BAB III

POLINOMIAL SEPARABEL

DARI LAPANGAN BERHINGGA

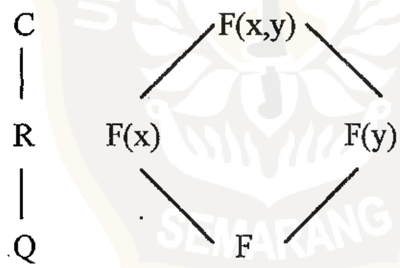
3.1 Lapangan perluasan

Definisi 3.1.1

E adalah suatu lapangan perluasan dari lapangan F, maka dapat ditulis dengan $F \leq E$.

Contoh:

Q lapangan bilangan rasional, R lapangan bilangan riil, dan C lapangan bilangan kompleks maka $Q \leqslant R \leqslant C$. R adalah lapangan perluasan dari Q dan C adalah lapangan perluasan dari R dan Q. Berikut ini diberikan diagram lattice untuk menggambarkan lapangan perluasan.



Definisi 3.1.2

$f(x) \in F[x]$ disebut polinomial tak tereduksi (irreducible polinomial) dalam $F[x]$ jika $f(x)$ tidak dapat difaktorkan sebagai dua polinomial-polinomial $g(x)h(x)$ dengan $g(x), h(x) \in F[x]$ keduanya berderajat lebih rendah dari $f(x)$.

Theorema 3.1.3

Misal F adalah lapangan dan f(x) polinomial yang tidak konstan dalam F[x], maka terdapat lapangan perluasan E dari F, dengan $\alpha \in$ E sedemikian sehingga $f(\alpha) = 0$.

Bukti:

F[x] adalah daerah ideal utama, karena daerah ideal utama merupakan daerah faktorisasi tunggal maka, $f(x) \in F[x]$ dapat difaktorkan secara tunggal sebagai $f(x) = p_1(x)p_2(x)\ldots p_n(x)$, dengan $p_i(x)$ (i=1,2…n) adalah polinomial prima yang tak tereduksi, karena p(x) polinomial tak tereduksi maka <p(x)> adalah ideal maximal dalam F[x], dengan $\frac{F[x]}{< p(x) >}$ suatu lapangan.

Didefinisikan suatu pemetaan ϕ dengan $\phi : F \to \frac{F[x]}{< p(x) >}$ dengan $a \to a + <p(x)>$.

ϕ adalah pemetaan 1-1, sebab $\forall$ a,b $\in$ F. Jika ϕ (a) = ϕ (b) maka $a + <p(x)> = b + <p(x)>$, atau $a\text{-}b \in <p(x)>$. tulis $a\text{-}b = k\, p(x)$

Jadi a-b suatu kelipatan p(x) yang berderajat 0 maka a-b = 0 atau a = b.

ϕ suatu monomorfisma ring, sebab

$$\begin{aligned} \phi\,(a+b) &= (a+b) + <p(x)> \\ &= (a + <p(x)>) + (b + <p(x)>) \\ &= \phi\,(a) + \ (b),\ \forall\, a,b \in F \end{aligned}$$

$$\begin{aligned} \phi\,(ab) &= (ab) + <p(x)> \\ &= (a + <p(x)>)\,(b + <p(x)>) \\ &= \phi\,(a)\,\phi\,(b),\ \forall\, a,b \in F \end{aligned}$$

maka $\phi(F) = \{a + \langle p(x)\rangle \mid a \in F\} \subseteq \dfrac{F[x]}{\langle p(x)\rangle}$ merupakan subfield dari $\dfrac{F[x]}{\langle p(x)\rangle}$,

jadi $F \cong \{a + \langle p(x)\rangle \mid a \in F\}$.

Misal $E = \dfrac{F[x]}{\langle p(x)\rangle}$ maka E merupakan lapangan perluasan dari F.

Akan dibuktikan $f(\alpha) = 0$, $\alpha \in E = \dfrac{F[x]}{\langle p(x)\rangle}$ ambil $\alpha \in E$ dengan $\alpha = x + \langle p(x)\rangle$

jika $p(x) = a_0x^0 + a_1x^1 + \ldots + a_nx^n$, $a_i \in F$, maka

$$
\begin{aligned}
p(\alpha) &= a_0\alpha^0 + a_1\alpha^1 + \ldots + a_n\alpha^n \\
&= a_0(x+\langle p(x)\rangle)^0 + a_1(x+\langle p(x)\rangle)^1 + a_2(x+\langle p(x)\rangle)^2 + \ldots + a_n(x+\langle p(x)\rangle)^n \\
&= (a_0x^0 + a_1x^1 + a_2x^2 + \ldots + a_nx^n) + \langle p(x)\rangle \\
&= p(x) + \langle p(x)\rangle = \bar{0} \in \frac{F[x]}{\langle p(x)\rangle}
\end{aligned}
$$

$p(\alpha) = 0$, karena $f(x) = p_1(\alpha).p_2(\alpha) \ldots p_n(\alpha)$, maka $f(\alpha) = 0$

Contoh:

Misal $f(x) = x^4 - x^2 - 2$ suatu polinomial tereduksi di F[x]. Karena f(x) polinom tereduksi maka f(x) dapat difaktorkan menjadi polinom – polinom tak tereduksi, yaitu $f(x) = x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$.

