BAB II

DASAR TEORI

Dalam bab ini dijelaskan teori yang dapat menunjang materi pembahasan pada bab 3 diantaranya grup, ring, polinomial ring, lapangan perluasan

2.1 Grup

Definisi 2.1.1

Suatu himpunan tak kosong G dengan operasi biner $*$ pada G, dinotasikan $(G,*)$ disebut grup jika memenuhi :

1. Tertutup. Untuk setiap $a,b \in G$ berlaku $a*b \in G$.
2. Assosiatif. Untuk setiap $a,b,c \in G$ berlaku $(a*b)*c = a*(b*c)$.
3. Elemen satuan. Terdapat elemen $e \in G$ yang memenuhi $a*e = e*a = a$ untuk semua $a \in G$. e disebut elemen satuan.
4. Invers. Untuk setiap elemen $a \in G$ terdapat elemen $a^{-1} \in G$ yang memenuhi $a*a^{-1} = a^{-1}*a = e$. elemen a^{-1} disebut invers dari a.

Contoh.

1. Jika **Z** himpunan semua bilangan bulat, dengan operasi penjumlahan pada **Z**, maka (**Z**,+) merupakan grup.
2. Jika $M_2(\mathbf{R})$ merupakan himpunan semua matrik bilangan riil tak singular berorde 2×2, dengan operasi pergandaan maka $(M_2(\mathbf{R}), \times)$ merupakan grup.

Definisi 2.1.2

Grup $(G,*)$ dikatakan komutatif jika untuk setiap elemen $a,b \in G$ berlaku $a*b=b*a$.

Definisi 2.1.3

Suatu Grup $(G,*)$ dikatakan berhingga jika mempunyai elemen yang berhingga banyaknya dan dikatakan tak hingga jika mempunyai elemen yang tak hingga banyaknya.

Contoh.

1. Himpunan bilangan bulat $\mathbb{Z}_5$, dengan operasi penjumlahan merupakan grup berhingga.
2. Himpunan bilangan riil $\mathbb{R}$ dengan operasi penjumlahan merupakan grup takhingga

2.2. Subgrup

Definisi 2.2.1

H himpunan bagian dari grup $G=(G,*)$ membentuk subgrup dari G jika

1. H tidak kosong
2. $(H,*)$ membentuk suatu grup.

Definisi 2.2.2

Jika H adalah subgrup G, $a \in G$, maka $Ha=\{ha|h \in H\}$. Ha disebut koset kanan dari H dalam G dan $aH=\{ah|h \in H\}$. aH disebut koset kiri dari H dalam G

Definisi 2.2.3

Subgrup H dari G dikatakan normal jika $Hg = gH$ untuk semua g di G

Teorema 2.2.1

Untuk subgrup H dari grup G pernyataan berikut adalah ekuivalen :

1. Subgrup H normal di G.
2. $gHg^{-1} \subseteq H$ untuk semua $g \in G$
3. $gHg^{-1} = H$ untuk semua $g \in G$

Bukti.

(1⇒2) Ambil $h \in H$ dan $g \in G$, dapat dilihat $gh \in gH$. Karena H subgrup normal maka $gH = Hg$, maka $gh \in Hg$, berarti untuk $gh = h_1 g$ suatu $h_1 \in H$. Sehingga akan diperoleh $ghg^{-1} = h_1 \in H$. Hubungan tersebut berlaku untuk semua $h \in H$ dan $g \in G$. Jadi $gHg^{-1} \subseteq H$ untuk semua $g \in G$.

(2⇒1) Ambil $h \in H$ dan $g \in G$, menurut 2 . $gHg^{-1} \subseteq H$ dan $g^{-1}Hg \subseteq H$. Sehingga $ghg^{-1} \in H$ atau $g^{-1}hg = h'$ dengan $h' \in H$. Didapat $gh = h'g$ yang berarti $gh \in gH$ untuk semua $h \in H$ atau $gH \subseteq Hg$. Demikian juga $g^{-1}Hg \subseteq H$ atau $g^{-1}hg = h''$ dengan $h'' \in H$ diperoleh $hg = gh''$ yang berarti $hg \in gH$ untuk semua $h \in H$ atau $Hg \subseteq gH$. Dengan demikian $gH = Hg$ berlaku untuk semua $g \in G$. Jadi subgrup H normal di G.

(2⇒3) Ambil $h \in H$ dan $g \in G$. Karena $gHg^{-1} \subseteq H$ untuk semua $g \in G$ maka didapat $g^{-1}h(g^{-1})^{-1} = g^{-1}hg = h_0$, dengan $h_0 \in H$ atau $h = gh_0g^{-1}$. Jadi

$h \in gHg^{-1}$ untuk semua $h \in H$ atau $H \subseteq gHg^{-1}$. Dengan demikian $gHg^{-1} = H$ untuk semua $g \in G$.

(3⇒2). Implikasi ini jelas berlaku.

(1⇒3). Dari (1⇒2) diperoleh hubungan $gHg^{-1} \subseteq H$ untuk semua $g \in G$.

Selanjutnya dari (2⇒3) dapat ditunjukkan bahwa $gHg^{-1} \supseteq H$ sehingga berlaku $gHg^{-1} = H$ untuk semua $g \in G$.

(3⇒1) . Dari (3⇒2) ditunjukkan implikasi benar, yaitu $gHg^{-1} = H$ untuk semua $g \in G$ maka $gHg^{-1} \subseteq H$ untuk semua $g \in G$ kemudian dari (2⇒1) dapat ditunjukkan bahwa subgrup H normal di G.

2.3. Grup simetris

Definisi 2.3.1.

Suatu permutasi himpunan A adalah fungsi dari A ke A yang sekaligus satu-satu (*one to one*) dan pada (*onto*). Dengan kata lain permutasi untuk A adalah fungsi satu-satu dari A pada A

Definisi 2.3.2.

Diberikan A adalah himpunan berhingga $\{1,2,3,4,\ldots,n\}$

Grup semua permutasi untuk A disebut grup simetrik pada n huruf, dan ditunjukkan dengan notasi S_n.

S_n mempunyai $n!$ elemen, dengan $n! = n(n-1)\ldots3.2.1$

2.4. Ring

Definisi 2.4.1

Misalkan suatu himpunan $R \neq \varnothing$, dengan operasi penjumlahan + dan pergandaan •, pasangan $(R,+,\bullet)$ disebut ring jika memenuhi :

1. Terhadap operasi + merupakan grup komutatif
2. Terhadap • bersifat tertutup dan assosiatif
3. Bersifat distributif yaitu untuk setiap $a,b,c \in R$, berlaku $(a+b)c = ac + bc$ dan $c(a+b) = ca + cb$

Definisi 2.4.2.

Misalkan R suatu ring, maka R disebut ring komutatif jika berlaku $ab = ba$, $\forall a,b \in R$

Contoh.

1. Misalkan $\mathbb{Z}$ himpunan semua bilangan bulat, $\mathbb{Q}$ himpunan semua bilangan rasional, $\mathbb{R}$ himpunan semua bilangan riil dan $\mathbb{C}$ himpunan semua bilangan komplek, maka $(\mathbb{Z},+,\bullet)$, $(\mathbb{Q},+,\bullet)$, $(\mathbb{R},+,\bullet)$, $(\mathbb{C},+,\bullet)$ merupakan ring komutatif.
2. Himpunan semua Matrik bilangan riil 2×2 $M_2(\mathbb{R})$ dengan operasi penjumlahan dan perkalian matrik merupakan ring yang tidak komutatif.

