

ABSTRAK

Nama : Aini Suri Talita

Program Studi: Matematika

Judul : Ciri-ciri Polinomial Permutasi atas *Finite Field*

Polinomial atas *finite field* $GF(q)$ memiliki aplikasi yang cukup luas mencakup area seperti *coding theory*, *cryptography*, *combinatoric*, konstruksi dari *error-correcting codes* maupun teknologi terkini seperti telepon seluler CDMA. Area-area tersebut sering menggunakan suatu polinomial dengan sifat khusus yang disebut polinomial permutasi. Polinomial f atas *finite field* $GF(q)$ merupakan polinomial permutasi jika pemetaan $f: GF(q) \rightarrow GF(q)$ adalah pemetaan satu-satu. Pada tugas akhir ini akan dibahas ciri-ciri dari suatu polinomial atas *finite field* $GF(q)$ sehingga menjadi polinomial permutasi. Hingga saat ini, belum didapatkan suatu ciri-ciri umum yang berlaku untuk sembarang polinomial atas *finite field* sehingga polinomial tersebut menjadi polinomial permutasi. Akan tetapi, untuk beberapa polinomial telah didapatkan ciri-cirinya agar menjadi polinomial permutasi atas *finite field*.

Kata kunci:

Finite field, polinomial, polinomial permutasi