BAB II
LANDASAN TEORI

Pada bab ini akan dibahas mengenai definisi suatu *ring* serta beberapa sifat yang diperlukan dalam pembahasan polinomial permutasi.

Penjelasan mengenai *ring* dimulai dengan definisi dari suatu sistem matematika.

Definisi 2.1

Jika R suatu himpunan tak kosong dan terdapat suatu pemetaan $\bullet : R \times R \to R$, maka $(R,\bullet)$ disebut ***sistem matematika.***

Jika pada R didefinisikan dua operasi $+$ dan $\bullet$ maka ditulis $(R,+,\bullet)$.

(Achmad Arifin, 2001, halaman 1)

Definisi 2.2

Suatu sistem matematika $(R,\bullet)$ disebut **grup** jika :

a. memenuhi sifat asosiatif, yaitu untuk setiap $x,y,z \in R$ berlaku $x \bullet (y \bullet z) = (x \bullet y) \bullet z$.

b. memiliki elemen identitas, dinotasikan sebagai e, sedemikian sehingga berlaku $x \bullet e = e \bullet x = x$ untuk setiap $x \in R$.

c. memiliki invers untuk setiap $x \in R$, dinotasikan sebagai x^{-1}, sedemikian sehingga berlaku $x \bullet x^{-1} = x^{-1} \bullet x = e$.

(I. N. Herstein, 1996, halaman 41)

Definisi 2.3

Suatu grup $(R,\bullet)$ yang memiliki sifat untuk setiap $x,y \in R$ berlaku $x \bullet y = y \bullet x$ disebut **grup *abelian*** atau **komutatif**.

(I. N. Herstein, 1996, halaman 43)

Bermula dari definisi grup yang menggunakan satu buah operasi, selanjutnya akan dibahas suatu sistem matematika dengan dua buah operasi yang disebut sebagai *ring* beserta sifat-sifatnya.

Definisi 2.4

Sistem matematika $(R,+,\bullet)$ disebut ***ring*** jika memenuhi :

a. $(R,+)$ merupakan grup komutatif.

b. $(R,\bullet)$ memenuhi sifat asosiatif, yaitu $x \bullet (y \bullet z) = (x \bullet y) \bullet z$ untuk setiap $x,y,z \in R$.

c. $(R,+,\bullet)$ memenuhi sifat distributif, yaitu $x \bullet (y+z) = x \bullet y + x \bullet z$ dan $(y+z) \bullet x = y \bullet x + z \bullet x$ untuk setiap $x,y,z \in R$.

(I. N. Herstein, 1996, halaman 126)

Ring dapat dibedakan menjadi dua jenis berdasarkan banyak elemennya, yaitu *ring* tak hingga dan *ring* hingga. ***Ring* tak hingga** adalah *ring* yang memiliki tak berhingga elemen sedangkan ***ring* hingga** adalah *ring* yang memiliki sejumlah berhingga elemen.

Contoh dari *ring* tak hingga adalah himpunan bilangan bulat dengan operasi penjumlahan dan perkalian umum pada bilangan bulat, dinotasikan $(\mathbb{Z},+,\times)$.

Sedangkan untuk memberikan contoh dari *ring* hingga, terlebih dahulu akan diberikan definisi mengenai kelas modulo.

Definisi 2.5

Kumpulan semua bilangan bulat yang mempunyai sisa *a* jika dibagi *n* disebut kelas dari *a* modulo *n*, dinotasikan sebagai $[a]_n$.

$[a]_n = \{a + nk \mid k \in \mathbb{Z}\}$.

(Alexander Bogomolny, 1996)

Sifat yang berlaku pada kelas modulo *n* dijelaskan pada sifat di bawah ini.

Sifat 2.6

$[a]_n$ dan $[b]_n$ dikatakan ekivalen, dinotasikan $\left[a\right]_n = \left[b\right]_n$, jika dan hanya jika n habis membagi $a-b$, atau terdapat suatu bilangan bulat k sedemikian sehingga $a-b=nk$.

Bukti :

$(\Rightarrow)$ Diketahui $\left[a\right]_n = \left[b\right]_n$, maka akan ditunjukkan terdapat suatu bilangan bulat k sedemikian sehingga $a-b=nk$.

$\left[a\right]_n = \left[b\right]_n$ berarti untuk setiap c, c di $[a]_n$ maka c juga di $[b]_n$.

Dengan memandang c di $[a]_n$, c dapat dinyatakan sebagai

$c = a + nl$, untuk suatu bilangan bulat l. (2.1)

Tetapi jika memandang c di $[b]_n$, c dinyatakan sebagai

$c = b + nl'$, untuk suatu bilangan bulat l'. (2.2)

Dari persamaan (2.1) dan (2.2) diperoleh

$a - b = nl' - nl$, atau

$a - b = nk$, untuk suatu bilangan bulat $k = l' - l$.

Jadi, terbukti jika diketahui $\left[a\right]_n = \left[b\right]_n$ maka terdapat suatu bilangan bulat k sedemikian sehingga $a-b=nk$.

$(\Leftarrow)$ Diketahui $a-b=nk$, untuk suatu bilangan bulat k, maka akan ditunjukkan $\left[a\right]_n = \left[b\right]_n$.

$$[a]_n = \{a + nl \mid l \in \mathbb{Z}\}$$

$$= \{(b + nk) + nl \mid l \in \mathbb{Z}\}$$, untuk suatu bilangan bulat k

$$= \{b + n(k + l) \mid l \in \mathbb{Z}\}$$

$$= \{b + nk' \mid k' \in \mathbb{Z}\}$$, dengan $k' = k + l$

$$= [b]_n .$$

Sehingga terbukti bahwa $[a]_n = [b]_n$.