Definisi 2.4.3

Ring yang mempunyai elemen satuan disebut ring dengan elemen satuan maka berlaku $ea = ae$, $\forall a \in R$, $a \neq 0$. Dan dikatakan ring yang mempunyai invers

pergandaan jika berlaku $\forall a \in R$, $a \neq 0$ terdapat $a^{-1} \in R$, sedemikian sehingga $aa^{-1} = 1 = a^{-1}a$, a^{-1} invers dari a.

Definisi 2.4.4

Ring R dengan elemen satuan dan setiap elemen tak nolnya mempunyai invers terhadap perkalian disebut ring pembagian (*division ring*).

Contoh.

1. Ring $(\mathbb{R},+,\bullet)$ mempunyai elemen satuan dan $\forall x \in \mathbb{R}$, $x \neq 0$, $\exists x^{-1} \in \mathbb{R}$, sehingga $x.x^{-1} = 1 = x^{-1}.x$, maka $(\mathbb{R},+,\bullet)$ adalah ring pembagian. Ring $(\mathbb{C},+,\bullet)$ dan $(\mathbb{Q},+,\bullet)$ juga merupakan ring pembagian.
2. Pada ring $(\mathbb{Z},+,\bullet)$, $\forall x \in \mathbb{Z}$, misalkan ambil $x = \pm 2$, x tidak mempunyai invers perkalian, sehingga $(\mathbb{Z},+,\bullet)$ bukan merupakan ring pembagian.

Definisi 2.4.5

Misalkan R adalah ring, elemen $a \in R$, $a \neq 0$ disebut pembagi nol jika terdapat $b \in R$, $b \neq 0$ sehingga $ab = 0$ atau $ba = 0$. Sehingga ring yang tidak mempunyai pembagi nol akan memenuhi

1. $a \neq 0$, $b \neq 0 \Rightarrow ab \neq 0$ atau
2. $ab = 0 \Rightarrow a = 0$ atau $b = 0$.

Definisi 2.4.6

Daerah integral adalah ring komutatif dengan elemen satuan dan tidak mempunyai pembagi nol.

Contoh.

1. Ring $(\mathbb{Z},+,\bullet)$, $(\mathbb{Q},+,\bullet)$, $(\mathbb{R},+,\bullet)$, dan $(\mathbb{C},+,\bullet)$ adalah daerah integral.
2. Ring $(\mathbb{Z}_n,+,\bullet)$ dengan n bilangan prima merupakan daerah integral.

Definisi 2.4.7

Lapangan (*field*) adalah ring pembagian yang komutatif atau ring komutatif dengan elemen satuan dan setiap elemen taknol mempunyai invers perkalian.

Contoh.

Ring $(\mathbb{Q},+,\bullet)$, $(\mathbb{R},+,\bullet)$, dan $(\mathbb{C},+,\bullet)$ dan $(\mathbb{Z}_n,+,\bullet)$ dengan n bilangan prima merupakan lapangan.

Teorema 2.4.1

Setiap lapangan adalah daerah integral.

Bukti.

Misalkan L adalah lapangan dan $a,b \in L$. Maka L adalah ring komutatif dengan elemen satuan. Selanjutnya akan dibuktikan L tidak mempunyai pembagi nol.

Misalkan $a \neq 0$, maka ada a^{-1} di L sehingga $aa^{-1} = e$

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

$\Rightarrow (a.a^{-1})b = a^{-1}.0$ (sifat assosiatif)

$\Rightarrow e.b = 0$

$\Rightarrow b = 0$

Jadi L tidak mempunyai pembagi nol, terbukti L daerah integral. ■

2.5. Ideal dan Ring Kuosien

Definisi 2.5.1

Misalkan $I \subseteq R$ dan $I \neq \emptyset$. I disebut ideal dari R jika memenuhi :

1. $\forall a,b \in I \Rightarrow a - b \in I$
2. $\forall a \in I$ dan $r \in R \Rightarrow ar \in I$ dan $ra \in I$

Definisi 2.5.2

Suatu ideal yang dibangun oleh satu elemen saja disebut ideal utama. Ideal utama yang dibangun oleh a ditulis $\langle a \rangle = \{ra | r \in R\}$

Suatu ring dengan setiap idealnya adalah ideal utama dinamakan daerah ideal utama.

Teorema 2.5.1

Misalkan I adalah ideal dari R. Maka himpunan koset penjumlahan $R/I = \{r + I = r \mid r \in R\}$ dengan operasi penjumlahan dan pergandaan yang didefinisikan dengan

$\overline{a} + \overline{b} = \overline{a+b}$

$\overline{a}.\overline{b} = \overline{a.b}$

membentuk suatu ring yang disebut ring kuosien R oleh I

Bukti

Akan ditunjukkan dahulu penjumlahan dan pergandaan diatas terdefinisi dengan baik. Misalkan $\overline{a} = \overline{a'}$ dan $\overline{b} = \overline{b'}$. Kita punya $a - a' \in I$ dan $b - b' \in I$ atau $a = a' + x$ dan $b = b' + y$ untuk $x,y \in I$ kita peroleh

$a + b = (a' + x)(b' + y) = (a' + b') + (x + y) = (a' + b') + m$

$ab = (a' + x)(b' + y) = a'b' + (a'y + b'x + xy) = a'b' + n$

untuk suatu $n,m \in I$. Dengan demikian $(a + b) - (a' + b') \in I$ dan $ab - a'b' \in I$, atau $\overline{a} + \overline{b} = \overline{a+b}$ dan $\overline{a}.\overline{b} = \overline{a.b}$. Jadi penjumlahan dan pergandaan terdefinisi dengan baik.

Selanjutnya akan ditunjukkan bahwa R/I merupakan suatu ring.

1. Terhadap penjumlahan
   a. Bersifat tertutup : diperoleh dari definisi.
   b. Bersifat assosiatif : $\forall \overline{a}, \overline{b}, \overline{c} \in R/I$ berlaku $\left(\overline{a} + \overline{b}\right) + \overline{c} = \overline{a+b} + \overline{c}$ = $\overline{a+b+c} = \overline{a} + \left(\overline{b+c}\right) = \overline{a} + \left(\overline{b} + \overline{c}\right)$
   c. Terdapat $\overline{0} \in R/I$ sehingga $\forall \overline{a} \in R/I$ berlaku $\overline{a} + \overline{0} = \overline{a+0}$ = $\overline{a+0} = \overline{a} + \overline{0} = \overline{a}$. Yang merupakan elemen netral dari R/I
   d. Untuk $\forall \overline{a} \in R/I$ terdapat $\overline{-a} \in R/I$ sehingga berlaku $\overline{a} + (\overline{-a}) = \overline{a + (-a)}$ = $\overline{a - a} = \overline{0}$. Elemen $\overline{-a} \in R/I$ dinamakan invers penjumlahan dari $\overline{a} \in R/I$
2. Terhadap pergandaan
   a. Tertutup pergandaan diperoleh dari definisi.
   b. Bersifat assosiatif : $\forall \overline{a}, \overline{b}, \overline{c} \in R/I$ berlaku $\left(\overline{a}.\overline{b}\right)\overline{c} = \overline{a.b}.\overline{c}$ = $\overline{a.b.c}$ = $\overline{a}.\left(\overline{b.c}\right) = \overline{a}.\left(\overline{b}.\overline{c}\right)$
3. Terhadap pergandaan dan penjumlahan secara bersama bersifat distributif

   $\forall \overline{a}, \overline{b}, \overline{c} \in R/I$ berlaku

$$(\overline{a}+\overline{b})\overline{c} = \overline{(a+b)c} = \overline{a.c+b.c} = \overline{a.c}+\overline{b.c}$$

$$\overline{a}(\overline{b}+\overline{c}) = \overline{a(b+c)} = \overline{a.b+a.c} = \overline{a.b}+\overline{a.c}$$

Jadi R/I adalah ring. ■

Definisi 2.5.3

Suatu ideal M dalam ring R dikatakan ideal maksimal jika untuk setiap ideal N di R dan berlaku $M \subseteq N \subseteq R$ maka $N = M$ atau N = R.