Dengan memandang polinom tak tereduksi $x^2 - 2$, maka menurut teorema 3.1.3 E merupakan perluasan lapangan dari F yang memuat $\sqrt{2}$, sedemikian sehingga $\left(\sqrt{2}\right)^2 - 2 = 2 - 2 = 0$. Demikian juga dengan polinomial tak tereduksi $x^2 + 1$, maka C merupakan lapangan perluasan dari F yang memuat i sedemikian sehingga $i^2 + 1 = -1 + 1 = 0$

Definisi 3.1. 4

$\alpha \in E$ disebut aljabar atas F dengan $F \leq E$ jika $f(\alpha) = 0$, untuk suatu $f(x) \neq 0 \in F[x]$, jika α bukan aljabar atas F maka α disebut transendental atas F.

Contoh :

C adalah lapangan perluasan dari Q, maka $\alpha = \sqrt{2}$ adalah elemen aljabar atas Q dalam C sebab ada $f(x) = x^2 - 2, \in Q[x]$ sedemikian sehingga $f(\alpha) = 0$.

Jika F adalah sub field dari lapangan E, maka E dapat dipandang sebagai ruang vektor atas lapangan F. Dimensi ruang vektor E(F) disebut derajat dari lapangan perluasan E atas F, yang untuk selanjutnnya diberi notasi [E:F]. Lebih lanjut lapangan perluasan disebut perluasan berhingga bila [E:F] berhingga..

Definisi 3.1.5

E adalah lapangan perluasan (extension field) lapangan F dikatakan perluasan aljabar (algebraic extension) jika setiap elemen dari E merupakan aljabar atas F.

Definisi 3.1.6

Jika E suatu lapangan perluasan dari F yang mempunyai dimensi berhingga n sebagai ruang vektor atas F, maka E disebut perluasan berhingga dengan derajat n atas F yang dinotasikan dengan [E:F] = n. Selanjutnya E disebut perluasan tak berhingga jika derajat perluasannya tak berhingga, ditulis [E:F] = ∞.

[E:F] = 1 jika hanya jika E = F dan [E:F] = 1 jika hanya jika E = F(1) = F.

Theorema 3.1.7

Setiap perluasan berhingga (finite extension) suatu lapangan merupakan perluasan aljabar.

Bukti:

Pandang E perluasan berhingga dari lapangan F yang mempunyai derajat n, maka ruang vektor E atas F memiliki dimensi n. Akan ditunjukkan E adalah perluasan aljabar, berarti setiap elemen di dalam E adalah aljabar atas F. Ambil α sembarang elemen dalam E, dan $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ elemen-elemen dalam E dan jika 1 adalah unit dari E maka $1, \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ merupakan elemen-elemen di dalam E berjumlah (n + 1).

Karena ruang vektor E berdimensi n, maka setiap himpunan (n + 1) elemen atau lebih tak bebas linear, sehingga himpunan $\{1, \alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n\}$ tak bebas linear, jadi terdapat elemen-elemen $a_0, a_1, a_2, \ldots, a_n$ dari F yang tidak semuanya nol sedemikian sehingga $a_0.1 + a_1\alpha + a_2\alpha^2 + \ldots + a_n\alpha^n = 0$.

Ini menunjukkan bahwa α adalah akar dari polinomial tidak nol.

$$a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \text{ dalam } F[x]$$

Sehingga α adalah aljabar atas F, karena α adalah sebarang elemen dalam E, maka E adalah perluasan aljabar.

Theorema 3.1.8

Jika F, E, K adalah lapangan – lapangan sedemikian sehingga E adalah perluasan berhingga dari F dan K adalah perluasan berhingga dari E, maka K adalah perluasan berhingga dari F dengan [K:F] = [K:E] [E:F]

Bukti:

Misal [K:E] = m dan [E:F] = n, dan $\{\alpha_i \mid i = 1,2,\ldots,n\}$adalah basis E atas F, dan $\{\beta_j \mid j = 1,2,\ldots,m\}$adalah basis K atas E. Dalam hal ini akan ditunjukkan bahwa m·n elemen-elemen $\alpha_i\beta_j$ membentuk suatu basis untuk ruang vektor K atas F. Ambil $\gamma \in K$, karena β_j membentuk basis K atas E maka diperoleh

$$\gamma = b_1\beta_1 + b_2\beta_2 + b_3\beta_3 + \ldots + b_m\beta_m$$

$$\gamma = \sum_{j=1}^{m} b_j\beta_j \text{ untuk } b_j \in E.$$

karena α_i basis dari E atas F maka

$$b_j = a_{1j}\alpha_1 + a_{2j}\alpha_2 + \ldots + a_{nj}\alpha_n$$

$$b_j = \sum_{i=1}^{n} a_{ij}\alpha_i \text{ untuk } a_{ij} \in F \text{ dengan tunggal}$$

sehingga

$$\gamma = b_1\beta_1 + b_2\beta_2 + b_3\beta_3 + \ldots + b_m\beta_m$$

$$\gamma = (a_{11}\alpha_1 + a_{21}\alpha_2 + \ldots + a_{n1}\alpha_n)\beta_1 + \ldots + (a_{1m}\alpha_1 + a_{2m}\alpha_2 + \ldots + a_{nm}\alpha_n)\beta_m$$

$$\gamma = \sum_{j=1}^{m}\left(\sum_{i=1}^{n} a_{ij}\alpha_i\right)\beta_j$$

$$\gamma = \sum_{i,j}^{m\,n} a_{ij}(\alpha_i\beta_j) \text{ dengan } a_{ij} \text{ tunggal di dalam F.}$$

