BAB 2

LANDASAN TEORI

Pada bab ini dibahas landasan teori yang akan digunakan untuk menentukan ciri-ciri dari polinomial permutasi atas *finite field*.

Hal ini dimulai dengan memberikan pengertian dari *group* beserta sifat-sifatnya.

Definisi 2.1

Suatu himpunan tak kosong G dengan operasi $*$, dinotasikan dengan $(G,*)$, disebut *group* apabila memenuhi sifat berikut:

a) $a, b \in G$ mengakibatkan $a * b \in G$.
b) $(a * b) * c = a * (b * c)$ untuk $a, b, c \in G$.
c) Terdapat $\boldsymbol{e} \in G$ sedemikian sehingga $a * \boldsymbol{e} = \boldsymbol{e} * a = a$, untuk setiap $a \in G$. $\boldsymbol{e}$ merupakan elemen identitas pada G.
d) Untuk setiap $a \in G$, terdapat $b \in G$ sedemikian sehingga $a * b = b * a = \boldsymbol{e}$, b biasa dinotasikan dengan $-a$.

(Herstein, *Abstract* 41)

Untuk penyederhanaan tulisan, selanjutnya $(G,*)$ akan ditulis sebagai G saja.

Selanjutnya akan ditampilkan beberapa penamaan atau istilah dari *group* yang berkaitan dengan sifat yang dimiliki oleh anggota *group*.

Definisi 2.2

a) *Finite group* merupakan *group* dengan banyak anggotanya berhingga (Herstein, *Abstract* 42).

b) Untuk G *finite group*, banyaknya anggota G disebut *order* G (Herstein, *Abstract* 42).

c) *Abelian group* merupakan *group* yang memenuhi sifat $a * b = b * a$ untuk setiap a, b anggota *group* (Herstein, *Abstract* 43).

d) Misalkan G suatu *finite group*. $a \in G$. Bilangan bulat positif terkecil m sedemikian sehingga $a^m = \boldsymbol{e}$ disebut *order* a (Herstein, *Abstract* 60).

Berkaitan dengan definisi *finite group* diperoleh teorema berikut.

Teorema 2.3

Misalkan G merupakan *finite group* dengan *order* n, $n \in \mathbb{N}$, maka $a^n = \boldsymbol{e}$, untuk setiap $a \in G$ (Herstein, *Abstract* 60).

Berikut ini diberikan pengertian dari suatu *group* dengan bentuk khusus.

Definisi 2.4

Misalkan G suatu *group*. G disebut *cyclic group* jika terdapat sebuah anggota G, misalkan a, sedemikian sehingga untuk setiap $m \in G$ dapat dinyatakan sebagai $m = a^i$, untuk suatu bilangan bulat i.

Akibat dari Definisi 2.4 diperoleh bahwa *order* dari a adalah banyaknya anggota G dan a disebut *generator* G (Herstein, *Abstract* 55).

Berkaitan dengan sifat dari *cyclic group* diperoleh Lemma 2.5.

Lemma 2.5

Cyclic group merupakan *abelian group* (Herstein, *Abstract* 55).

Suatu *finite abelian group* dapat dikaitkan dengan bilangan prima yang membagi *order group* tersebut. Hal ini ditunjukkan oleh teorema berikut.

Teorema 2.6

Misalkan G adalah suatu *finite abelian group* dan p adalah bilangan prima yang membagi *order* G, maka terdapat suatu anggota G, sebut $a \neq \boldsymbol{e}$, sedemikian sehingga *order a* adalah p (Herstein, *Abstract* 80).

Sebelumnya telah dibahas bahwa *group* adalah suatu struktur aljabar dengan satu operasi, berikut ini akan dibahas suatu struktur aljabar dengan dua operasi yang dikenal dengan sebutan *ring*.

Definisi 2.7

Suatu himpunan tak kosong R dengan operasi $+$ dan $\cdot$, dinotasikan dengan $(R, +, \cdot)$, disebut *ring* apabila memenuhi sifat berikut:

a) $(R, +)$ merupakan *abelian group* dengan elemen identitas $\mathbf{0}$.
b) $a, b \in R$ mengakibatkan $a \cdot b \in R$.
c) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ untuk $a, b, c \in R$.
d) $a \cdot (b + c) = a \cdot b + a \cdot c$ dan $(b + c) \cdot a = b \cdot a + c \cdot a$ untuk $a, b, c \in R$.

(Herstein, *Abstract* 126)

Untuk pembahasan selanjutnya $(R, +, \cdot)$ ditulis sebagai R saja dan $a \cdot b$ ditulis ab saja.

Sifat dari operasi perkalian pada *ring* berkaitan dengan elemen identitas terhadap operasi penjumlahan diberikan pada Lemma 2.8.

