ABSTRAK

Misal F suatu lapangan berhingga dengan p elemen, yang dinotasikan dengan GF_p. Perluasan dari F yakni GF_{p^n} sangatlah penting, misalnya untuk mengkostruksi suatu rancangan percobaan (*block design*) dan mengkodekan pesan asli menjadi kode biner pada alat-alat pengirim pesan. Untuk mengkonstruksi GF_{p^n} dibutuhkan suatu polinomial yang disebut polinomial minimal.

Jika E lapangan perluasan atas F dan $\alpha \in E$ elemen aljabar atas F, maka $p(x)$ polinomial dengan derajat terkecil yang memenuhi $p(\alpha)=0$ disebut polinomial minimal atas F. Jika α elemen primitif maka $p(x)$ yang disebut juga polinomial primitif adalah polinomial minimal atas F yang membangun GF_{p^n}. Polinomial minimal yang membangun GF_{p^n} merupakan faktor dari $f(x)=x^{p^n}-x$, karena elemen-elemen dari GF_{p^n} adalah akar-akar dari $f(x)=0$. Sehingga dengan membentuk $f(x)=x^{p^n}-x$ di mana p dan n diketahui kemudian memfaktorkannya, akan diperoleh $p(x)$, polinomial minimal atas F yang membangun GF_{p^n}, di mana $p(x)$ adalah suatu faktor tak tereduksi atas F dari $f(x)$ yang berderajat n dan mempunyai elemen primitif.

BAB I

1.1 Latar Belakang

Misalkan F himpunan tak kosong, himpunan F disebut lapangan (*field*) jika F merupakan ring komutatif dengan elemen satuan dimana setiap elemen tak nol dalam F mempunyai invers. Lapangan yang elemennya berhingga disebut lapangan berhingga. Lapangan berhingga disebut juga *Galois Field* (*Bose & Manvel, 1984*). Sehingga jelas bahwa jika p adalah bilangan prima maka sistem kelas residu (modulo p) adalah lapangan. Lapangan dari kelas residu (modulo p) merupakan *Galois Field*, dinotasikan dengan GF_p. Dan untuk setiap bilangan prima p dan bilangan bulat positif n ada tepat satu lapangan berhingga dengan order p^n (*Raisinghania, 1980*). Lapangan tersebut dinotasikan dengan GF_{p^n}.

Diketahui bahwa selalu terdapat polinomial modulo sedemikian sehingga jika polinomial tersebut dapat digunakan untuk mengkonstruksi lapangan GF_{p^n}, maka kelas residu x-nya mempunyai elemen primitif (*Bose & Manvel, 1984*) . Polinomial tersebut dinamakan fungsi minimal atau polinomial minimal. Sehingga, misalkan E lapangan perluasan atas F dan $\alpha \in E$ elemen aljabar atas F, polinomial minimal adalah polinomial tak tereduksi $M(x) \in F[x]$ dengan derajat terkecil sedemikian sehingga $M(\alpha)=0$, yang mana jika $g(x) \in F[x]$ sedemikian sehingga $g(\alpha)=0$, maka $M(x) \mid g(x)$, dan $M(x)$ mempunyai elemen primitif.