Jadi ruang vektor K = [$\{\alpha_i\beta_j\}$] atas F dengan $\{\alpha_i\beta_j\}$adalah basis dari K atas F, (i = 1,2,..., n) dan (j = 1,2,...,m). Jadi [K:F] = [K:E] [E:F] = m.n

Dengan demikian jika F_i adalah suatu lapangan untuk i = 1, 2, ..., r dan F_{i+1} adalah perluasan berhingga F_i, maka F_r adalah perluasan berhingga dari F_1 dan $[F_r:F_1] = [F_r:F_{r-1}]\,[F_{r-1}:F_{r-2}]\ldots[F_2:F_1]$.

Teorema 3.1.9

Misal E adalah perluasan aljabar dari F, maka terdapat elemen-elemen $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$ sedemikian sehingga $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ merupakan ruang vektor yang mempunyai dimensi berhingga atas F, jika dan hanya jika E perluasan berhingga dari F.

Bukti:

($\Rightarrow$)Misalkan $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ dengan $\alpha_1 \in E$. Akan ditunjukkan E perluasan berhingga dari F. Karena E perluasan aljabar dari F maka $\alpha_1, \alpha_2, \ldots, \alpha_n$ merupakan aljabar atas F, maka jelaslah bahwa α_i (i = 1,2,...,n) merupakan aljabar atas setiap perluasan dari F dalam E , akibatnya

$F(\alpha_1)$	=	perluasan aljabar atas F
$F(\alpha_1, \alpha_2)$	=	perluasan aljabar atas $F(\alpha_1)$
$F(\alpha_1, \alpha_2, \alpha_3)$	=	perluasan aljabar atas $F(\alpha_1, \alpha_2)$
.		
.		
.		
$F(\alpha_1, \alpha_2, \ldots, \alpha_n)$	=	perluasan aljabar atas $F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$

$$\text{Sehingga } E = (F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}))(\alpha_n) = F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n)$$

$$\Big| \ (m_n) : \text{dimensi}$$

$$(F(\alpha_1, \alpha_2, \ldots, \alpha_{n-2}))(\alpha_{n-1}) = F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$$

$$\Big| \ (m_{n-1}) : \text{dimensi}$$

$$(F(\alpha_1, \alpha_2, \ldots, \alpha_{n-3}))(\alpha_{n-2}) = F(\alpha_1, \alpha_2, \ldots, \alpha_{n-2})$$

$$\vdots$$

$$(F(\alpha_1, \alpha_2))(\alpha_3) = F(\alpha_1, \alpha_2, \alpha_3)$$

$$\Big| \ (m_3) : \text{dimensi}$$

$$(F(\alpha_1))(\alpha_2) = F(\alpha_1, \alpha_2)$$

$$\Big| \ (m_2) : \text{dimensi}$$

$$(F(\alpha_1)) = F(\alpha_1)$$

$$\Big| \ (m_1) : \text{dimensi}$$

$$F = F$$

Karena α_n = aljabar atas $F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})$, sehingga

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n) : (F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})] = m_n$$

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) : (F(\alpha_1, \alpha_2, \ldots, \alpha_{n-2})] = m_{n-1}$$

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_{n-2}) : (F(\alpha_1, \alpha_2, \ldots, \alpha_{n-3})] = m_{n-2}$$

$$\vdots$$

$$[F(\alpha_1) : F] = m_1$$

menurut teorema 3.1.8

$$[F(\alpha_1, \alpha_2, \ldots, \alpha_n) : F] = [F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}, \alpha_n) : (F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})] \,.\, [F(\alpha_1, \alpha_2, \ldots, \alpha_{n-1}) : (F(\alpha_1, \alpha_2, \ldots, \alpha_{n-2})] \,.\, [F(\alpha_1, \alpha_2, \ldots, \alpha_{n-2}) : (F(\alpha_1, \alpha_2, \ldots, \alpha_{n-3})] \ldots [F(\alpha_1) : F]$$

$$[F(\alpha_1, \alpha_2, ..., \alpha_n) : F] = m_n \,.\, m_{n-1} \,.\, m_{n-2} \ldots m_2 \,.\, m_1 < \infty.$$

$$[E:F] \;=\; m_n \,.\, m_{n-1} \,.\, m_{n-2} \ldots m_2 \,.\, m_1 < \infty.$$

Sehingga E adalah perluasan berhingga dari F.

($\Leftarrow$) E perluasan berhingga dari F, maka E berdimensi hingga atas F. Jika $[E:F] = 1$ maka $E = F(1) = F$, tidak ada yang harus dibuktikan.

Jika $E \neq F$, ambil sembarang $\alpha_1 \in E$, $\alpha_1 \notin F$ maka $[F(\alpha_1) : F] > 1$ (sebab $F(\alpha_1) \neq F$).

Jika $F(\alpha_1) = E$, maka tidak ada yang harus dibuktikan.

