

## MENENTUKAN POLINOMIAL MINIMAL ATAS $GF_p$ YANG MEMBANGUN $GF_{p^n}$

Nunung Andriani<sup>1</sup> dan Bambang Irawanto<sup>2</sup>

<sup>1,2</sup>Jurusan Matematika FMIPA UNDIP

Jl. Prof. H. Soedarto, S.H, Tembalang, Semarang.

**Abstract.** Let  $F$  is finite field with  $p$  elements, denoted by  $GF_p$ . If  $E$  be an extension field of  $F$  and  $\alpha \in E$  is the algebra element of  $F$ , then  $p(x)$ , polynomial of  $F$  of smallest degree such that  $p(\alpha) = 0$  called minimal polynomial of  $F$ . If  $\alpha$  is primitive element, then  $p(x)$  whose called primitive polynomial, is the minimal polynomial of  $F$  whose generate the elements of  $GF_{p^n}$ . The minimal polynomial of  $F$  whose generate the elements of  $GF_{p^n}$  is the factor of  $f(x) = x^{p^n} - x$ , because the elements of  $GF_{p^n}$  are the solution of  $f(x) = 0$ . So, if  $p$  and  $n$  are known we have  $f(x) = x^{p^n} - x$ . If we factoring it, will be obtained  $p(x)$ , the minimal polynomial of  $F$  whose generate the elements of  $GF_{p^n}$ , where  $p(x)$  is some irreducible factor in  $F[x]$  of degree  $n$  that contain a primitive element.

**Keyword:** finite field, extension field, irreducible polynomial, minimal polynomial, primitive element.

### 1. PENDAHULUAN

Misalkan  $F$  adalah lapangan,  $F[x]$  himpunan semua polinomial dalam  $x$  atas  $F$  dan  $f(x) \in F[x]$  suatu polinomial monik dan tak tereduksi.

Suatu himpunan yang dibangun oleh suatu polinomial tak tereduksi merupakan ideal maksimal [4]. Selanjutnya Gallian juga menyatakan suatu ring hasil bagi  $R$  oleh ideal maksimalnya merupakan lapangan. Akibatnya, jika  $F$  lapangan dan  $p(x)$  adalah polinomial yang tak tereduksi atas  $F$ , maka  $\frac{F[x]}{\langle p(x) \rangle}$  adalah lapangan

Lapangan yang elemennya berhingga disebut lapangan berhingga. Lapangan berhingga dengan  $p$  elemen, dengan  $p$  prima disebut juga *Galois Field* dan dinotasikan dengan  $GF_p$ . Pandang polinomial  $f(x)$  atas lapangan  $F$ , [6] mengatakan bahwa setiap polinomial berderajat positif atas  $F$  dapat disajikan

sebagai pergandaan dari koefisien utama dan sejumlah polinomial monik yang tak tereduksi atas  $F$ . Dengan demikian, polinomial berderajat  $n$  atas  $F$ ,  $n$  bilangan bulat positif, mempunyai paling banyak  $n$  akar yang berbeda dalam  $F$ . Dalam tulisan ini dibahas metode atau langkah-langkah untuk memperoleh polinomial minimal atas  $GF_p$  yang membangun  $GF_{p^n}$ .

### 2. LAPANGAN PEMISAH

Suatu lapangan yang memuat lapangan yang lain sebagai himpunan bagiannya disebut lapangan perluasan.

#### Definisi 1 [5]

Misalkan  $E$  dan  $F$  lapangan,  $E$  disebut lapangan perluasan dari  $F$  jika  $F$  adalah lapangan bagian (*subfield*) dari  $E$ , ditulis dengan  $F \leq E$ .

Dengan demikian jika  $E$  lapangan perluasan dari  $F$  maka  $F$  adalah lapangan bagian dari  $E$  dan jika  $F$  adalah lapangan bagian dari  $E$  maka  $E$  dapat dipandang sebagai ruang vektor atas  $F$ . Dimensi dari ruang vektor  $E$  atas  $F$  atau  $E(F)$  disebut derajat dari lapangan perluasan  $E$  atas  $F$ , dinotasikan dengan  $[E : F]$  [ 7].

Keberadaan lapangan perluasan dari suatu lapangan dijamin oleh teorema Kronecker berikut ini

**Teorema 2 (Teorema Kronecker)**

Jika  $F$  adalah lapangan dan  $f(x)$  polinomial yang tidak konstan di dalam  $F[x]$ , maka terdapat lapangan perluasan  $E$  dari  $F$  di mana terdapat akar dari  $f(x)$ . Artinya terdapat  $\alpha \in E$  sedemikian sehingga  $f(\alpha) = 0$ .