Teorema 2.5.2

Misalkan R suatu ring dengan elemen satuan dan M adalah suatu ideal di R, maka M ideal maksimal jika dan hanya jika R/M adalah lapangan.

Bukti.

Misalkan R ring komutatif dengan elemen satuan dan M ideal di R. Jelas bahwa R/M adalah komutatif. Misalkan M ideal maksimal akan ditunjukkan bahwa R/M adalah lapangan. Ambil sembarang elemen tak nol di R/M, misalkan $a + M$. Maka $a \notin M$. Sekarang dibentuk himpunan $I = \{ar + m \mid r \in R, m \in M\}$.

Jelas bahwa I tidak kosong karena R dan M tidak kosong. Ambil sembarang elemen $x,y \in I$, $x = ar_1 + m_1$ dan $y = ar_2 + m_2$ dengan $r_1,r_2 \in R$ dan $m_1,m_2 \in M$ maka

i. $x - y = a(r_1 - r_2) + (m_1 - m_2)$, karena $r_1 - r_2 \in R$ dan $m_1 - m_2 \in M$ maka $x - y \in I$

ii. ambil sembarang $r \in R$ maka $xr = rx = a(r_1r) + (m_1r)$ karena $r_1r \in R$ dan $m_1r \in M$, maka $xr = rx \in I$.

Jadi I adalah ideal di R

Ambil sembarang $m \in M$ maka m dapat ditulis $m = a0 + m$ dengan $0 \in R$ dan $m \in M$. Akibatnya $m \in I$. Ini memberikan $M \subseteq I$.

Selanjutnya ambil $ae + 0 = a \in I$, jelas bahwa $a \notin M$. Dengan demikian terdapat elemen di I yang bukan elemen M, jadi $I \supset M$. Karena M adalah ideal maksimal maka haruslah $I = R$. Dengan demikian elemen $e \in R$ dapat ditulis sebagai $e = ar + m$ untuk suatu $r \in R$ dan $m \in M$.

Maka $e + M = (ar + m) + M = ar + M = (a + M)(r + M)$. Ini berarti $r + M$ invers dari $a + M$. Dengan kata lain $a + M$ mempunyai invers. Sehingga setiap elemen taknol di R/M punya invers maka R/M suatu lapangan

Sebaliknya, misalkan R/M suatu lapangan dan misalkan I ideal di R sehingga $M \subset I \subseteq R$. karena $M \subset I$ maka terdapat $a \in I$ dan $a \notin M$.

Dengan demikian $a + M \in R/M$. Ambil sembarang $b \in R$, karena R/M suatu lapangan dan $a + M$ elemen taknol di R/M maka berlaku $(a + M)(x + M) = b + M$ atau $ax + aM + xM + M = ax + M = b + M$ sehingga $ax - b = m$, untuk suatu $m \in M$ atau $b = ax - m$. Perhatikan bahwa $ax \in I$ (I ideal) dan $m \in I$ ($M \subset I$). Sehingga $b \in I$. Karena b sembarang maka $R \subseteq I$. Jadi $I = R$ atau M ideal maksimal. ■

Definisi 2.5.4

Suatu ideal I dari ring R dikatakan ideal prim jika untuk setiap unsur a,b di R yang memenuhi $ab \in I$ maka $a \in I$ atau $b \in I$.

Teorema 2.5.3

Misalkan R suatu ring komutatif dan I ideal dalam R, maka R/I daerah integral jika dan hanya jika I ideal prim.

Bukti

Misalkan R/I daerah integral. Ambil elemen $a,b \in R$ yang memenuhi $ab \in I$. Kita punya $\overline{ab} = \overline{0}$ karena R/I daerah integral maka $\overline{a} = \overline{0}$ atau $\overline{b} = \overline{0}$. Dengan kata lain $a \in I$ atau $b \in I$. Ini memberikan bahwa I ideal prim.

Sebaliknya misalkan I ideal prim dan $\overline{c}, \overline{d} \in R/I$ memenuhi $\overline{cd} = \overline{0}$. Kita punya $\overline{cd} = \overline{0}$ atau $cd \in I$. Karena I ideal prim maka $c \in I$, atau $d \in I$. Dengan kata lain $\overline{c} = \overline{0}$ atau $\overline{d} = \overline{0}$ ini memberikan R/I suatu daerah integral. ■

2.6. Homomorfisma Ring

Definisi 2.6.1

Misalkan $(R,+,.)$ dan $(R',+,.)$ masing-masing merupakan ring dan pemetaan $\sigma : R \to R'$. Pemetaan $\sigma : R \to R'$ disebut homomorfisma ring dari R ke R' apabila memenuhi sifat-sifat untuk setiap $a,b \in R$ berlaku :

1. $\sigma(a+b) = \sigma(a) + \sigma(b)$
2. $\sigma(a.b) = \sigma(a).\sigma(b)$.

Definisi 2.6.2

Jika $\sigma : R \to R'$ suatu homomorfisma maka kernel dari σ ditulis $Ker(\sigma)$ adalah himpunan semua elemen a di R yang dipetakan ke $0'$, yaitu

$Ker(\sigma) = \{a \in R | \sigma(a) = 0'\}$

Definisi 2.6.3

Suatu homomorfisma $\sigma : R \to R'$ dikatakan isomorfisma jika σ merupakan pemetaan yang bersifat satu-satu dan pada.

Jika $\sigma : R \to R'$ suatu isomorfisma maka dikatakan R dan R' isomorfis dan ditulis $R \approx R'$

2.7. Ring Polinomial

Definisi 2.7.1

Diberikan ring R. $f(x)$ yang didefinisikan sebagai

$f(x) = a_0x^0 + a_1x^1 + \Lambda + a_nx^n + \mathrm{K} = \sum_{i=0}^{\infty} a_ix^i$ dengan $a_i \in R$ dan hampir semua $a_i = 0$ dan i = 1,2,... disebut polinomial dalam bentuk tak tentu (*indeterminate*) x dan elemen a_i di R disebut koefisien dari $f(x)$.

$R[x]$ adalah kumpulan semua polinomial dengan *indeterminate* x dan koefisien-koefisiennya dalam ring R. Jika R[x] tidak mempunyai elemen satuan 1 di R maka $x \notin R[x]$ tetapi jika R mempunyai unsur satuan 1 maka x dapat dinyatakan dengan $1.x$ dan $1.x \in R[x]$.

Untuk $i > 0$, $a_i \neq 0$ maka nilai terbesar i adalah pangkat atau derajat dari $f(x)$. Derajat $f(x)$ dinotasikan dengan *der*($f(x)$). Misalkan *der*($f(x)$) = n maka ditulis $f(x) = \sum_{i=0}^{n} a_ix^i$. Jika tidak dipenuhi $i > 0$ maka $f(x)$ berderajat nol yang disebut konstanta.