Jika $F(\alpha_1) \neq E$, ambil $\alpha_2 \in E$, $\alpha_2 \notin F(\alpha_1)$, maka $[F(\alpha_1, \alpha_2) : F(\alpha_1)] > 1$ (sebab $F(\alpha_1,\alpha_2) \neq F(\alpha_1)$).

Jika $F(\alpha_1,\alpha_2) = E$, maka tidak ada yang harus dibuktikan

Jika $F(\alpha_1,\alpha_2) \neq E$, ambil $\alpha_3 \in E$, $\alpha_3 \notin F(\alpha_1, \alpha_2)$

.
. dan seterusnya
.

maka karena $[E:F] < \infty$ akan didapat $\alpha_4, \alpha_5, ..., \alpha_n \ni F(\alpha_1, \alpha_2, ..., \alpha_n) : E$.

E merupakan perluasan berhingga dari F maka diperoleh indek n adalah berhingga.

Jika E perluasan dari F dan $\alpha,\beta \in E$ adalah aljabar atas F, maka $\alpha+\beta$, $\alpha\beta$, $\alpha-\beta$ dan α/β aljabar atas F dengan $\beta \neq 0$.

Teorema 3.1.10

Misal E suatu lapangan perluasan dari F , maka

$$\overline{F_E} = \{\alpha \in E \mid \alpha \text{ adalah aljabar atas } F\}$$

Merupakan sub field dari E, selanjutnya disebut penutup aljabar dari F dalam E.

Bukti: (bahwa = $\overline{F_E}$ subfield dari E)

Ambil sembarang α, $\beta \in \overline{F_E}$. Maka α, β merupakan aljabar atas F. Menurut theorema 3.1.9 $F(\alpha, \beta)$ merupakan perluasan berhingga dari F karena $F(\alpha, \beta)$ perluasan berhingga atas F, maka menurut theorema 3.1.7 $F(\alpha, \beta)$ perluasan aljabar atas F yaitu $F(\alpha,\beta) \subseteq \overline{F_E}$, karena $F(\alpha, \beta)$ suatu lapangan $\alpha, \beta \in F(\alpha, \beta)$ maka $\alpha+\beta$, $\alpha\beta$, $\alpha-\beta$, $\alpha\beta^{-1}$, $\beta\neq 0 \in F(\alpha, \beta) \subseteq \overline{F_E}$.

Jadi $\overline{F_E}$ = subfield dari E

Definisi 3.1.11

Suatu lapangan F tertutup secara aljabar jika setiap polinomial tidak konstan dalam F[x] memiliki akar di F.

Teorema 3.1.12

Suatu lapangan F tertutup secara aljabar jika dan hanya jika untuk setiap polinomial tidak konstan $f(x) \in F[x]$ dapat difaktorisasi atas faktor-faktor linear.

Bukti:

($\Rightarrow$)Misal F adalah tertutup secara aljabar. Ambil sembarang f(x) tidak konstan dalam F[x] maka $(\exists\ a \in F).f(a) = 0$. Menurut akibat 2.3.4 (x-a) adalah faktor dari f(x) sehingga f(x) = (x-a) g(x).

Jika g(x) = c (konstan) maka f(x) = c(x-a), $c \in F$ maka bukti selesai. Jika $g(x) \neq c$ (konstan) maka $(\exists\ b \in F).g(b) = 0$.Menurut akibat 2.3.4 (x-b) adalah faktor dari g(x), sehingga g(x) = (x-b) h(x).

Jika $h(x) = d$ (konstan) maka $g(x) = d\,(x-b)$, $d \in F$ sehingga $f(x) = (x-a)(x-b)d$, $d \in F$. Jika $h(x) \neq d$ (konstan) maka $(\exists\, c \in F).h(c) = 0$, sehingga $h(x) = (x-c)\, t(x)$ .... dan seterusnya. Proses ini dapat diteruskan dan karena derajat $f(x)$ berhingga maka proses ini berhingga, sehingga didapatkan $f(x) = (x-a)(x-b)(x-c) \ldots (x-d)\, k$ dengan $k \in F$.

($\Leftarrow$) Misalkan $f(x)$ adalah polinom tak konstan di $F[x]$ dan dapat difaktorkan dalam faktor linear. Jika $(ax-b) \in F[x]$ faktor linear dari $f(x)$ maka $b/a \in F$ merupakan akar dari $(ax-b)$, sehingga b/a akar dari $f(x)$.

Maka $(\forall\, f(x) \neq \text{konstan} \in F[x])\ (\exists\, b/a \in F)\ .\ f(b/a) = 0$. Jadi F tertutup secara aljabar

3.2 Lapangan Berhingga

Lapangan disebut lapangan berhingga jika lapangan tersebut memiliki elemen yang banyaknya berhingga.

Theorema 3.2.1

E adalah perluasan berhingga dengan derajat n dan F adalah lapangan berhingga dengan q elemen, sedemikian sehingga $[E:F] = n$, maka E memiliki q^n elemen.