Lemma 2.8

Misalkan R suatu *ring* dan $a \in R$. Maka $a\mathbf{0} = \mathbf{0}a = \mathbf{0}$ (Herstein, *Abstract* 137).

Istilah-istilah berikut berkaitan dengan *ring* beserta sifat yang dimilikinya.

Definisi 2.9

Misalkan R suatu *ring* dan $u \in R$. u disebut elemen *unit* dari R jika untuk setiap $v \in R$ berlaku $uv = vu = v$.

Untuk selanjutnya, elemen *unit* dinotasikan dengan **1**.

Definisi 2.10

a) Misalkan R suatu *ring*. R disebut *commutative ring* jika berlaku $ab = ba$, untuk $a, b \in R$.
b) Suatu *commutative ring* R disebut *integral domain* jika $ab = \mathbf{0}$ mengakibatkan $a = \mathbf{0}$ atau $b = \mathbf{0}$, untuk $a, b \in R$.
c) Suatu *ring* R dengan elemen *unit* **1** disebut *division ring* jika untuk setiap $a \neq \mathbf{0} \in R$ terdapat $b \in R$ sedemikian sehingga $ab = ba = \mathbf{1}$, dengan b biasa dinotasikan a^{-1}.

(Herstein, *Abstract* 127).

Berdasarkan pengertian *ring* dan sifat-sifat yang berlaku pada *ring*, diperoleh pengertian dari *field* berikut ini.

Definisi 2.11

Suatu *ring* R disebut *field* jika R merupakan *commutative division ring* (Herstein, *Abstract* 127).

Selanjutnya diberikan hubungan antara suatu *field* dengan suatu *integral domain.*

Teorema 2.12

Suatu *field* F merupakan *integral domain* (Herstein, *Abstract* 133).

Suatu *field* yang mempunyai sejumlah berhingga anggota dinamakan *finite field* atau yang dikenal juga sebagai Galois *field*. Suatu *finite field* dengan banyaknya anggota q dinotasikan dengan $GF(q)$.

Pada *field* dikenal suatu istilah karakteristik yang pengertiannya diberikan oleh definisi berikut.

Definisi 2.13

Misalkan F suatu *field*. F memiliki karakteristik $p \neq 0$ jika p merupakan bilangan bulat positif terkecil dimana berlaku $px = \mathbf{0}$, untuk setiap $x \in F$ (Herstein, *Abstract* 178).

Berkaitan dengan karakteristik dari suatu *field* dan jumlah anggotanya diperoleh teorema berikut.

Teorema 2.14

Misalkan F suatu *finite field*. Maka F memiliki p^m anggota, dimana bilangan prima p merupakan karakteristik dari F, untuk suatu bilangan asli m (Herstein, *Topics* 357).

Terdapat suatu sifat dari operasi penjumlahan anggota dari suatu *field* apabila dipangkatkan dengan karakteristik dari *field* yang memuatnya.

Teorema 2.15

Misalkan F suatu *field* dengan karakteristik bilangan prima p. Untuk $a, b \in F$ berlaku:

$(a+b)^p = a^p + b^p$

(Koblitz 58)

Berikut ini diberikan teorema yang menghubungkan suatu *finite field* dengan *cyclic group*.

Teorema 2.16

Misalkan F suatu *finite field*. $F - \{\mathbf{0}\}$ merupakan *cyclic group* terhadap operasi perkalian pada F (Lidl and Pilz 138).

Berdasarkan Teorema 2.16 diperoleh bahwa untuk *finite field* F, $F - \{\mathbf{0}\}$ merupakan *cyclic group*. Sesuai dengan definisi *cyclic group*, diperoleh bahwa $F - \{\mathbf{0}\}$ mempunyai paling sedikit satu *generator*.

Definisi 2.17

Misalkan F suatu *finite field*. *Generator* dari *cyclic group* $F - \{\mathbf{0}\}$ disebut elemen *primitive* dari F (Lidl and Pilz 139).

Sebelum membahas sifat-sifat dari elemen *primitive* suatu *finite field* lebih lanjut, diperlukan Definisi 2.18 yang berkaitan dengan sifat bilangan bulat yaitu apabila diberikan dua buah bilangan bulat maka dapat ditentukan suatu bilangan yang merupakan *greatest common divisor* (*gcd*) dari dua buah bilangan bulat tersebut.

Definisi 2.18

Diberikan dua buah bilangan bulat a, b, tidak keduanya nol, maka *greatest common divisor* (*gcd*) dari a dan b adalah c jika dipenuhi:

a) $c > 0$
b) c membagi a dan c membagi b.
c) Jika d membagi a dan d membagi b maka d membagi c.

