# BAB I

# PENDAHULUAN

Persamaan polinomial $x^n$ - 1 atas lapangan berhingga seperti halnya persamaan polinomial yang lain dapat ditemukan faktor - faktornya dengan menggunakan pemfaktoran. Faktor - faktor tersebut dapat dibedakan menjadi dua yaitu faktor tereduksi dan faktor tak tereduksi.

Persamaan polinomial yang akan difaktorkan hanya $x^n$ - 1. Hal ini dikarenakan pemfaktoran $x^n - 1$ atas lapangan berhingga sangat penting dalam mempelajari kode siklik.

Lapangan berhingga dikemukakan pertama kali oleh Galois sehingga untuk menghilangkan kebingungan maka lapangan berhingga dinotasikan dengan $GF(q)$. Pemfaktoran polinomial $x^n$ - 1 atas lapangan berhingga selanjutnya diganti dengan pemfaktoran $x^n - 1$ atas $GF(q)$. Elemen – elemen lapangan seperti polinomial diganti dengan pangkat – pangkat suatu pembangun ($\alpha$). Untuk mempermudah pemfaktoran $x^n - 1$ atas $GF(q)$ digunakan tabel log Zech's ($1 + \alpha^i = \alpha^{z(i)}$). Faktor – faktor $x^n - 1$ atas $GF(q)$ juga didapat dengan menggunakan PPT (pembagi persekutuan terbesar) antara $f(x)$ dan $g(x)$ dengan derajat $g(x) < n - 1$ dan 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 )

Permasalahan yang akan diuraikan dalam tugas akhir ini adalah menentukan faktorisasi $x^n - 1$ atas $GF(q)$ serta menentukan faktor tak tereduksi dari $f(x) = x^n - 1$ atas $GF(q)$ dalam $GF(q^m)$.

Tujuan penulisan dalam tugas akhir ini adalah mendapatkan faktorisasi $x^n - 1$ atas $GF(q)$ serta faktor tak tereduksi dari polinomial $x^n - 1$ atas $GF(q)$.

Sistematika penulisan tugas akhir ini tediri dari empat bab. Bab I berisi pendahuluan. Bab II yaitu teori penunjang yang berisi : bilangan bulat, relasi dan modulo, grup, ring dan lapangan, ruang vektor, ring polinomial, dan faktorisasi polinomial. Bab III yaitu faktorisasi $x^n - 1$ atas $GF(q)$ yang berisi : lapangan berhingga, sifat – sifat lapangan berhingga, polinomial minimal, polinomial siklotomik, tabel log Zech's, lapangan berhingga dan pemfaktoran $x^n - 1$ atas $GF(q)$, dan pemfaktoran $x^n - 1$ atas $GF(q)$. Bab IV yaitu penutup.

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 )