Bukti:

Karena $[E:F] = n$ maka E dapat dipandang sebagai ruang vektor atas lapangan F dengan dimensi n. Misal $\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n\}$adalah basis dari ruang vektor E atas F, maka $\forall\ \alpha \in E$ terdapat dengan tunggal b_i, $i = 1,2,\ldots,n \in F$ sehingga $\alpha = b_1\alpha_1, b_2\alpha_2, \ldots, b_n\alpha_n$. Karena untuk setiap b_i dapat diisi oleh q elemen dari F maka banyak kombinasi linear yang berbeda dari $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ adalah $|E| = q^n$ elemen. Jadi E terdiri atas q^n elemen.

Sehingga jika q adalah bilangan prima maka F lapangan berhingga dengan n elemen sedemikian sehingga $[E:F] = n$ maka E memiliki q^n elemen.

Definisi 3.2.2

Misal G grup terhadap pergandaan, a elemen sembarang dalam G. Order elemen a adalah bilangan bulat positif terkecil m sedemikian sehingga $a^m = e$, dengan e adalah elemen identitas dalam G, dinotasikan $O(a) = m$.

3.3 Perluasan Separabel

Definisi 3.3.1

Misal F suatu lapangan dengan penutup aljabar (algebraic closure) $\overline{F}$, $\{f_i(x) \mid i \in I\}$ koleksi dari polinomial – polinomial dalam F[x]. Suatu lapangan $E \leq \overline{F}$ lapangan pemisah dari $\{f_i(x) \mid i \in I\}$ atas F jika E adalah sub field terkecil dari $\overline{F}$ yang memuat F dari setiap $f_i(x)$, untuk $i \in I$. Suatu lapangan $E \leq \overline{F}$ adalah lapangan pemisah atas F, jika $E \leq \overline{F}$ adalah lapangan pemisah dari himpunan sembarang polinomial – polinomial dalam F[x].

Contoh :

$Q(\sqrt{2}, \sqrt{3})$ adalah lapangan pemisah dari $f(x) = x^4 - 5x^2 + 6$ sebab

$f(x) = (x^2 - 2)(x^2 - 3)$

$= (x + \sqrt{2})(x - \sqrt{2})(x + \sqrt{3})(x - \sqrt{3})$

Teorema 3.3.2

Misal $f(x) \in F[x]$ polinomial tidak konstan dalam lapangan F dan E lapangan perluasan dari lapangan F. $\alpha \in E$ adalah akar ganda dari f(x) jika dan hanya jika α adalah akar persekutuan dari f(x) dan $f^1(x)$.

Bukti

($\Rightarrow$) Misal α akar ganda dari f(x), dan misalkan m adalah banyaknya α dengan $m \geq 2$ dan $f(x) = (x-\alpha)^m g(x)$, dimana g(x) polinomial atas lapangan F sedemikian sehingga $g(\alpha) \neq 0$, sehingga

$$f^1(x) = m\,(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g^1(x)$$

$$f^1(\alpha) = m\,(\alpha-\alpha)^{m-1}g(\alpha) + (\alpha-\alpha)^m g^1(\alpha) = 0.$$

Karena $m \geq 2$ dan $f^1(\alpha) = 0$, maka α adalah akar persekutuan dari f(x) dan $f^1(x)$.

($\Leftarrow$) α akar persekutuan dari f(x) dan $f^1(x)$, maka α adalah akar ganda dari f(x).

Andaikan α bukan akar ganda dari f(x), dalam hal ini $f(x) = (x-\alpha)g(x)$, dengan g(x) polinomial atas lapangan F sedemikian sehingga $g(\alpha) \neq 0$, maka

$$f^1(x) = (x-\alpha)g^1(x) + g(x)$$

$$f^1(\alpha) = (\alpha-\alpha)g^1(x) + g(\alpha) = g(\alpha) \neq 0.$$

Sehingga dapat disimpulkan bahwa α bukan akar persekutuan dari f(x) dan $f^1(x)$, terjadi kontradiksi, maka pengandaian harus diingkar. Jadi α adalah akar ganda dari f(x).

Teorema 3.3.3

Misal f(x) polinomial tak tereduksi atas lapangan F, maka f(x) mempunyai akar ganda dalam lapangan perluasan jika dan hanya jika $f^1(x) = 0$.

Bukti

($\Rightarrow$) Misal f(x) polinomial tak terduksi atas lapangan F dan α akar ganda dari f(x) dalam lapangan perluasan E atas F, sedemikian sehingga α adalah akar dari $f^1(x)$ (teorema 3.3.2). Karena f(x) polinomial tak tereduksi yang memiliki akar α dan $f^1(x)$ polinomial lain yang juga memiliki akar α, maka f(x) adalah pembagi dari $f^1(x)$. Jika $f^1(x) \neq 0$, maka deg $f^1(x)$ < deg f(x) sehingga berakibat f(x) tidak bisa membagi $f^1(x)$. Oleh karena itu $f^1(x) = 0$.

