

BAB II

TINJAUAN PUSTAKA

Dalam bab ini dijelaskan beberapa teorema dan definisi yang dapat menunjang materi pembahasan pada bab III, antara lain ring, lapangan, ring polinomial dan faktorisasi polinomial.

2.1 Ring

Definisi 2.1.1

Ring adalah suatu himpunan R yang tidak kosong yang dilengkapi dengan operasi biner penjumlahan (+) dan pergandaan (\bullet) yang ditulis dengan $(R, +, \bullet)$ yang memenuhi aksioma-aksioma dibawah ini :

I. R merupakan grup komutatif terhadap penjumlahan, jika:

1. Memenuhi sifat tertutup

$$(\forall a, b \in R) (\exists c \in R), a + b = c$$

2. Memenuhi sifat assosiatif

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

3. Terdapat unsur 0 di R sedemikian sehingga

$$0 + a = a + 0 = a, \forall a \in R$$

4. Untuk setiap $a \in R$ dapat ditemukan elemen $-a \in R$ sehingga

$$(\forall a \in R) (\exists -a \in R), -a + a = a + (-a) = 0$$

5. Memenuhi sifat komutatif

$$a + b = b + a, \forall a, b \in R$$

II. Terhadap operasi pergandaan

1. Memenuhi sifat tertutup

$$(\forall a, b \in R)(\exists c \in R) a \bullet b = c$$

2. Memenuhi sifat asosiatif

$$(a \bullet b) \bullet c = a \bullet (b \bullet c), \forall a, b, c \in R$$

III. Kedua aturan komposisi diatas dapat dihubungkan dengan aksioma distributivitas

$$a \bullet (b + c) = ab + ac, \forall a, b, c \in R$$

$$(b + c) \bullet a = ba + bc, \forall a, b, c \in R$$

Contoh:

Misalkan Z himpunan bilangan bulat, Q himpunan bilangan rasional, R himpunan bilangan nyata dan C himpunan bilangan kompleks maka $\langle Z, +, \bullet \rangle$, $\langle Q, +, \bullet \rangle$, $\langle R, +, \bullet \rangle$, dan $\langle C, +, \bullet \rangle$ merupakan suatu ring.

Definisi 2.1.2

Suatu ring R yang memuat e sehingga berlaku $eb = be = b, \forall b \in R$ disebut ring dengan elemen satuan dimana elemen satuannya adalah e .

Apabila ring R memiliki elemen satuan maka elemen satuan tersebut adalah tunggal.

Definisi 2.1.3

Misalkan R suatu ring, maka R dikatakan ring komutatif jika berlaku $cd = dc, \forall c, d \in R$.

Definisi 2.1.4

Misalkan R ring dan $S \subseteq R$. S disebut subring dari R jika memenuhi

$$(i) \forall x, y \in S \Rightarrow x - y \in S$$

$$(ii) \forall x, y \in S \Rightarrow xy \in S \text{ dan } yx \in S$$

Definisi 2.1.5

Jika R dan R' adalah ring, maka ring homomorfisma dari R ke R' merupakan pemetaan $\phi : R \rightarrow R'$ sedemikian sehingga:

$$(i) \phi(x + y) = \phi(x) + \phi(y)$$

$$(ii) \phi(xy) = \phi(x) \phi(y)$$

untuk semua x, y dalam R .

Definisi 2.1.6

Misalkan R dan R' adalah suatu ring. Suatu pemetaan $\phi : R \rightarrow R'$ dikatakan ring isomorfis dari R ke R' jika dipenuhi kondisi sebagai berikut :

1. ϕ merupakan pemetaan bijektif dari R ke R'
2. $\phi(x + y) = \phi(x) + \phi(y)$, untuk $x, y \in R$
3. $\phi(xy) = \phi(x) \phi(y)$, untuk $x, y \in R$

Jika pemetaan isomorfis dari R ke R' ada, maka dapat dikatakan bahwa R isomorfis ke R' .

2.2 Lapangan

Definisi 2.2.1

Misalkan R suatu ring, elemen $c \in R$ dan $c \neq 0$ disebut pembagi nol sejati jika terdapat $d \in R$ dan $d \neq 0$ sehingga berlaku $cd = dc = 0$.