Dengan demikian Sifat 2.6 terbukti. ■

Sekarang pandang $\mathbb{Z}_n = \{ [a]_n \mid a \in \mathbb{Z} \}$ yaitu kumpulan bilangan bulat modulo n, $n \in \mathbb{Z}$, $n \geq 1$ dengan operasi :

$+ : [a]_n + [b]_n = [a + b]_n$

$\bullet : [a]_n \bullet [b]_n = [ab]_n$.

Kemudian akan ditunjukkan bahwa operasi $+$ dan $\bullet$ di $\mathbb{Z}_n$ terdefinisi dengan baik, yaitu dengan menunjukkan jika $[a]_n = [a']_n$ dan $[b]_n = [b']_n$ maka $[a + b]_n = [a' + b']_n$ dan $[ab]_n = [a'b']_n$.

Untuk $[a]_n = [a']_n$ maka n habis membagi $a - a'$. Sedangkan untuk $[b]_n = [b']_n$ maka n juga habis membagi $b - b'$.

Karena

$$(a+b)-(a'+b')=(a-a')+(b-b'),$$

dan n habis membagi $a-a'$ dan $b-b'$, maka n juga habis membagi $(a+b)-(a'+b')$ atau dapat dikatakan $[a+b]_n=[a'+b']_n$.

Begitu juga karena

$$(ab-a'b')=(a-a')b+a'(b-b'),$$

dan n habis membagi $a-a'$ dan $b-b'$ maka n juga habis membagi $(ab-a'b')$ atau dapat dikatakan $[ab]_n=[a'b']_n$.

Dengan demikian terbukti bahwa operasi $+$ dan $\bullet$ di $\mathbb{Z}_n$ terdefinisi dengan baik.

Sistem matematika $(\mathbb{Z}_n,+,\bullet)$ adalah *ring* karena memenuhi sifat-sifat berikut :

a. $(\mathbb{Z}_n,+)$ merupakan grup komutatif.

b. $(\mathbb{Z}_n,\bullet)$ memenuhi sifat asosiatif.

c. $(\mathbb{Z}_n,+,\bullet)$ memenuhi sifat distributif.

Karena himpunan $\mathbb{Z}_n$ berisi $\{[a]_n \mid a=0,...,n-1\}$, maka banyaknya elemen dari $\mathbb{Z}_n$ adalah *n* elemen.

Dengan demikian $(\mathbb{Z}_n,+,\bullet)$ merupakan suatu *ring* hingga.

Berikut akan diberikan sifat pada *ring* hingga $(\mathbb{Z}_n,+,\bullet)$ yang terkait dalam pembahasan mengenai polinomial permutasi di *ring* $\mathbb{Z}_n$.

Sifat 2.7

Jika $[a]_n$ sembarang anggota di $\mathbb{Z}_n$ dan p sembarang bilangan bulat maka berlaku sifat berikut :

a. $p[a]_n = [pa]_n$

b. $([a]_n)^p = [a^p]_n$.

Bukti :

a. $$p[a]_n = \underbrace{[a]_n + [a]_n + [a]_n + ... + [a]_n}_{\text{sebanyak } p \text{ kali}}$$

$$= \left[\underbrace{a + a + a + ... + a}_{\text{sebanyak } p \text{ kali}}\right]_n$$

$$= [pa]_n .$$

b. $$([a]_n)^p = \underbrace{[a]_n \bullet [a]_n \bullet ... \bullet [a]_n}_{\text{sebanyak } p \text{ kali}}$$

$$= \left[\underbrace{a\ a\ ...\ a}_{\text{sebanyak } p \text{ kali}}\right]_n$$

$$= [a^p]_n .$$

Dengan demikian terbukti bahwa $p[a]_n = [pa]_n$ dan $([a]_n)^p = [a^p]_n$. ■

Sifat 2.8

Jika $[a]_n$ di $\mathbb{Z}_n$ dengan a,n bilangan genap positif dan $a = \frac{n}{2}$ maka berlaku dua hal berikut :

a. $p[a]_n = [0]_n$ untuk p bilangan genap, dan

b. $p[a]_n = [a]_n$ untuk p bilangan ganjil.

Bukti :

a. Berdasarkan Sifat 2.7, $p[a]_n = [pa]_n$, maka akan ditunjukkan $[pa]_n = [0]_n$ atau n habis membagi $pa - 0 = pa$.

Karena p merupakan bilangan genap maka p dapat dinyatakan sebagai $p = 2k$ untuk suatu bilangan bulat k. Sehingga $pa = (2k)\left(\frac{n}{2}\right) = nk$.

Dengan demikian n habis membagi pa.

b. Analog dengan pembuktian bagian a, dengan demikian akan ditunjukkan $[pa]_n = [a]_n$ atau n habis membagi $pa - a = (p-1)a$.

Karena p merupakan bilangan ganjil maka p dapat dinyatakan sebagai $p = 2k+1$ untuk suatu bilangan bulat k, sehingga $p - 1 = 2k$. Sehingga $(p-1)a = (2k)\left(\frac{n}{2}\right) = nk$. Dengan demikian n habis membagi $(p-1)a$.

Jadi kedua sifat tersebut telah terbukti. ■