($\Leftarrow$) misal f(x) polinomial tak tereduksi berderajat n atas lapangan F sedemikian sehingga $f^1(x) = 0$

Misal E lapangan pemisah dari f(x) atas lapangan F, maka:

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$$

dimana $\alpha_1,\alpha_2,\ldots,\alpha_n$ adalah n akar dari f(x) dalam E dan c elemen tidak nol dalam F.

sehingga

$$f^1(x) \;=\; c[(x-\alpha_2)(x-\alpha_3)\ldots(x-\alpha_n)+(x-\alpha_1)(x-\alpha_3)\ldots(x-\alpha_n)+\ldots+(x-\alpha_1)(x-\alpha_2)..(x-\alpha_{n-1})$$

$$f^1(\alpha_i) \;= c[(\alpha_i-\alpha_2)(\alpha_i-\alpha_3)\ldots(\alpha_i-\alpha_n)+(\alpha_i-\alpha_1)(\alpha_i-\alpha_3)\ldots(\alpha_i-\alpha_n)+\ldots+(\alpha_i-\alpha_1)$$
$$(\alpha_i-\alpha_2)\ldots(\alpha_i-\alpha_{n-1})]$$

$$f^1(\alpha_i) = c\prod_{j\neq i}(\alpha_i-\alpha_j)\neq 0\,,\ \ \forall\, i = 1,2,3,\ldots,n$$

karena $\alpha_1, \alpha_2, \ldots, \alpha_n$ semuanya berbeda, padahal $f^1(x) = 0$ maka salah satu dari akar-akar $\alpha_1, \alpha_2, \ldots, \alpha_n$ harus merupakan akar ganda dari f(x). Oleh karena itu f(x) mempunyai akar ganda dalam E.

Teorema 3.3.4

Tidak ada polinomial tak tereduksi atas lapangan dengan karakteristik nol yang mempunyai akar ganda dalam lapangan perluasannya.

Bukti:

Misal $f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ polinomial tak tereduksi dengan derajat $n \geq 1$ atas lapangan F yang memiliki karakteristik nol.

Maka $a_n \neq 0$ dan $f^1(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$.

Karena F lapangan dengan karakterisitik nol dan $a_n \neq 0$ maka $na_n \neq 0$ dan $f^1(x) \neq 0$.

Jika mungkin misal f(x) mempunyai akar ganda, sebut α dalam lapangan perluasan E atas F, maka α juga merupakan akar dari $f^1(x)$. Karena f(x) polinomial tak tereduksi yang memiliki akar α dan $f^1(x)$ polinomial lain yang juga memiliki akar α, maka f(x) adalah pembagi dari $f^1(x)$. Jika $f^1(x) \neq 0$, maka deg $f^1(x) <$ deg f(x) sehingga berakibat f(x) tidak bisa membagi $f^1(x)$. Oleh karena itu $f^1(x) = 0$.

Akibatnya α bukan akar dari $f^1(x)$ dan α tidak bisa menjadi akar ganda dari f(x).

Definisi 3.3.5

Polinomial tak tereduksi f(x) dalam lapangan F adalah separabel dalam F jika semua akar-akar dari f(x) dalam lapangan pemisahnya adalah simple, yaitu jika f(x) tidak mempunyai akar-akar ganda dalam lapangan pemisah.

Dengan demikian

(i) Sesuai dengan definisi separabel dan teorema 3.3.3. mengakibatkan bahwa polinomial tak terduksi f(x) disebut separabel jika dan hanya jika $f^1(x) \neq 0$

(ii) Sesuai dengan definisi separabel dan teorema 3.3.4 mengakibatkan bahwa untuk setiap polinomial tidak nol yang memiliki karakteristik nol adalah separabel.

Definisi 3.3.6

Misal E adalah suatu perluasan aljabar dari F, maka $\alpha \in E$ dikatakan separabel atas F jika polinomial minimal untuk α atas F merupakan polinomial separabel yaitu semua akar-akarnya berbeda. Jika α tidak separabel, maka disebut inseparabel.

Contoh:

$Q(\sqrt{2})$ merupakan perluasan aljabar dari Q. $f(x) = (x^2 - 2)$ merupakan polinomial separabel atas Q, sebab $f(x) = (x + \sqrt{2})(x - \sqrt{2})$.

Definisi 3.3.7

Suatu perluasan aljabar E atas F dikatakan separabel jika untuk setiap elemen dalam E adalah separabel atas F, jika tidak maka E disebut perluasan inseparable.

3.4 Lapangan Perfect

Definisi 3.4.1

Suatu lapangan F dikatakan perfect jika semua perluasan berhingga dari F adalah separabel.

Teorema 3.4.2

Setiap lapangan dengan karakteristik nol adalah perfect.

Bukti:

Misal F adalah lapangan dengan karakteristik nol dan E adalah perluasan berhingga dari F. Kemudian untuk menunjukkan F adalah perfect, maka harus ditunjukkan E adalah separabel, yaitu dengan menunjukkan bahwa untuk setiap elemen dalam E adalah separabel atas F atau polinomial minimal untuk tiap-tiap elemen dari F atas E adalah separabel yaitu mempunyai akar-akar yang berbeda. Misal α sembarang elemen dalam E dan

$f(x) = a_0 + a_1x + \ldots + a_nx^n$ dengan $a_n \neq 0$ adalah suatu polinomial minimal α atas F, maka

$$f^1(x) = a_1 + 2a_2x + \ldots + na_nx^{n-1}$$

Jika f(x) memiliki akar ganda dalam E maka dari teorema 3.3.3. telah ditunjukkan bahwa $f^1(x) = 0$, yaitu

$$a_1 + 2a_2x + \ldots + na_nx^{n-1} = 0 = 0x + 0x^2 + \ldots + 0x^{n-1}$$

yang berarti bahwa

$$a_1 = 0, 2a_2 = 0, \ldots, na_n = 0$$

Tetapi F adalah lapangan dengan karakteristik nol dan hal ini dapat terjadi jika

$a_1 = 0, a_2 = 0, \ldots, a_n = 0$, yaitu jika f(x) adalah konstan

Hal ini kontradiksi.