Dari definisi diatas ring R dikatakan tidak memiliki pembagi nol sejati jika dipenuhi :

1. $c \neq 0, d \neq 0 \Rightarrow cd \neq 0, \forall c, d \in R$ atau
2. $cd = 0 \Rightarrow c = 0 \vee d = 0, \forall c, d \in R$

Contoh:

1. Ring $\langle \mathbb{Z}, +, \cdot \rangle, \langle \mathbb{Q}, +, \cdot \rangle, \langle \mathbb{R}, +, \cdot \rangle$ dan $\langle \mathbb{C}, +, \cdot \rangle$ tidak memuat pembagi nol sejati.
2. Ring $\langle \mathbb{Z}_8, +, \cdot \rangle$ memuat pembagi nol sejati karena dalam \mathbb{Z}_8 terdapat elemen $\bar{2} \cdot \bar{4} = \bar{0}$. Jadi $\bar{2}$ dan $\bar{4}$ adalah pembagi nol sejati dari ring \mathbb{Z}_8 .

Definisi 2.2.2

Suatu ring komutatif dengan elemen satuan dan tidak memuat pembagi nol sejati disebut daerah integral.

Definisi 2.2.3

Suatu ring komutatif dengan elemen satuan dan setiap elemen tak nolnya memiliki invers disebut lapangan (field).

Teorema 2.2.4

Setiap daerah integral berhingga disebut lapangan.

Bukti:

Misalkan $0, 1, a_1, a_2, \dots, a_n$ elemen didalam daerah integral berhingga D , maka akan ditunjukkan bahwa untuk $a \in D$ dan $a \neq 0$ terdapat $b \in D$ sedemikian sehingga $ab = 1$.

Andaikan $a_1, a_2, \dots, a_n \in D$, maka:

$$aa_i = aa_j$$

$$a_i = a_j \quad (\text{hukum kanselasi})$$

Karena D tidak memiliki pembagi nol maka tidak ada elemen dalam D bernilai 0.

Oleh karena a_1, a_2, \dots, a_n merupakan elemen dalam $1, a_1, \dots, a_n$ maka didapat $a_1 = 1, aa_i = a_1$, untuk $i = 1, 2, \dots, n$ sehingga $a = 1$, sedemikian sehingga a memiliki invers.

Akibat 2.2.5

Jika p suatu bilangan prima maka Z_p adalah lapangan.

Definisi 2.2.6

Dalam ring R apabila terdapat bilangan bulat positif terkecil m sedemikian sehingga $m \cdot a = 0, a \in R$ maka R dikatakan memiliki karakteristik m , jika tidak maka R dikatakan memiliki karakteristik nol.

Contoh:

Misalkan $R = I_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$, maka bilangan 4 mempunyai sifat bahwa $4 \cdot \bar{a} = \bar{0}$ untuk setiap $\bar{a} \in I_4$. Bilangan 8, 12, 16, ... mempunyai sifat yang sama dengan bilangan 4. Akan tetapi karena 4 merupakan bilangan bulat positif yang paling kecil maka 4 disebut karakteristik dari R .

Teorema 2.2.7

Jika R merupakan ring komutatif yang memuat elemen satuan, maka R memiliki karakteristik $m > 0$ jika dan hanya jika m bilangan bulat positif terkecil sedemikian sehingga $m \cdot 1 = 0$.

Bukti:

(\Rightarrow) Dari definisi 2.2.6 didapat bahwa jika R memiliki karakteristik $m > 0$ maka $m \cdot a = 0$ untuk semua $a \in R$, sehingga $m \cdot 1 = 0$

(\Leftarrow) Akan ditunjukkan m suatu bilangan bulat positif sedemikian sehingga berlaku $m \cdot 1 = 0$. Untuk semua $a \in R$,

$$\begin{aligned} m \cdot a &= a + a + a + \dots + a \\ &= a(1 + 1 + \dots + 1) \\ &= a(m \cdot 1) = a \cdot 0 = 0 \end{aligned}$$

sehingga diperoleh bahwa m merupakan bilangan bulat positif.

Definisi 2.2.8

Grup Siklik adalah grup yang dihasilkan atau dibangun oleh satu elemen. Misalkan a sebagai elemen pembangun dari suatu grup siklik maka grup siklik tersebut dapat dinotasikan dengan $[a]$.