(Herstein, *Abstract* 23)

Berkaitan dengan Teorema 2.16 dan Definisi 2.17 diperoleh teorema berikut.

Teorema 2.19

Misalkan α adalah elemen *primitive* dari *finite field* $GF(q)$ dengan banyak anggota q, $q \in \mathbb{N}$. Maka:

a) $F = \{\mathbf{0}, \mathbf{1}, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{q-2}\}$.
b) $\alpha^{q-1} = \mathbf{1}$.

c) α^k juga merupakan elemen *primitive* jika dan hanya jika $gcd(k, q-1) = 1$.

(Lidl and Pilz 139)

Jumlah dari pangkat masing-masing anggota *field* dapat dibatasi menjadi dua kemungkinan nilai saja. Hal ini diberikan pada Lemma 2.20.

Lemma 2.20

Misalkan $GF(q)$ suatu *finite field* dengan banyak anggota q, $q \in \mathbb{N}$, dan $a_0, a_1, \ldots, a_{q-1} \in GF(q)$. Maka

a) $\sum_{i=0}^{q-1} {a_i}^t = \mathbf{0}$, untuk $1 \leq t \leq q-2$.
b) $\sum_{i=0}^{q-1} {a_i}^t = -\mathbf{1}$, untuk $t = q-1$.

(Lidl and Pilz 150).

Salah satu contoh dari *finite field* adalah $\mathbb{Z}_n$, n bilangan prima. Berikut ini diberikan definisinya.

Definisi 2.21

Untuk $a, b \in \mathbb{Z}$, n tertentu di $\mathbb{Z}$, $n > 1$

a) Didefinisikan suatu relasi ekivalen kongruen modulo n pada himpunan bilangan bulat $\mathbb{Z}$. a kongruen modulo n ke b, dinotasikan dengan $a \equiv b \bmod n$, jika n membagi $(a-b)$.
b) Kumpulan semua bilangan bulat yang mempunyai sisa a jika dibagi oleh n disebut kelas ekivalen dari a dan dinotasikan dengan $[a]_n$. $[a]_n = \{b | b = a + nk, k \in \mathbb{Z}\}$.

c) Definisikan $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\}$.

d) Didefinisikan dua buah operasi pada $\mathbb{Z}_n$, operasi $+$ dan $\cdot$ yaitu untuk sembarang $[a]_n, [b]_n \in \mathbb{Z}_n$, $[a]_n + [b]_n = [a \circ b]_n$ dan $[a]_n \cdot [b]_n = [a * b]_n$, dimana $\circ$ merupakan operasi penjumlahan pada bilangan bulat dan $*$ merupakan operasi perkalian pada bilangan bulat.

(Herstein, *Abstract* 60-61)

Berkaitan dengan definisi $\mathbb{Z}_n$, diperoleh Lemma 2.22.

Lemma 2.22

Untuk setiap $[a]_n, [b]_n \in \mathbb{Z}_n$, $[a]_n = [b]_n$ jika dan hanya jika n membagi $(a - b)$ (Herstein, *Abstract* 61).

$\mathbb{Z}_n$ merupakan salah satu contoh *field*, namun hal ini tidak berlaku apabila n bukan bilangan prima.

Teorema 2.23

$\mathbb{Z}_n$ merupakan *field* jika dan hanya jika n merupakan bilangan prima (Herstein, *Abstract* 133).

Berikut ini akan dibahas mengenai definisi polinomial atas *finite field*.

Definisi 2.24

a) Pandang F suatu *field* dan $x \in X \subseteq F$, suatu ekspresi formal $p(x) = \sum_{i=0}^{n} a_i x^i$, $n \geq 0$, dinamakan polinomial dalam x.

b) Jika a_i, $i = 0,1,2,\dots,n$, koefisien dari polinomial $p(x)$ merupakan anggota F maka $p(x)$ disebut polinomial dalam x atas F.

Kumpulan semua polinomial dalam x atas F dinotasikan dengan $F[x]$.

Berikut ini akan didefinisikan suatu anggota *field* dengan sifat khusus.

Definisi 2.25

Misalkan F suatu *field*. $x^n - \mathbf{1} \in F[x]$.

a) Nilai $\alpha \in F$ yang memenuhi $x^n - \mathbf{1} = \mathbf{0}$ disebut *nth root of unity*.
b) *Order* dari suatu *nth root of unity* α adalah bilangan bulat positif terkecil k sedemikian sehingga $\alpha^k = \mathbf{1}$.
c) Suatu *nth root of unity* yang memiliki order n disebut *primitive nth root of unity*.

(Lidl and Pilz 144)

Definisi 2.26 dan Definisi 2.27 diperlukan untuk pendefinisian suatu jenis polinomial yang akan diberikan pada Definisi 2.28.