Karena polinomial minimal α atas F tidak memiliki akar ganda, sehingga dari definisi 3.3.5 maka α adalah separabel atas F.

Karena α adalah sembarang elemen dalam E, maka untuk setiap elemen dalam E adalah separabel atas F, sehingga E adalah perluasan separabel atas F dan F adalah perfect.

Teorema 3.4.3

Suatu polinomial tak tereduksi f(x) atas F dengan karakteristik $p > 0$ adalah inseparable jika dan hanya jika f(x) adalah polinomial dalam x^p.

Bukti:

Misal $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ polinomial tak tereduksi dengan derajat $n > 1$ atas lapangan F sedemikian sehingga $a_n \neq 0$, dan $f^1(x) = a_1 + 2a_2x + \dots + na_nx^{n-1}$.

($\Rightarrow$) Akan ditunjukkan bahwa f(x) adalah polinomial dalam x^p

Pertama kali akan ditunjukkan bahwa polinomial tak terduksi f(x) adalah inseparabel jika dan hanya jika $f^1(x) = 0$. Asumsikan f(x) adalah inseparabel yaitu f(x) setidaknya mempunyai satu akar ganda sebut α dalam lapangan pemisahnya atas F, maka menurut teorema 3.3.2, α juga merupakan akar dari $f^1(x)$.

Karena f(x) polinomial tak tereduksi yang memiliki akar α dan $f^1(x)$ polinomial lain yang juga memiliki akar α, maka f(x) harus membagi $f^1(x)$. Jika $f^1(x) \neq 0$, maka jelas bahwa deg $f^1(x) <$ deg f(x), sehingga f(x) tidak dapat membagi $f^1(x)$. Oleh karena itu $f^1(x) = 0$.

Selanjutnya jika $f^1(x) = 0$ dan E suatu lapangan pemisah dari f(x) atas F, maka:

$f(x) = c(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$,

dimana $\alpha_1,\alpha_2,\ldots,\alpha_n$ adalah n akar dari f(x) dalam E dan c elemen tidak nol dalam F.

Sehingga

$f^1(x) = c[(x-\alpha_2)(x-\alpha_3)\ldots(x-\alpha_n)+ (x-\alpha_1)(x-\alpha_3)\ldots(x-\alpha_n)+\ldots+ (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_{n-1})]$

$f^1(\alpha_i) = c[(\alpha_i -\alpha_2)(\alpha_i -\alpha_3)\ldots(\alpha_i -\alpha_n)+ (\alpha_i -\alpha_1)(\alpha_i -\alpha_3)\ldots(\alpha_i -\alpha_n)+\ldots+ (\alpha_i -\alpha_1)$

$(\alpha_i -\alpha_2)\ldots(\alpha_i -\alpha_{n-1})]$

$f^1(\alpha_i) = c \prod_{j\neq i}(\alpha_i - \alpha_j) \neq 0$, $\forall$ i =1,2,3,…,n

karena $\alpha_1,\alpha_2,\ldots,\alpha_n$ semuanya berbeda, padahal $f^1(x) = 0$ maka salah satu dari akar-akar $\alpha_1,\alpha_2,\ldots,\alpha_n$ harus merupakan akar ganda dari f(x). Oleh karena itu f(x) mempunyai akar ganda dalam E dan f(x) inseparabel atas F.

Sehingga f(x) inseparabel $\Leftrightarrow f^1(x) = 0$

$\Leftrightarrow a_1 +2\, a_2x+\ldots+na_nx^{n-1} = 0$

$\Leftrightarrow a_1 = 0,\ 2a_2 = 0,\ldots,\ na_n =0$

Sekarang jika karakteristik dari F adalah $p \neq 0$, maka masing –masing elemen tidak nol memiliki order p. Jadi untuk sebarang k, $1 \leq k \leq n$, $ka_k = 0$ dan $a_k \neq 0$

$\Rightarrow$ p adalah pembagi dari k

Akibatnya jika $ka_k = 0$ maka (i) salah satu $a_k = 0$ atau p adalah pembagi dari k

(ii) salah satu $a_k = 0$ atau $a_k \neq 0$ maka $k = k_1p$ untuk

k_1 bilangan bulat positif.