Contoh:

Misalkan perkalian bilangan bulat yang dibangun oleh 1 karena $1 \cdot 1 = 1$, $2 \cdot 1 = 2$, $3 \cdot 1 = 3$, ..., $n \cdot 1 = n$. Jadi $[1]$ adalah grup siklik.

Teorema 2.2.9 (Teorema Lagrange)

Order suatu subgrup dari suatu grup berhingga harus membagi order dari grup tersebut.

Akibat 2.2.10

Order satu elemen dari suatu grup berhingga harus membagi order dari grup tersebut.

2.3 Ring Polinomial

Definisi 2.3.1

Misalkan R ring, maka polinomial $f(x)$ dengan koefisien tak hingga dalam R dapat ditulis sebagai:

$$f(x) = \left(\sum_{i=0}^{\infty} a_i x^i \right), \text{ dengan } a_i = 0 \text{ dan } a_i \in R.$$

Jika $f(x) = a_0 x^0 + a_1 x^1 + a_2 x^2 + \dots$ polinomial atas ring R sedemikian sehingga $a_n \neq 0$ dan $a_i = 0 \forall i > n$, maka polinomial tersebut dikatakan polinomial berderajat n dan ditulis $\deg(f(x)) = n$.

Derajat dari suatu polinomial nol tidak didefinisikan. Suatu polinomial dikatakan konstan jika polinomial tersebut mempunyai $\deg 0$.

Definisi 2.3.2

$$\text{Misalkan } f(x) = \sum_{i=0}^p a_i x^i = a_0 x^0 + a_1 x^1 + a_2 x^2 + \dots + a_p x^p$$

$$\text{dan } g(x) = \sum_{i=0}^q b_i x^i = b_0 x^0 + b_1 x^1 + b_2 x^2 + \dots + b_q x^q$$

adalah dua polinomial di $R[x]$ maka $f(x) = g(x)$ jika $a_i = b_i, i \geq 0$.

Definisi 2.3.3

$$\text{Misalkan } f(x) = \sum_{i=0}^p a_i x^i = a_0 x^0 + a_1 x^1 + a_2 x^2 + \dots + a_p x^p$$

dan
$$g(x) = \sum_{i=0}^q b_i x^i = b_0 x^0 + b_1 x^1 + b_2 x^2 + \dots + b_q x^q$$

termuat dalam $R[x]$ maka dapat didefinisikan :

(i)
$$f(x) + g(x) = \sum_{i=0}^k (a_i + b_i) x^i, \text{ dengan } k = \max\{p, q\}$$

(ii)
$$f(x)g(x) = \sum_{i=0}^{p+q} c_i x^i, \text{ dengan } c_i = \sum_{j=0}^i a_j b_{i-j}$$

Contoh

Misalkan $f(x) = 3 + 2x$ dan $g(x) = 2 - 4x + x^2$

Maka didapat $a_0 = 3, a_1 = 2, a_2 = 0, a_3 = a_4 = \dots = 0$

$$b_0 = 2, b_1 = -4, b_2 = 1, b_3 = b_4 = \dots = 0$$

Untuk operasi penjumlahan

$$\begin{aligned} f(x) + g(x) &= \sum_{i=0}^2 (a_i + b_i) x^i \\ &= (a_0 + b_0) x^0 + (a_1 + b_1) x^1 + (a_2 + b_2) x^2 \\ &= (3 + 2) + (2 - 4)x + (0 + 1)x^2 \\ &= 5 - 2x + x^2 \end{aligned}$$

Untuk operasi penggandaan

$$f(x)g(x) = \sum_{i=0}^3 c_i x^i$$

dengan

$$c_0 = a_0 b_0 = 3 \cdot 2 = 6$$

$$c_1 = a_0 b_1 + a_1 b_0 = 3 \cdot (-4) + 2 \cdot 2 = -8$$

$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 = 3 \cdot 1 + 2 \cdot (-4) + 0 \cdot 2 = -5$$

$$c_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 = 3.0 + 2.1 + 0.(-4) + 0.2 = 2$$

$$c_4 = a_0 b_4 + a_1 b_3 + a_2 b_2 + a_3 b_1 + a_4 b_0 = 3.0 + 2.0 + 0.1 + 0.(-4) + 0.2 = 0$$

$$c_5 = c_6 = \dots = 0$$

$$\text{maka } f(x)g(x) = c_0 + c_1 x^1 + c_2 x^2 + c_3 x^3$$

$$= 6 - 8x - 5x^2 + 2x^3$$

Teorema 2.3.4

Jika R ring komutatif dengan elemen satuan maka $R[x]$ adalah ring komutatif dengan elemen satuan.