Definisi 2.7.2

Misalkan $f(x)=\sum_{i=0}^{n} a_i x^i$ dan $g(x)=\sum_{j=0}^{m} b_j x^j$ untuk $f(x)$ dan $g(x)$ di $R[x]$ didefinisikan penjumlahan dan perkalian polinomial adalah sebagai berikut

i. $f(x) = g(x) \Leftrightarrow \forall i \geq 0, a_i = b_i$

ii. Penjumlahan polinomial.

$$f(x)+g(x) = \sum_{i=0}^{n} a_i.x^i + \sum_{j=0}^{m} b_j.x^j = \sum_{k=0}^{r} (a_k + b_k).x^k$$

$$= \sum_{k=0}^{r} c_k.x^k,\ c_k = a_i + b_j,\ \ r = \max(n,m)$$

iii. Perkalian polinomial.

$$f(x).g(x) = \sum_{i=0}^{n} a_i.x^i . \sum_{j=0}^{m} b_j.x^j = \sum_{k=0}^{n+m} (\sum_{r=0}^{k} a_r b_{k-r}).x^k$$

$$= \sum_{k=0}^{n+m} (\sum_{i+j=k} a_i b_j).x^k = \sum_{k=0}^{n+m} d_k x^k$$

dengan $d_k = \sum_{r=0}^{k} a_r b_{k-r} = \sum_{i+j=k} a_i b_j$.

Teorema 2.7.1

Dengan aturan penjumlahan dan perkalian polinomial seperti definisi diatas, himpunan $R[x]$ merupakan ring komutatif dengan elemen satuan.

Bukti.

Misalkan $f(x)=\sum_{i=0}^{n} a_i x^i$, $g(x)=\sum_{j=0}^{m} b_j x^j$ dan $h(x)=\sum_{k=0}^{r} c_k x^k$

adalah polinomial di $R[x]$. Dari definisi 2.7.2 penjumlahan dan pergandaan polinomial di $R[x]$ adalah polinomial di $R[x]$, sehingga $R[x]$ tertutup untuk operasi penjumlahan dan perkalian polinomial. Selanjutnya akan ditunjukkan $R[x]$ mempunyai sifat :

1. Terhadap operasi penjumlahan merupakan grup komutatif.
   a. Sifat tertutup ditunjukkan oleh definisi
   b. Bersifat assosiatif.

$$[f(x)+g(x)]+h(x) = (\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j) + \sum_{k=0}^{r} c_k x^k$$

$$= \sum_{i=0}^{s} (a_i + b_i) x^i + \sum_{k=0}^{r} c_k x^k, \quad s = \max(n,m)$$

$$= \sum_{i=0}^{t} ((a_i + b_i) + c_i) x^i, t = \max(s,r)$$

$$= \sum_{i=0}^{u} (a_i + (b_i + c_i)) x^i, u = \max(n,m,r)$$

$$= \sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{v} (b_j + c_j) x^j, v = \max(m,r)$$

$$= \sum_{i=0}^{n} a_i x^i + (\sum_{j=0}^{m} b_j x^j + \sum_{k=0}^{r} c_k x^k)$$

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

   c. Ada elemen identitas terhadap penjumlahan yaitu $e(x) = \sum_{i=0}^{n} 0.x^i$, sehingga untuk $f(x)$ di $R[x]$ berlaku :

$$f(x)+e(x) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} 0.x^i = \sum_{i=0}^{n} (a_i + 0)x^i$$

$$= \sum_{i=0}^{n} a_i x^i = f(x)$$

$$e(x)+f(x) = \sum_{i=0}^{n} 0.x^i + \sum_{i=0}^{n} a_i.x^i = \sum_{i=0}^{n} (0 + a_i)x^i = f(x)$$

d. Untuk semua $f(x)$ di $R[x]$ mempunyai invers penjumlahan yaitu

$-(f(x)) = \sum_{i=0}^{n} (-a_i)x^i$ sehingga dapat ditunjukkan

$$f(x)+(-f(x)) = \sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} (-a_i)x^i$$

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

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

e. Penjumlahan bersifat komutatif

$$f(x)+g(x) = \sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j = \sum_{k=0}^{r} (a_k + b_k)x^k$$

$$= \sum_{k=0}^{r} (b_k + a_k)x^k, r = \max(n,m) = \max(m,n)$$

$$= \sum_{j=0}^{m} b_j x^j + \sum_{i=0}^{n} a_i x^i = g(x) + f(x).$$

2. Terhadap pergandaan

a. Bersifat assosiatif

$$f(x)[g(x)h(x)] = \sum_{i=0}^{n} a_i x^i (\sum_{j=0}^{m} b_j x^j . \sum_{k=0}^{r} c_k x_k)$$

$$= \sum_{i=0}^{n} a_i x^i \sum_{p=0}^{m+r} (\sum_{j+k=p} b_j c_k) x^p$$

misalkan $d_p = \sum_{j+k=p} b_j c_k$

$$f(x)[g(x)h(x)] = \sum_{q=0}^{n+(m+r)} (\sum_{i+p=q} a_i d_p) x^q$$

$$= \sum_{q=0}^{n+m+r} (\sum_{i+p=q} a_i (\sum_{j+k=p} b_j c_k)) x^q$$

$$= \sum_{q=0}^{n+m+r} (\sum_{i+j+k=q} a_i b_j c_k) x^q$$

$$= \sum_{q=0}^{(n+m)+r} (\sum_{p+k=q} (\sum_{i+j=p} a_i b_j) c_k) x^q$$

$$= \sum_{p=0}^{n+m} (\sum_{i+j=p} a_i b_j) x^p . \sum_{k=0}^{r} c_k x^k$$

$$= (\sum_{i=0}^{n} a_i x^i . \sum_{j=0}^{m} b_j x^j) . \sum_{k=0}^{r} a_k x^k$$

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

b. Bersifat komutatif : $f(x)g(x) = \sum_{p=0}^{n+m} (\sum_{i+j=p} a_i b_j) x^p = \sum_{p=0}^{n+m} (\sum_{i+j=p} b_i a_j) x^p = g(x)f(x)$

c. Terdapat elemen satuan yaitu $1 = 1x^0$, karena

$$f(x).1x^0 = \sum_{i=1}^{n} (a_i.1) x^i = \sum_{i=1}^{n} (1.a_i) x^i = 1.f(x) = f(x)$$

3. Bersifat distributif terhadap pergandaan dan penjumlahan

$$f(x)[g(x)+h(x)]=\sum_{i=0}^{n}a_ix^i(\sum_{j=0}^{m}b_jx^j+\sum_{k=0}^{r}c_kx^k)$$

$$=\sum_{i=0}^{n}a_ix^i.\sum_{p=0}^{s}(b_p+c_p)x^p, s=\max(m,r)$$

$$f(x)[g(x)+h(x)]=\sum_{q=0}^{n+s}(\sum_{i+p=q}a_i(b_p+c_p))x^q=\sum_{q=0}^{n+s}(\sum_{i+p=q}(a_ib_p+a_ic_p))x^q$$

$$=\sum_{q=0}^{\max(n+m,n+r)}(\sum_{i+p=q}a_ib_p+\sum_{i+p=q}a_ic_p)x^q$$

$$=\sum_{q=0}^{n+m}(\sum_{i+p=q}a_ib_p)x^q+\sum_{q=0}^{n+r}(\sum_{i+p=q}a_ic_p)x^q$$

$$=\sum_{i=0}^{n}a_ix^i.\sum_{j=0}^{m}b_jx^j+\sum_{i=0}^{n}a_ix^i.\sum_{k=0}^{r}c_kx^k$$

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

dengan cara yang sama dapat ditunjukkan bahwa $[f(x)+g(x)]h(x)=f(x)h(x)+g(x)h(x)$ terbukti bahwa $R[x]$ ring komutatif dengan elemen satuan.■

Teorema 2.7.2

Misalkan $f(x),g(x) \in F[x]$ dan $f(x) \neq 0$, maka terdapat dengan tunggal polinomial $q(x)$ dan $r(x)$ sehingga berlaku $g(x) = f(x)q(x) + r(x)$, dengan $r(x) = 0$ atau $der(r(x)) < der(f(x))$

Bukti

Jika $g(x) = 0$, pilih $q(x) = 0$ maka $r(x) = g(x)$. Maka kita punyai

$g(x) = f(x)q(x) + r(x)$, dengan $r(x) = 0$.

