BAB IV

PENUTUP

Berdasarkan pembahasan pada Bab III, Diketahui bahwa polinomial minimal dari $\alpha \in F^*$ adalah monic, tunggal, dan tak tereduksi serta dapat dinyatakan dalam bentuk $m_\alpha(x) = \prod_{\beta \in C(\alpha)} (x - \beta)$ dengan $C(\alpha)$ adalah himpunan konjugasi dari α. Polinomial minimal dari $\beta \in GF(q^m)$, $m_\beta(x) = \prod_{i=0}^{t-1} (x - \beta^{q^i})$ adalah juga suatu faktor tak tereduksi dari $f(x) = x^n - 1$ atas $GF(q)$. Faktor – faktor tak tereduksi $f(x) = x^n - 1$ atas $GF(q)$ didapat dengan memperluas $m_\beta(x)$, dan dengan menggunakan tabel log Zech's, $m_\beta(x)$ mudah didapatkan dan dievaluasi. Selanjutnya derajat $m_\beta(x)$ adalah sama dengan order dari koset – koset siklotomik sehingga banyaknya faktor - faktor tak tereduksi dari $f(x) = x^n - 1$ atas $GF(q)$ adalah sama dengan banyaknya koset - koset siklotomik dari q modulo n. Selain itu faktor - faktor tak tereduksi dari $f(x) = x^n - 1$ atas $GF(q)$ juga dapat diperoleh melalui operasi – operasi PPT $(f(x), g(x))$ dimana $f(x)$ suatu polinomial monic derajat n atas $F = GF(q)$ dan $g(x)$ suatu polinomial atas $GF(q)$ dengan deg $g(x) \leq n - 1$ serta memenuhi $[g(x)]^q \equiv g(x) (\text{mod } f(x))$, sehingga $f(x) = \prod_{s \in F} \text{PPT } (f(x), g(x) - s)$.

This document is Undip Institutional Repository Collection. The author(s) or copyright owner(s) agree that UNDIP-IR may, without changing the content, translate the submission to any medium or format for the purpose of preservation. The author(s) or copyright owner(s) also agree that UNDIP-IR may keep more than one copy of this submission for purpose of security, back-up and preservation:
(http://eprints.undip.ac.id)