Teorema 2.3.5

Untuk setiap R ring komutatif dengan elemen satuan maka polinomial ring $R[x]$ memuat subring R' yang isomorfis terhadap R .

Bukti:

Misalkan $R' \in R[x]$, maka untuk ax^0 dan bx^0 elemen sebarang dalam R' berlaku : $ax^0 - bx^0 = (a - b)x^0$ dan $(ax^0)(bx^0) = (ab)x^0$ sedemikian sehingga R' merupakan subring dari $R[x]$. Jika $\phi(a) = ax^0$, untuk setiap $a \in R$ maka menurut definisi 2.1.8 diperoleh:

$$\phi(a) = \phi(b) \Leftrightarrow ax^0 = bx^0 \Leftrightarrow a = b$$

$$\phi(a + b) = (a + b)x^0 = ax^0 + bx^0 = \phi(a) + \phi(b)$$

$$\phi(ab) = (ab)x^0 = (ax^0)(bx^0) = \phi(a) \phi(b)$$

Jadi R' isomorfis terhadap R .



2.4 Faktorisasi Polinomial

Teorema 2.4.1

Misalkan $f(x) = a_0 + a_1 x + \dots + a_{p-1} x^{p-1} + a_p x^p$

$$g(x) = b_0 + b_1 x + \dots + b_{q-1} x^{q-1} + b_q x^q$$

adalah dua elemen dalam $F[x]$, dengan a_p dan b_q elemen – elemen tak nol di F dan $q > 0$, maka terdapat polinomial tunggal (unique polinomial) $s(x)$ dan $r(x)$ dalam $F[x]$ sedemikian sehingga $f(x) = g(x)s(x) + r(x)$, dimana $\deg r(x) < \deg g(x)$.

Bukti:

Misalkan $S = \{f(x) - g(x)s(x) \mid s(x) \in F[x]\}$. Ambil $r(x)$ sebagai derajat paling kecil dalam S , maka $f(x) = g(x)s(x) + r(x)$, untuk $s(x) \in F[x]$. Ambil m sebagai $\deg g(x)$, sehingga $\deg r(x) < m$. Maka

$$r(x) = c_t x^t + c_{t-1} x^{t-1} + \dots + c_0, \text{ dimana } c_j \in F \text{ dan } c_t \neq 0.$$

Andaikan $t \geq m$, maka :

$$f(x) - g(x)s(x) - (c_t/b_m)x^{t-m} g(x) = r(x) - (c_t/b_m)x^{t-m} g(x)$$

$$f(x) - g(x)[s(x) - (c_t/b_m)x^{t-m}] = r(x) - (c_t/b_m)x^{t-m} g(x)$$

Karena $r(x) - c_t x^t + c_{t-1} x^{t-1} - \dots$ memiliki derajat polinomial yang lebih kecil dari t , maka didapat bahwa $f(x) - g(x)[s(x) - (c_t/b_m)x^{t-m}]$ juga berada didalam S . Sehingga terjadi kontradiksi, maka pengandaian harus diingkar.

Yang benar adalah $\deg r(x) < \deg g(x)$. Untuk sifat ketunggalannya, jika :

$f(x) = g(x)s_1(x) + r_1(x)$ dan $f(x) = g(x)s_2(x) + r_2(x)$. Karena derajat dari $r_1(x) = r_2(x)$ lebih kecil dari derajat $g(x)$ maka harus dipenuhi $s_1(x) - s_2(x) = 0$ atau $s_1(x) = s_2(x)$



Akibat 2.4.2

$a \in F$ adalah akar dari $f(x) \in F[x]$ jika dan hanya jika $(x - a)$ adalah faktor dari $f(x)$ di $F[x]$.

Akibat 2.4.3

Suatu polinomial tak nol $f(x) \in F[x]$ yang mempunyai derajat n , paling banyak memiliki n akar di F .