Sehingga jika terdapat $a_k x^k$ dalam f(x) sedemikian sehingga $a_k \neq 0$, maka dapat dituliskan $a_{k_1p} x^{k_1p} = a_{k_1p}\left(x^p\right)^{k_1}$ sedemikian sehingga

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

$$f(x) = a_0 + a_{k_1p}x^{k_1p} + a_{k_2p}x^{k_2p} + \ldots + a_{k_np}x^{k_np}$$

$$f(x) = a_0 + a_{k_1p}\left(x^p\right)^{k_1} + a_{k_2p}\left(x^p\right)^{k_2} + \ldots + a_{k_np}\left(x^p\right)^{k_n}$$

$$f(x) = a_0 + a_{1p}\left(x^p\right)^1 + a_{2p}\left(x^p\right)^2 + \ldots + a_{np}\left(x^p\right)^n$$

$f(x) = b_0 + b_1x^p + 2x^{2p} + \ldots + b_mx^{mp}$, untuk m bulat positif, dimana $b_i = a_{ip}$. Jadi jika f(x) adalah insparabel, maka f(x) polinomial di x^p

($\Leftarrow$) f(x) adalah polinomial di x^p maka f(x) adalah inseparabel

Misal $f(x) = b_0 + b_1x^p + 2x^{2p} + \ldots + b_mx^{mp}$ adalah polinomial tak tereduksi atas lapangan F. Asumsikan bahwa f(x) separabel yaitu f(x) tidak memiliki akar ganda dalam lapangan pemisahnya. Andaikan α bukan akar ganda dari f(x), maka

$$f(\alpha) = b_0 + b_1\alpha^p + b_2\alpha^{2p} + \ldots + b_m\alpha^{mp} = 0$$

$$f^1(\alpha) = pb_1\alpha^{p-1} + 2pb_2\alpha^{2p-1} + \ldots + mpb_m\alpha^{mp-1}$$

Karena p adalah karakteristik dari f(x) maka

$$f^1(\alpha) = 0 + 0 + \ldots + 0 = 0$$

Sehingga diperoleh $f(\alpha) = 0$ dan $f^1(\alpha) = 0$, maka terjadi kontradiksi, sehingga pengandaian harus diingkari, oleh karena itu α merupakan akar ganda dari f(x). Maka f(x) inseparabel.

Teorema 3.4.4

Suatu lapangan dengan karakteristik $p \neq 0$ sedemikian sehingga untuk setiap elemen dari lapangan itu berbentuk pangkat p dari elemen – elemen lain yang berbeda adalah perfect.

Bukti:

Misal F adalah suatu lapangan yang memiliki karakteristik $p \neq 0$ sedemikian sehingga untuk setiap elemen dari lapangan itu berbentuk pangkat p dari elemen – elemen lain yang berbeda. Kemudian untuk menunjukkan F adalah perfect maka harus ditunjukkan bahwa setiap perluasan berhingga dari F merupakan perluasan separabel atas F. Misal E perluasan berhingga dari F. Untuk menujukkan E adalah separabel atas F, maka harus ditunjukkan bahwa untuk setiap elemen dari E adalah separabel atas F, hal ini cukup ditunjukkan bahwa untuk setiap polinomial tak tereduksi atas F adalah separabel. Tetapi dari teorema 3.4.3 telah ditunjukkan bahwa hanya polinomial-polinomial yang inseparable atas F dengan karakteristik $p \neq 0$ adalah polinomial-polinomial dalam x^p. Tetapi jika kita telusuri ada beberapa polinomial – polinomial dalam x^p atas F yang memiliki bentuk

$$f(x^p) = a_0 + a_1x^p + \ldots + a_mx^{mp}, \quad \text{m adalah bilangan bulat positif}$$

Menurut hipotesis yang diberikan, terdapat hubungan antara elemen-elemen $a_0, a_1, \ldots, a_m$ dengan $b_0, b_1, \ldots, b_m$ dalam F, sedemikian sehingga

$$a_0 = b_0^p,\ a_1 = b_1^p,\ \ldots,\ a_m = b_m^p$$

sehingga

$$f(x^p) = b_0^p + b_1^px^p + b_2^px^{2p} + \ldots + b_m^px^{mp}$$

$$= b_0^p + (b_1x)^p + (b_2x^2)^p + \ldots + (b_mx^m)^p$$

$$= (b_0 + b_1x + b_2x + \ldots + b_mx^m)^p$$

karena $f(x^p)$ tak tereduksi, dan tidak ada polinomial tak tereduksi atas F yang inseparabel maka $f(x^p)$ separabel sehingga terbukti F adalah perfect.

Akibat 3.4.5

Setiap lapangan berhingga adalah perfect.

Bukti :

Misal F adalah lapangan dengan karakteristik $p \neq 0$.

Menurut pemetaan $\phi : F \to F : \phi(x) = x^p \ \forall\, x \in F$

ϕ merupakan pemetaan homomorfisma sebab

$$\phi(x+y) = (x + y)^p$$
$$= x^p + y^p$$
$$= \phi(x) + \phi(y)$$

$$\phi(x.y) = (x\,.y)^p$$
$$= x^p\,.\,y^p$$
$$= \phi(x)\,.\,\phi(y)$$

ϕ merupakan pemetaan satu-satu untuk

$$\phi(x) = \phi(y)$$
$$\Rightarrow \phi(x) - \phi(y) = 0$$
$$\Rightarrow \phi(x) - \phi(y) = \phi(0)$$
$$\Rightarrow \phi(x) + (\phi(-y)) = \phi(0)$$
$$\Rightarrow \phi(x + (-y)) = \phi(0)$$
$$\Rightarrow \phi(x - y) = \phi(0)$$

$\Rightarrow (x - y)^p = 0^p$

$\Rightarrow x - y = 0$

$\Rightarrow x = y$

Sehingga ϕ adalah pemetaan monomorfisma dan onto. Akibatnya untuk setiap elemen dari F memiliki pangkat p. Sehingga menurut teorema 3.4.4. F adalah perfect.