Dalam hal $g(x) \neq 0$, misalkan $der(g(x)) = m$ dan $der(f(x)) = n$, akan terdapat dua kemungkinan :

1. $der\,(g(x)) < der(f(x))$

   Pilih $q(x) = 0$ dan $r(x) = g(x)$ maka akan diperoleh $g(x) = f(x)q(x) + r(x)$ dengan $der(r(x) < der(f(x))$.

2. $der(g(x)) \geq der(f(x))$

   Pembuktian dilakukan dengan induksi matematika.

   Misalkan $g(x) = b_0 + b_1x + ... + b_mx^m$ dan $f(x) = a_0 + a_1x + ... + a_mx^m$.

   Dalam hal $m = n$ pilih $q(x) = b_ma_n^{-1}$ dan $r(x) = g(x) - b_ma_n^{-1} f(x)$.

   Diperoleh $g(x) = f(x)q(x) + r(x)$ dengan $\text{der}(r(x)) < n\text{-}1 < \text{der}(f(x))$. Jadi sifat berlaku, selanjutnya, misalkan sifat berlaku untuk $m < n + k$ dengan $k > 0$.

   Akan dibuktikan berlaku juga untuk $m = n + (k+1)$.

   Pandang polinomial $g'(x) = g(x) - b_ma_n^{-1}x^{k+1}f(x)$, diperoleh $der(g'(x)) < n + k$.

   Menurut pemisalan induksi terdapat $q'(x), r(x) \in F[x]$ yang memenuhi $g'(x) = q'(x)f(x) + r(x)$ dengan $r(x) = 0$ atau $der(r(x)) < der(f(x))$.

   Selanjutnya kita punyai

   $$g(x) = g'(x) + b_ma_n^{-1}x^{k+1}f(x) = (q'(x)f(x) + r(x)) + b_ma_n^{-1}x^{k+1}f(x)$$

   $$= (q'(x) + b_ma_n^{-1}x^{k+1})f(x) + r(x) = q(x)f(x) + r(x)$$

   dengan $q(x) = q'(x) + b_ma_n^{-1}x^{k+1}$ dan $r(x) = 0$ atau $der(r(x)) < der(f(x))$.

   Untuk membuktikan ketunggalannnya,

   Misalkan $g(x) = q_1(x)f(x) + r_1(x) = q_2(x)f(x) + r_2(x)$ dengan $q_1(x) \neq q_2(x)$ dan $r_1(x) \neq r_2(x)$. Maka $q_1(x) - q_2(x) \neq 0$ *dan* $r_1(x) - r_2(x) \neq 0$.

   Misalkan $der(r_1(x) - r_2(x)) = s$, jelas bahwa $s < n = der(f(x))$ .....(1)

Selanjutnya dari hubungan $q_1(x)f(x) + r_1(x) = q_2(x)f(x) + r_2(x)$ diperoleh $0 = (q_1(x) - q_2(x))f(x) + (r_1(x) - r_2(x))$ atau $r_1(x) - r_2(x) = (q_1(x) - q_2(x))f(x)$. Akibatnya $der(r_1(x) - r_2(x)) = der(q_1(x) - q_2(x)) + der(f(x) \geq n$. Jadi bertentangan dengan (1). Jadu haruslah $q_1(x) = q_2(x)$ *dan* $r_1(x) = r_2(x)$. ■

Definisi 2.7.3

Misalkan R adalah ring komutatif dengan elemen satuan. Polinomial bukan konstanta $f(x)$ di $R[x]$ disebut tak teruraikan (*irreducible*) di $R[x]$ jika $f(x)$ tidak dapat dinyatakan sebagai perkalian polinomial $g(x)h(x)$, dengan $der(g(x)) < der(f(x))$ dan $der(h(x)) < der(f(x))$ dan $g(x), h(x)$ bukan polinomial satuan di $R[x]$.

Untuk menentukan suatu polinomial teruraikan atau tak teruraikan ada beberapa cara yang digunakan salah satunya adalah kriteria Eisentein dengan teorema berikut

Teorema 2.7.4 (Kriteria *Eisentein*)

Misalkan F adalah lapangan. Jika $f(x) = \sum_{i=0}^{n} a_i x^i$ adalah polinomial berderajat $n \geq 1$ di $F[x]$, terdapat bilangan prima p, dengan p tidak membagi a_n, p membagi a_i untuk semua $i < n$, dan p^2 tidak membagi a_0. maka $f(x)$ tak teruraikan di $F[x]$

Bukti.

Andaikan $f(x)$ teruraikan, misalkan $f(x) = g(x)h(x)$ dengan $g(x) = \sum_{j=0}^{m} b_j x^j$

dan $h(x) = \sum_{k=0}^{r} c_k x^k$ di $F(x)$, $m, r \geq 1$ dan $b_m c_r \neq 0$.

Karena $a_0 = b_0 c_0$ dan p membagi a_0, maka p membagi salah satu b_0 atau c_0. dari p^2 tidak membagi a_0 maka p tidak membagi keduanya yaitu b_0 dan c_0, katakanlah p tidak membagi b_0 dan p membagi c_0. karena $a_n = b_m c_r$ dan p tidak membagi a_n maka p tidak membagi c_r. misalkan s adalah bilangan bulat terkecil sehingga p tidak membagi c_s. maka $a_s = b_0 c_s + b_1 c_{s-1} + \Lambda + b_s c_0$, karena p tidak membagi c_s dan b_0 maka p tidak membagi $c_s b_0$. Dipihak lain p membagi $b_1 c_{s-1}$, p membagi $b_2 c_{s-2}$ dan seterusnya sampai p membagi $b_s c_0$. Maka p tidak membagi a_s, hal ini kontradiksi dengan p membagi a_i, untuk $i<n$. Sehingga $f(x)$ takteruraikan di $F[x]$.■

Teorema 2.7.5

Misalkan $f(x) \in F[x]$ merupakan polinomial yang berderajat > 1. Jika $f(a) = 0$ untuk $a \in F$ maka $f(x)$ teruraikan di F

Bukti.

$f(x)$ dapat ditulis $f(x) = (x-a)q(x) + r$, dengan $r \in F$. Selanjutnya $0 = f(a) = r$, jadi $f(x) = (x-a)q(x)$, karena f(x) mempunyai derajat >1 maka $f(x)$ teruraikan di F. ■

Definisi 2.7.4

Suatu polinomial $f(x) = a_0 + a_1 x^1 + \Lambda + a_n x^n$ pada lapangan F adalah monic jika $a_n = 1$.