Contoh:

Misalkan $f(x) = 4x^3 + 3x - 2$ dan $g(x) = 2x^2 + 4x + 6$ adalah dua polinomial tak nol dari lapangan R . Akan dibuktikan dengan menggunakan algoritma pembagi (division algorithm).

$$\begin{array}{r}
 x - \frac{1}{4} \\
 4x^2 + 4x - 3 \overline{) 4x^3 + 3x^2 - 6} \\
 \underline{4x^3 + 4x^2 - 3x} \\
 -x^2 + 3x - 6 \\
 \underline{-x^2 - x + \frac{3}{4}} \\
 4x - \frac{27}{4}
 \end{array}$$

maka diperoleh bentuk $f(x) = g(x)s(x) + r(x)$

$$4x^3 + 3x^2 - 6 = (4x^2 + 4x - 3) \left(x - \frac{1}{4} \right) + \left(4x - \frac{27}{4} \right)$$

$$\text{dimana } s(x) = \left(x - \frac{1}{4} \right) \text{ dan } r(x) = \left(4x - \frac{27}{4} \right)$$

karena $\deg r(x) = 1$ maka didapat bahwa $\deg r(x) < \deg g(x)$.

Teorema 2.4.4

Jika R adalah daerah integral, $f(x)$ dan $g(x)$ adalah dua polinomial tidak nol dalam $R[x]$ maka:

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

dengan $\deg f(x) \leq \deg (f(x)g(x))$ dan $\deg g(x) \leq \deg (f(x)g(x))$.

Bukti:

Misalkan R daerah integral.

$f(x) = \sum_{i=0}^p a_i x^i$ berderajat p dan $g(x) = \sum_{i=0}^q b_i x^i$ berderajat q , keduanya berada

dalam $R[x]$ maka masing-masing mempunyai koefisien pemimpin a_p dan b_q .

Karena a_p dan $b_q \in F$ dan F adalah suatu lapangan maka F juga suatu daerah

integral sehingga $a_p b_q \neq 0$, sedemikian sehingga koefisien pemimpin dari $f(x)g(x)$

adalah $a_p b_q$. Karena $f(x)g(x) = \sum_{i=0}^{p+q} \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i$ dan dari definisi 2.3.3 sehingga

$$\deg (f(x)g(x)) = p + q = \deg f(x) + \deg g(x).$$

Definisi 2.4.5

Misalkan R adalah ring komutatif dan f adalah suatu polinomial atas R .

Suatu elemen $\alpha \in R$ disebut polinomial nol dari f jika $f(\alpha) = 0$.

Lemma 2.4.6

Jika F adalah suatu lapangan, f merupakan polinomial tidak tereduksi atas

F , dan g, h , adalah polinomial atas F sedemikian sehingga f membagi $g.h$ oleh

karena itu, f membagi g atau f membagi h .

Bukti:

Misalkan f bukan pembagi g dan anggap bahwa f adalah bilangan prima terhadap g . Jika terdapat d sebagai faktor persekutuan terbesar atas f dan g , sedangkan f tidak tereduksi dan $d|f$ maka $d = kf$ atau $d = k$, untuk $k \in F$. Hal ini bertentangan dengan hipotesis diatas, sehingga $f|g$. Oleh karena 1 juga merupakan faktor persekutuan terbesar atas f dan g maka f merupakan bilangan prima terhadap g (coprime). Dengan demikian terdapat polinomial a dan b atas F , sehingga :

$$1 = af + bg$$

Jika dikalikan dengan h didapat $h = haf + hbg$. Karena $f|gh$ maka $f|haf$ dan $f|hbg$ sedemikian sehingga $f|h$.

Definisi 2.4.7

Misalkan E lapangan perluasan dari F dan $\alpha \in E$ sebagai elemen aljabar atas F . Maka α dikatakan polinomial minimal jika α merupakan derajat terkecil dari suatu polinomial monic. Dan jika derajat polinomial minimal dari α atas F adalah n maka α disebut suatu elemen aljabar atas F dengan derajat n .

Teorema 2.4.8

Jumlah polinomial nol dari suatu lapangan, dihitung sesuai dengan keserbaragamannya, yaitu kurang dari atau sama dengan derajat polinomialnya.