika terdapat

$\alpha \in E$ sedemikian sehingga $E=F(\alpha)$.

Contoh 5.3.1

Misalkan R field bilangan real dan C field bilangan kompleks yang merupakan perluasan dari field R. Untuk bilangan imaginer $i \in C$, misalkan ϕ_i adalah homomorfisme evaluasi dari R[x] ke C. Untuk setiap $\phi_i(f(x)) \in R(i)$, di mana $f(x) \in R[x]$. Karena $irr(i,R) = 1+x^2$, maka dengan algoritma pembagian pada R[x], diperoleh $f(x) = (1+x^2)h(x) + a+bx$, untuk suatu $h(x)$ di dalam R[x]. Sehingga

$$\phi_i(f(x)) = \phi_i((1+x^2)h(x) + a + bx)$$
$$= a+bi.$$

Jadi $\phi_i(f(x))$ di dalam C.

Sebaliknya untuk setiap $a+bi \in C$, maka terdapat $a+bx \in R[x]$ sedemikian hingga $a+bi = \phi_i(a+bx)$ untuk suatu $a+bx \in R[x]$. Sehingga a+bi di dalam $\phi_i(R[x])=R(i)$.

Jadi $R(i)=C$. Jadi C merupakan perluasan sederhana field R.

Teorema 5.3.2

Misalkan E perluasan sederhana $F(\alpha)$ dari field F, α bersifat aljabar atas F, dan derajat $irr(\alpha,F) = n \geq 1$. Maka setiap $\beta \in E$ dapat dinyatakan secara tunggal sebagai $\beta = b_o + b_1\alpha + b_2\alpha^2 + \ldots + b_{n-1}\alpha^{n-1}$ untuk $b_o, b_1, b_2, \ldots, b_{n-1}$ di dalam F.

Bukti

Misalkan ϕ_α adalah homomorfisme evaluasi dari F[x] ke E. Maka setiap elemen dari

$$F(\alpha) = \phi_\alpha(F[x])$$

pasti berbentuk $\phi_\alpha(f(x)) = f(\alpha)$, untuk $f(x) \in F[x]$.

Misalkan

$$irr(\alpha,F) = p(x) = a_o + a_1x + \ldots + a_{n-1}x^{n-1} + x^n.$$

Maka $p(\alpha) = 0$, sehingga

$$\alpha^n = -a_o - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1}.$$

Elemen ini berada di dalam $F(\alpha)$, dan dapat digunakan untuk menyatakan setiap α^m untuk $m \geq n$ dalam pangkat-pangkat dari α yang kurang dari n.

Misalkan

$$\begin{aligned}\alpha^{n+1} = \alpha\,\alpha^n &= \alpha\,(-a_o - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1}) \\ &= -a_o\alpha - a_1\alpha^2 - \ldots - a_{n-1}\alpha^n \\ &= -a_o\alpha - a_1\alpha^2 - \ldots - a_{n-1}(-a_o - a_1\alpha - \ldots - a_{n-1}\alpha^{n-1}).\end{aligned}$$

Jadi jika $\beta \in F(\alpha)$, maka β berbentuk $\phi_\alpha(f(x)) = f(\alpha)$ yaitu $\beta = a_o + a_1\alpha + \ldots + a_m\alpha^m$ dengan $a_o, a_1, \ldots, a_m \in F$.

Karena setiap α^m, $m \geq n$ dapat dinyatakan dalam pangkat-pangkat dari α yang kurang dari n, maka β dapat dinyatakan dalam bentuk $b_o + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$.

Misal

$$\begin{aligned}\beta &= a_o + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} + a_n\alpha^n \\ &= a_o + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} + a_n(-a_o - a_1\alpha - \ldots \\ &\quad -a_{n-1}\alpha^{n-1}) \\ &= a_o + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} - a_oa_n - a_1a_n\alpha - \ldots - a_{n-1}a_n\alpha^{n-1} \\ &= (a_o - a_oa_n) + (a_1 - a_1a_n)\alpha + \ldots + (a_{n-1} - a_{n-1}a_n)\alpha^{n-1}.\end{aligned}$$

Jika $a_o - a_oa_n = b_o$, $a_1 - a_1a_n = b_1$, $\ldots$, $a_{n-1} - a_{n-1}a_n = b_{n-1}$, untuk suatu $b_i \in F$, maka $\beta = b_o + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}$.

Jika

$$b_o + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1} = b_o^* + b_1^*\alpha + \ldots + b_{n-1}^*\alpha^{n-1}$$

untuk $b_i^* \in F$, maka

$$h(x) = (b_o - b_o^*) + (b_1 - b_1^*)x + \ldots + (b_{n-1} - b_{n-1}^*)x^{n-1}$$

berada di dalam F[x], dan $h(\alpha)=0$. Karena $d(h(x)) < d(p(x))$ dan karena $p(x) = irr(\alpha,F)$ adalah polinomial dengan derajat terendah ≥ 1 dalam F[x] yang mempunyai akar α, maka haruslah $h(x)=0$. Jadi $b_i = b_i^*$. ∎

BAB VI

KESIMPULAN

Dari uraian-uraian pada bab-bab sebelumnya dapat disimpulkan hal-hal sebagai berikut :

1. Ring polinomial R[x] adalah ring yang elemen-elemennya adalah polinomial-polinomial dalam x atas suatu ring R. Ring polinomial R[x] merupakan daerah integral, jika R merupakan daerah integral. Faktorisasi dari polinomial bukan konstanta ke dalam polinomial-polinomial irreducible pada ring polinomial atas suatu field F merupakan faktorisasi yang tunggal tanpa memperhatikan urutan dan faktor-faktor unit dari F.
2. Jika D daerah faktorisasi tunggal, maka D[x] juga merupakan daerah faktorisasi tunggal.
3. Ring faktor polinomial F[x]/(p(x)) akan menjadi field bila dan hanya bila p(x) irreducible atas field F. Selanjutnya jika p(x) irreducible atas field F, maka terdapat subfield dari ring faktor polinomial F[x]/(p(x)) yaitu $\{(p(x)) + a \mid a \in F\}$ yang isomorfik dengan F.
4. Suatu polinomial yang bukan konstanta atas field F pasti mempunyai akar di dalam suatu perluasan dari F.

DAFTAR PUSTAKA

[1] Chaudhuri, N.P. (1983), *Abstract Algebra*, Tata McGraw-Hill Publishing Company Limmited, New Delhi.

[2] Durbin, John R. (1985), *Modern Algebra. An Introduction*, 2nd ed., John Wiley and Sons, New York.

[3] Fraleigh, John B. (1982), *A First Course in Abstract Algebra*, 3rd ed., Addison-Wesley Publishing Company, Inc.,Philippines.

[4] Herstein, I.N. (1964), *Topics in Algebra*, Blaisdell Publishing Company, A division of Ginn and Company, New york.

[5] Johnson, Richard E (1966), *University Algebra*, Prentice-Hall, Inc., Englewood Cliffs, New Jersey.

[6] McCoy, N.H. (1960), *Introduction to Modern Algebra*, Allyn and Bacon, Inc., Boston.

[7] Narayan, S. and Pal, S. (1979), *A Text Book of Modern Abstract Algebra*, Sixth Revised Ed., S. Chand & Company LTD, Ram Nagar, New Delhi.

[8] Whitelaw, Thomas A. (1978), *An Introduction to Abstract Algebra*, Blackie, Glasgow.