2.8. Ruang Vektor

Definisi 2.8.1

Ruang vektor V atas lapangan F adalah

I. Sistem $V = (V,+)$

1. $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$ untuk semua $\boldsymbol{u},\boldsymbol{v} \in V$
2. $(\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w} = \boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w})$ untuk semua elemen $\boldsymbol{u},\boldsymbol{v},\boldsymbol{w} \in V$
3. Terdapat elemen $\mathbf{0} \in V$ dengan sifat $\boldsymbol{v} + 0 = \boldsymbol{v}$ untuk semua $\boldsymbol{v} \in V$
4. Untuk setiap $\boldsymbol{v} \in V$ terdapat $-\boldsymbol{v} \in V$ yang memenuhi $\boldsymbol{v} + (-\boldsymbol{v}) = \mathbf{0}$

II. Pemetaan $F \times V \rightarrow V$ dengan fungsi pemetaan $(a,\boldsymbol{v}) \rightarrow a\boldsymbol{v}$

untuk semua $(a,\boldsymbol{v}) \in F \times V$, dan untuk semua $a,b \in F$ dan $\boldsymbol{v},\boldsymbol{w} \in V$ berlaku :

1. $a(\boldsymbol{v} + \boldsymbol{w}) = a\,\boldsymbol{v} + a\,\boldsymbol{w}$.
2. $(a + b)\,\boldsymbol{v} = a\boldsymbol{v} + b\boldsymbol{v}$
3. $(ab)\boldsymbol{v} = a(b\boldsymbol{v}) = b(a\boldsymbol{v})$
4. $1\boldsymbol{v} = \boldsymbol{v}$

Definisi 2.8.2.

Misalkan X subhimpunan ruang vektor V, dengan $V, X \neq \varnothing$.

1. Vektor $\boldsymbol{v} \in V$ disebut kombinasi linier dari X jika untuk setiap $\boldsymbol{x} \in X$ terdapat $a_x \in F$, yang memenuhi $\boldsymbol{v} = \sum_{x \in X} a_x \boldsymbol{x}$.
2. Subhimpunan X dikatakan bebas linier jika kombinasi linier $\sum_{x \in X} a_x \boldsymbol{x} = 0$, hanya dipenuhi oleh $a_x = 0$ untuk semua $\boldsymbol{x} \in X$.

3. Subhimpunan X dikatakan bergantung linier jika X tidak bebas linier, artinya untuk setiap $x \in X$ terdapat $a_x \in F$ yang tidak semuanya 0 yang memenuhi $\sum_{x \in X} a_x x = 0$.
4. Subhimpunan X dikatakan membangun V jika setiap vektor di V kombinasi linier dari X.
5. Subhimpunan X disebut basis ruang V jika setiap vektor di V kombinasi linier dari X secara tunggal, artinya setiap vektor $v \in V$ kombinasi linier dari X, jika $v = \sum_{x \in X} a_x x = \sum_{x \in X} b_x x$, maka $a_x = b_x$, untuk semua $x \in X$.

Definisi 2.8.3.

Misalkan V ruang vektor atas F, maka yang dimaksud dengan dimensi V atas F ditulis $dim_F(V)$ adalah banyaknya elemen dalam basis V atas F.

2.9. Perluasan Lapangan

Definisi 2.9.1

Jika F adalah sublapangan dari lapangan E, maka E dikatakan sebagai perluasan dari lapangan F.

Definisi 2.9.2.

Misalkan E adalah perluasan dari F. Maka dimensi dari E yang dianggap sebagai ruang vektor atas F adalah derajat E atas F. Derajat E atas F ditulis $[E:F]$

Definisi 2.9.3

Jika $[E:F]<\infty$, maka E dikatakan peluasan berhingga dari F, sebaliknya E dikatakan perluasan takhingga dari F

Teorema 2.9.1

Misalkan F, E, K lapangan dengan $F \subseteq E \subseteq K$. Jika $[K:E]<\infty$ dan $[E:F]<\infty$ maka

(i) $[K:F]<\infty$

(ii) $[K:F] = [K:E][E:F]$

Bukti

Misalkan $\{v_1,v_2,....,v_m\}$ dengan $m = [K:E]$ adalah basis dari K atas E, dan misalkan $\{w_1,w_2,....,w_n\}$ dengan $n = [E:F]$ adalah basis dari E atas F. Jika $u \in K$, maka

$$u = \sum_{i=1}^{m} a_i v_i \text{ , dengan } a_i \in E \qquad .....(1)$$

karena $a_i \in E$ maka

$$a_i = \sum_{j=1}^{n} b_{ij} w_j \text{ , dengan } b_{ij} \in F \qquad .....(2)$$

substitusi (2) ke (1) maka didapat

$$u = \sum_{i=i}^{m}\sum_{j=1}^{n} b_{ij} v_i w_j \text{ , dengan } b_{ij} \in F$$

hal tersebut menunjukkan bahwa $[K:F]<\infty$

untuk membuktikan (2) akan ditunjukkan $v_i w_j$ bebas linier atas F. Misalkan dipunyai persamaan

$$\sum_{i=i}^{m}\sum_{j=1}^{n} c_{ij} v_i w_j = 0 \text{ dengan } c_{ij} \in F$$

persamaan diatas dapat ditulis kembali sebagai

$$\sum_{i=1}^{m} \lambda_i v_i = 0 \text{ dengan } \lambda_i = \sum_{j=1}^{n} c_{ij} w_j \in E, i = 1,2,...,m$$

karena v_i adalah bebas linier atas E, persamaan terakhir memberikan

$\lambda_i = 0$, dengan $i = 1,2,...,m$

$$\sum_{i=1}^{n} c_{ij} w_j = 0 \text{, dengan } i = 1,2,...,m$$

karena $c_{ij} \in F$ dan v_i bebas linier maka w_j bebas linier atas F maka $c_{ij} = 0$, untuk $i = 1,...,m$ dan $j = 1,...,n$

yang menunjukkan $v_i w_j$, merupakan basis dari K atas F. Sehingga diperoleh dimensi dari K atas F adalah mn atau $[K:F] = [K:E][E:F]$ ■

Akibat 2.9.1

Dari teorema diatas jika F_i lapangan dengan $i = 1,...,r$ dan F_{i+1} adalah perluasan berhingga dari F_i maka F_r perluasan berhingga dan berlaku

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

2.10. Perluasan Aljabar

Definisi 2.10.1

Diberikan E dan F lapangan, $\alpha \in E$ disebut aljabar atas F dengan $F \subset E$, jika terdapat suatu $f(x) \neq 0 \in F[x]$ sehingga $f(\alpha) = 0$, sebaliknya jika α bukan aljabar atas E disebut elemen transenden

Contoh.

1. $\mathbb{Q} \subseteq \mathbb{C}$, maka $\alpha = \sqrt{2}$ adalah elemen aljabar atas $\mathbb{Q}$ dalam $\mathbb{C}$ sebab terdapat $f(x) = x^2 - 2 \in \mathbb{Q}(x)$ sedemikian sehingga $f(\alpha) = 0$.
2. $\alpha = \pi$ adalah transenden atas $\mathbb{Q}$, karena yang memenuhi $f(\pi) = 0$ hanyalah $f(x) = x - \pi$, padahal $f(x) = x - \pi \notin \mathbb{Q}(x)$.

Definisi 2.10.2

E adalah perluasan lapangan F, E merupakan perluasan aljabar jika setiap elemen dari E adalah aljabar atas F.