Definisi 2.26

a) Misalkan M suatu *field* dan F himpunan bagian dari M. F disebut *subfield* dari M jika F merupakan *field* dengan operasi yang berlaku di M.
b) Misalkan α anggota *field* M dan F *subfield* M. $F(\alpha)$ merupakan irisan dari semua *subfield* dari M yang mengandung F dan α (Lidl and Pilz 129).

Definisi 2.27

Fungsi Euler $\varphi(n)$ didefinisikan dengan $\varphi(1) = 1$, dan untuk $n > 1 \in \mathbb{N}, \varphi(n)$ adalah banyaknya bilangan bulat positif m dengan $1 \leq m < n$ sedemikian sehingga m dan n saling relatif prima yaitu $gcd(m, n) = 1$ (Herstein, *Abstract* 62).

Berikut ini diberikan definisi dari suatu polinomial yang berkaitan dengan *nth root of unity*. Pada bab 3 akan dibahas ciri-ciri dari polinomial tersebut sehingga menjadi polinomial permutasi atas *finite field*.

Definisi 2.28

Misalkan n adalah suatu bilangan bulat positif dan F suatu *field* yang karakteristiknya tidak membagi n. Misalkan α merupakan *primitive nth root of unity* dan $\varphi(n)$ merupakan Fungsi Euler. Polinomial

$$Q_n \coloneqq (x - \alpha_1) \dots (x - \alpha_{\varphi(n)}) \in F(\alpha)[x]$$

dengan $\alpha_1, \alpha_2, \dots, \alpha_{\varphi(n)}$ adalah *primitive nth root of unity* pada $F(\alpha)$, disebut *nth cyclotomic polynomial* atas F (Lidl and Pilz 145).

Berikut beberapa teorema yang berkaitan dengan *cyclotomic polynomial*.

Teorema 2.29

Misalkan Q_n merupakan *nth cyclotomic polynomial* atas *field* F yang karakteristiknya bukan p.

Jika p prima dan p tidak membagi m, maka

a) $Q_{mp^k} = Q_{pm} \circ (x^{p^{k-1}})$

b) $Q_{pm} = \frac{Q_m \circ (x^p)}{Q_m}$

(Lidl and Pilz 151)

Teorema 2.30

Misalkan p prima dan Q_n merupakan *nth cyclotomic polynomial* atas *field F* yang karakteristiknya bukan p. Misalkan pula m bilangan bulat positif. Maka

a) $Q_{p^m} = \mathbf{1} + x^{p^{m-1}} + \cdots + x^{(p-1)p^{m-1}}$

b) $Q_{p^m} = \frac{x^{p^m}-\mathbf{1}}{x^{p^{m-1}}-\mathbf{1}}$

(Lidl and Pilz 146)

Pada Definisi 2.18 diberikan definisi dari gcd dari dua buah bilangan bulat. Teorema 2.31 berikut ini berisi jaminan bahwa gcd dari dua bilangan dapat dinyatakan sebagai kombinasi linier dari dua bilangan tersebut.

Teorema 2.31

Jika a, b merupakan bilangan bulat yang tidak keduanya 0, maka terdapat tepat satu *greatest common divisor* (*gcd*) dari a dan b, misal c, dimana $c = ma + nb$, untuk suatu bilangan bulat m dan n (Herstein, *Abstract* 23).

Karena pada tulisan ini akan dibahas ciri-ciri polinomial permutasi atas *finite field* yang membutuhkan fungsi satu-satu, maka berikut ini diberikan *lemma* mengenai sifat dari komposisi fungsi satu-satu.

Lemma 2.32

Jika $g: S \to T$ dan $f: T \to U$ merupakan fungsi satu-satu maka $f \circ g: S \to U$ juga fungsi satu-satu (Herstein, *Abstract* 12).

Teorema 2.33 berisikan jaminan bahwa setiap bilangan asli yang lebih dari satu dapat dinyatakan sebagai perkalian dari pangkat bilangan prima.

Teorema 2.33

Diberikan $n \in \mathbb{Z}, n > 1$. Maka terdapat tepat satu cara untuk menyatakan n dalam bentuk $n = {p_1}^{a_1} {p_2}^{a_2} \dots {p_k}^{a_k}$, dengan $p_1 < p_2 < p_3 \dots < p_k$ bilangan-bilangan prima, dan $a_1, a_2, \dots, a_k$ bilangan bulat positif (Herstein, *Abstract* 27).

Teorema 2.34 menerangkan bentuk dari koefisien penjumlahan anggota *commutative ring* apabila dipangkatkan dengan bilangan bulat nonnegatif.

Teorema 2.34

Jika x, y anggota *commutative ring* dan n bilangan bulat nonnegatif. Maka

$$(x + y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$$

(Rotman 118)