BAB 1

PENDAHULUAN

1.1 Latar Belakang

Finite field maupun polinomial atas *finite field* memiliki aplikasi yang cukup luas sehingga menarik untuk dibahas.

Aplikasi tersebut mencakup area seperti *coding theory*, *cryptography*, *combinatoric*, konstruksi dari *error-correcting codes* maupun teknologi terkini seperti telepon seluler CDMA (Blake et al. 1-4).

Area-area di atas sering melibatkan suatu polinomial atas *finite field* dengan sifat khusus yang disebut polinomial permutasi.

Polinomial f atas *finite field* $GF(q)$ merupakan polinomial permutasi jika pemetaan $f: GF(q) \to GF(q)$ adalah pemetaan satu-satu (Mollin and Small 535).

Suatu polinomial yang merupakan polinomial permutasi di suatu *finite field* belum tentu merupakan polinomial permutasi di *finite field* yang lain. Sebagai contoh, $f(x) = x^2$ merupakan polinomial permutasi pada $\mathbb{Z}_2$ karena $f([0]_2) = [0]_2$ dan $f([1]_2) = [1]_2$. Namun, $f(x) = x^2$ bukan polinomial permutasi pada $\mathbb{Z}_3$, karena $f([1]_3) = [1]_3 = f([2]_3)$.

Polinomial permutasi atas *finite field* memiliki beberapa aplikasi khusus seperti *modular enciphering* dan *Imai-Matsumoto system* yang berkaitan dengan *cryptosystem*, *latin square* berkaitan dengan *combinatoric*, maupun pembentukan *key* berkaitan dengan *cryptography* (Lidl and Pilz 243, 252, 398; Koblitz 80).

Untuk menentukan apakah suatu polinomial atas *finite field* merupakan polinomial permutasi dapat digunakan cara yang paling sederhana yaitu dengan mendaftarkan semua hasil peta fungsi polinomial tersebut, kemudian memeriksa apakah himpunan peta yang didapat memuat semua anggota *finite field*. Akan tetapi, hal ini sulit

dilakukan apabila jumlah anggota *finite field* besar. Karena itu, diperlukan suatu kriteria sederhana untuk memeriksa apakah suatu polinomial atas *finite field* merupakan polinomial permutasi atau bukan.

1.2 Permasalahan

Apa ciri-ciri dari suatu polinomial atas *finite field* sehingga polinomial tersebut merupakan polinomial permutasi?

1.3 Tujuan Penulisan

Menentukan ciri-ciri polinomial permutasi atas *finite field*.

1.4 Sistematika Penulisan

Tugas akhir ini terdiri dari empat bab yang dimulai dengan Bab 1 yang menerangkan secara garis besar isi dari tugas akhir ini. Bab 2 berisi landasan teori tentang *group*, *ring*, dan *field* yang akan digunakan pada pembahasan tugas akhir ini. Pembahasan tentang ciri-ciri suatu polinomial permutasi atas suatu *finite field* ditunjukkan pada Bab 3. Bab 4 berisi kesimpulan dari tugas akhir ini.