Teorema 2.10.1

Misalkan E adalah lapangan perluasan dari F, $\alpha \in E$ adalah aljabar atas F, dan $f(x) \in F[x]$ adalah polinomial dengan derajat terkecil sedemikian sehingga $f(\alpha) = 0$ maka :

1. $f(x)$ takteruraikan atas F.
2. Jika $g(x) \in F[x]$ sedemikian sehingga $g(\alpha) = 0$, maka $f(x) | g(x)$
3. Terdapat dengan tunggal polinomial monic $f(x) \in F[x]$ dengan derajat terkecil yang memenuhi $f(\alpha) = 0$

Bukti.

1. Andaikan $f(x)$ teruraikan, maka $f(x) = f_1(x)f_2(x)$, untuk suatu $f_1(x), f_2(x) \in F[x]$ dengan $der(f_1(x)) < der(f(x))$ dan $der(f_2(x)) < der(f(x))$. Karena $f(\alpha) = 0$ maka $f_1(x).f_2(x) = 0$. Didapat $f_1(\alpha) = 0$ atau $f_2(\alpha) = 0$. Sehingga α memenuhi suatu

polinomial yang berderajat lebih kecil dari $f(x)$. Hal ini bertentangan dengan $f(x)$ berderajat terkecil. Jadi $f(x)$ takteruraikan atas F.

2. Misalkan $g(x) \in F[x]$ sedemikian sehingga $g(\alpha) = 0$, Dengan algoritma pembagian dapat dibentuk $g(x) = f(x)q(x) + r(x)$, untuk suatu $q(x), r(x) \in F[x]$ dengan $r(x) = 0$ atau $der(r(x) < der(f(x))$. Selanjutnya karena $g(\alpha)=0$ maka $f(\alpha)q(\alpha) + r(\alpha) = 0$, dan mengingat $f(\alpha) = 0$ diperoleh $r(\alpha) = 0$. Jadi kita punyai $r(x) \in F[x]$, dengan $der(r(x)) < der(f(x))$. Karena $f(x)$ merupakan polinomial derajat terkecil yang memenuhi $f(\alpha) = 0$, maka haruslah $r(x)=0$, dan kita punya $g(x) = f(x)q(x)$. Dengan kata lain $f(x)|g(x)$.
3. Misalkan $f(x)$ polinomial monic dengan derajat terkecil yang memenuhi $f(\alpha) = 0$ dan misalkan $g(x)$ juga polinomial monic yang memenuhi $g(\alpha) = 0$. Akan ditunjukkan bahwa $f(x) = g(x)$. Menurut (2) diperoleh $f(x)|g(x)$ selanjutnya dengan membalik argumen diatas didapatkan $g(x)|f(x)$, akibatnya $f(x) = g(x)$. Hal ini menunjukkan bahwa $f(x)$ tunggal. ■

Lema 2.10.1

Jika F adalah sub lapangan dari K dan $\alpha \in K$ adalah aljabar atas F, dan $p(x) \in F[x]$ adalah polinomial minimal dari α berderajat n maka $[K:F] = n$

Bukti

Misalkan $p(x) \in F[x]$ polinomial minimal dari α, maka $f(x)$ adalah polinomial derajat terkecil yang memenuhi $f(\alpha) = 0$

Misalkan ambil sembarang $f(\alpha) \in F[\alpha]$ maka $f(x) \in F[x]$.

$f(x)$ dapat ditulis sebagai $f(x) = q(x)\, p(x) + r(x)$, untuk $q(x), r(x) \in F[x]$ dengan $der(r(x)) = 0$ *atau* $der(r(x)) < der(f(x))$

Karena $p(\alpha) = 0$ sehingga $f(\alpha) = r(\alpha)$.

Tulis $r(x) = a_0 + a_1x + \ldots + a_{n-1}x^{n-1}$ dengan $a_0,\ldots,a_{n-1} \in F$.

Dan $r(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$.

Sehingga $f(\alpha) = r(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$

Jadi $\{1, \alpha, \ldots \alpha^{n-1}\}$ membangun K. Andaikan $\{1, \alpha, \ldots \alpha^{n-1}\}$ bergantung linier maka terdapat $a_0,\ldots,a_{n-1} \in F$ yang tidak semuanya nol yang memenuhi $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = 0$, tulis $f(\alpha) = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = 0$

Jadi $f(\alpha) \in F[\alpha]$ dan $f(x) \in F[x]$. menurut teorema 2.10.1 $p(x)|f(x)$ tidak mungkin karena $der(f(x)) < der(p(x)$, jadi haruslah $\{1, \alpha, \ldots \alpha^{n-1}\}$ bebas linier dengan demikian $\{1, \alpha, \ldots \alpha^{n-1}\}$ adalah basis atas F dan $[K:F] = n$

Teorema 2.10.2

Setiap perluasan berhingga merupakan perluasan aljabar.

Bukti.

Misalkan $F(\alpha)$ adalah perluasan berhingga atas F maka akan dtunjukkan bahwa α adalah aljabar atas F. Misalkan $[F(\alpha):F] = n$ dan $\{1,\alpha,\ldots,\alpha^{n-1}\}$ adalah basis dari $F(\alpha)$ atas F maka $\{1,\alpha,\ldots,\alpha^n\}$ bergantung linier. Jadi terdapat $a_0,a_1,\ldots,a_n \in F$ yang tidak semuanya nol yang memenuhi $a_0 + a_1\alpha + \ldots + a\alpha^n = 0$.

Tulis $g(\alpha) = a_0 + a_1\alpha + \ldots + a\alpha^n = 0$ maka $g(x) \in F[x]$ polinomial yang memenuhi $g(\alpha) = 0$. Jadi α adalah aljabar atas F dan $F(\alpha)$ merupakan perluasan aljabar atas F. ■

Definisi 2.10.3

Suatu perluasan E dari F dikatakan dibangun secara berhingga jika terdapat jumlah berhingga dari elemen $a_1,a_2,\ldots,a_r \in E$ sedemikian sehingga subfield terkecil dari E memuat F dan $\{a_1,a_2,\ldots,a_r\}$ adalah E sendiri. Dapat ditulis $E = F(a_1, a_2,\ldots,a_r)$.

Teorema 2.10.3

Misalkan $E = F(a_1,a_2,\ldots,a_r)$ adalah perluasan yang dibangun secara berhingga dari F sedemikian sehingga setiap a_i, dengan $i = 1,2,\ldots,r$ adalah aljabar atas F. Maka E berhingga atas F dan karenanya merupakan perluasan aljabar atas F.

Bukti

Himpunan $E_i = F(a_1,a_2\ldots,a_i)$, $(1 \leq i \leq n)$. Setiap elemen di E adalah aljabar atas F maka Juga aljabar atas sembarang fielf K sedemikian sehingga $E \supset K \supset F$. Oleh karena itu setiap a_i adalah aljabar atas E_{i-1}, $i = 1,2,\ldots,r$ dengan $E_0 = F$.

Juga $E_i = E_{i-1}(a_i)$. Menurut teorema 2.9.1 $[E_i:E_{i-1}]$ adalah berhingga katakanlah n_i.

Menurut akibat 2.9.1

$[E:F] = [E:E_{r-1}]\,[E_{r-1}:E_{r-2}]\ldots\,[E_1:F]$

sehingga $[E:F] = n_r n_{r-1}\ldots n_1$, sehingga E adalah perluasan berhingga dari F dan juga perluasan aljabar atas F. ■

Definisi 2.10.4

Misalkan K dan L adalah lapangan perluasan dari F. Maka suatu homomorfisma yang satu-satu $\sigma: K \rightarrow L$ sedemikian sehingga $\sigma(a) = a$ untuk semua $a \in F$ dikatakan sebagai F-homomorfisma dari K ke L atau embedding dari K dalam L atas F

Definisi 2.10.5

Suatu lapangan K adalah tertutup secara aljabar jika setiap polinomial tak konstan $f(x)$ di F[x] memiliki akar di K

Jelas bahwa lapangan bilangan komplek adalah tertutup secara aljabar, sedangkan lapangan bilangan rasional dan lapangan bilangan nyata tidak tertutup secara aljabar.

Teorema 2.10.5

Lapangan F tertutup secara aljabar jika dan jika setiap polinomial tak konstan di $F[x]$ dapat difaktorkan ke dalam faktor-faktor linier.

Bukti.

$\Rightarrow$ Misalkan $f(x)$ polinomial tak kostan di $F[x]$. Karena F tertutup secara aljabar maka terdapat $a \in F$ sedemikian sehingga a akar dari $f(x)$. Tulis $f(x) = (x-a)g(x)$, untuk suatu $g(x) \in F[x]$. Jika $g(x)$ polinomial konstan tak nol maka bukti selesai. Jika $g(x)$ polinomial tak konstan maka terdapat $b \in F$ sehingga b akar dari $g(x)$. dapat dituliskan $f(x)=(x-a)(x-b)h(x)$ untuk suatu $h(x) \in$ F[x] dan seterusnya sehingga dapat difaktorisasi $f(x)$ di $F[x]$ adalah linier.

$\Leftarrow$ Misalkan $f(x)$ adalah polinomial tak konstan di $F[x]$ dan dapat difaktorkan kedalam faktor linier. Misalkan $ax - b$ adalah faktor dari $f(x)$ maka b/a adalah akar $f(x)$ dan karena F lapangan maka $b/a \in F$. sehingga setiap polinomial tak konstan di $F[x]$ memiliki akar di F. Jadi tertutup secara aljabar. ■

Definisi 2.10.6

Jika F sublapangan E, maka E dikatakan penutup aljabar penutup aljabar dari F jika

1. E adalah perluasan aljabar dai F
2. E tertutup secara aljabar

2.11. Lapangan Pemecah (*splitting field*).

Berikut adalah suatu lapangan perluasan yang dibangun dari akar-akar suatu polinomial $f(x)$ di $F[x]$

Definisi 2.11.1

Misalkan $f(x)$ merupakan polinomial di $F(x)$ berderajat ≥ 1. Maka perluasan K dari F dinamakan lapangan pemecah dari $f(x)$ atas F jika

(i) $f(x)$ dapat difaktorkan ke faktor-faktor linier dalam K, yaitu $f(x) = c(x-\alpha_1)\Lambda\ (x-\alpha_n), \alpha_i \in K$, atau

(ii) Jika lapangan K dibangun atas F dengan akar-akar $\alpha_1, \alpha_2, \Lambda\ , \alpha_n$ dari $f(x)$ *di* K atau $K = F(\alpha_1, \alpha_2, \Lambda\ , \alpha_n)$, $\alpha_i \in K$.

Contoh.

(i). Lapangan $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a,b \in \mathbb{Q}\}$merupakan lapangan pemecahan dari $x^2 - 2 \in \mathbb{Q}[x]$atas $\mathbb{Q}$

(ii).Lapangan pemecahan dari $x^2 + 1 \in \mathbb{R}[x]$ atas $\mathbb{R}$ adalah lapangan $\mathbb{C}$.

Teorema 2.11.1

Misalkan K adalah lapangan pemecah dari $f(x) \in F[x]$ atas F, maka K adalah perluasan berhingga dan perluasan aljabar dari F

Bukti

Misalkan $a_1,a_2,\ldots,a_n$ adalah akar-akar dari $f(x) \in F[x]$, Menurut definisi $K = F(a_1, a_2,\ldots,a_n)$, dan setiap a_i, $i = 1,2,\ldots,n$ aljabar atas F. Maka menurut teorema terbukti bahwa K adalah perluasan berhingga dan perluasan aljabar dari F. ■

2.12. Akar polinomial

Definisi 2.12.1

Misalkan $p(x) \in F[x]$, maka suatu elemen a yang memenuhi didalam beberapa perluasan dari F dinamakan akar $p(x)$ jika $p(a) = 0$

Lema 2.12.1

Misalkan $f(x) \in F(x)$, maka akan terdapat perluasan E dari F sehingga $f(x)$ mempunyai akar. Sehingga $[E:F] \leq der(f(x))$.

Bukti

Misalkan $p(x)$ adalah faktor takteruraikan dari $f(x)$. Semua akar $p(x)$ adalah akar dari $f(x)$. Diketahui $[E:F] = der(p(x)) \leq der(f(x))$. Oleh karena $p(x)$ mempunyai akar maka $f(x)$ mempunyai akar. ■

Teorema 2.12.1

Misalkan $f(x) \in F[x]$ dengan derajat $n \geq 1$. maka terdapat perluasan E dari F yang berderajat maksimal $n!$, dan $f(x)$ mempunyai n akar.

Bukti

Menurut lema 2.12.1 terdapat E_0 dari F dengan $[E_0:F] \leq n$ dengan $f(x)$ mempunyai akar a. Sehingga dalam $E_0[x]$, faktor dari $f(x)$ adalah $f(x) = (x - a)q(x)$, dengan $q(x)$ berderajat $n - 1$.

Dengan melanjutkan proses seperti diatas akan terdapat perluasan E dari E_0 yang berderajat $(n - 1)!$ dengan $q(x)$ mempunyai n -1 akar.

Karena semua akar dari $f(x)$ adalah a dan akar-akar dari $q(x)$. Kita dapatkan dalam E memuat semua n akar-akar dari $f(x)$.

Sehingga $[E:F] = [E:E_0][E_0:F] \leq (n - 1)!.n = n!$. ■

2.13. Peluasan normal

Selanjutnya akan ditunjukkan suatu perluasan dari suatu lapangan yang bersifat normal menurut definisi berikut :

Definisi 2.13.1

Suatu lapangan perluasan L atas K disebut perluasan normal jika

1. L merupakan perluasaan aljabar dari K

2. Setiap polinomial takteruraikan $f(x)$ atas K sedikitnya mempunyai satu akar di L dan memecah di L

Teorema 2.13.1

Setiap perluasan E dari F sedemikian sehingga $[E:F] = 2$ adalah perluasan normal.

Bukti

Misalkan $\alpha \in E$, $\alpha \notin F$. Misalkan $p(x)$ adalah polinomial dari α atas F. Maka $[F(\alpha):F]$ = derajat dari $p(x)$. Karena $[E: F(\alpha)][F(\alpha):F] = [E:F] = 2$ maka $[E: F(\alpha)] = 1$ dan $[F(\alpha):F] = 2$. sehingga $E = F(\alpha)$ dan derajat $p(x) = 2$. karena $p(x)$ mempunyai satu akar α di E maka $p(x)$ harus mempunyai akar lain yang juga di E. Sehingga $p(x)$ memecah di E, oleh karena itu E adalah lapangan pemecah dari $p(x) \in F[x]$ dan merupakan perluasan normal dari F

2.14. Perluasan separabel

Definisi 2.141

Suatu polinomial takteruraikan $f(x) \in F[x]$ dikatakan polinomial separabel jika tidak mempunyai akar ganda di lapangan pemecahannya.

Definisi 2.14.2

Suatu lapangan perluasaan K dikatakan separabel atas F jika setiap elemen dari K adalah akar dari polinomial separabel atas F.