Sementara definisi dan teorema mengenai lapangan pemisah (*Splitting Field*) adalah sebagai berikut.

**Definisi 3 [ 6]**

Jika  $E$  mengandung semua akar dari  $f(x) \in F[x]$ , dimana  $F \leq E$ , dan tidak ada lapangan bagian lain dari  $E$  selain  $E$  itu sendiri yang memuat semua akar ini maka  $E$  disebut lapangan pemisah dari  $f(x)$ .

**Contoh 1**

- 1) Lapangan pemisah dari polinomial  $f(x) = x^2 + 1 \in \mathbb{R}[x]$  atas  $\mathbb{R}$  adalah  $C$ , sebab  $f(x) = (x - i)(x + i)$ ,  $i \in C$  dan  $C = \{\mathbb{R}(i) = a + bi \mid a, b \in \mathbb{R}\}$
- 2) Lapangan pemisah dari polinomial  $f(x) = x^2 - 2 \in \mathbb{Q}[x]$  atas  $\mathbb{Q}$  adalah  $\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}b \mid a, b \in \mathbb{Q}\}$ , sebab  $f(x) = x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$

**Teorema 4 [5]**

Jika  $F$  suatu lapangan dan  $f(x)$  polinomial yang tidak konstan di dalam

$F[x]$  maka terdapat lapangan pemisah  $E$  untuk  $f(x)$  atas  $F$ .

**Bukti:**

Akan dibuktikan dengan induksi pada  $\deg(f(x)) = n$ . Jika  $\deg(f(x)) = 1$  maka  $f(x)$  polinomial linear dan  $F = E$ .

Diasumsikan benar untuk polinomial-polinomial yang berderajat lebih kecil dari  $n$ , akan dibuktikan benar untuk  $\deg(f(x)) = n$ . Misal  $p(x) \in F[x]$  adalah faktor tak tereduksi dari  $f(x)$  (mengingat  $F[x]$  suatu DFT). Menurut teorema 2

terdapatlah lapangan  $E \cong \frac{F[x]}{\langle p(x) \rangle}$  yang

merupakan lapangan perluasan dari  $F$  dan  $p(x)$  memiliki akar  $\alpha_1 \in E$  sehingga diperoleh  $p(x) = (x - \alpha_1)q(x)$  di dalam  $E[x]$ , dan  $f(x) = (x - \alpha_1)q(x)g(x)$ . Oleh karena  $q(x)g(x)$  memiliki derajat  $n - 1$ , maka dengan hipotesis induksi terdapatlah lapangan pemisah  $E$  untuk  $q(x)g(x)$  yang memuat akar-akar  $\alpha_2, \alpha_3, \dots, \alpha_n$  dari  $f(x)$ . Sehingga  $f(x)$  terfaktorasi linear dalam  $E[x]$  dan  $F(\alpha_1, \alpha_2, \alpha_3, \dots, \alpha_n) \leq E$  adalah lapangan pemisah dari  $f(x)$  atas  $F$ . Jika  $F$  suatu lapangan dan  $S = \{f_1(x), f_2(x), \dots, f_n(x)\} \subseteq F[x]$ , maka  $E = \bigcap_i E_i$  merupakan lapangan pemisah untuk  $S$ , dengan  $E_i$  lapangan pemisah untuk  $f_i(x)$  atas  $F$ ,  $i = 1, 2, 3, \dots, n$ .

Misalkan  $F$  adalah lapangan dan  $p(x) \in F[x]$  polinomial yang tak tereduksi atas  $F$ . Jika  $\alpha$  adalah akar dari  $p(x)$  di dalam perluasan  $E$  atas  $F$  maka  $F(\alpha)$ , lapangan yang dibangun oleh  $\alpha$ , isomorfis dengan  $\frac{F[x]}{\langle p(x) \rangle}$  [4].

Misalkan  $F$  lapangan dan  $E$  lapangan pemisah atau  $F \leq E$  maka menurut [6]  $E$  merupakan perluasan aljabar (*algebraic extension*). Artinya

setiap elemen  $E$  merupakan elemen aljabar atas  $F$  atau setiap elemen  $E$  merupakan akar-akar dari polinomial  $f(x) = x^{p^n} - x$ . Jika  $F$  lapangan berhingga dengan  $p$  elemen dan  $E$  adalah perluasan berhingga dari  $F$  sedemikian sehingga  $[E : F] = n$  maka  $E$  memiliki  $p^n$  elemen [7].

## 2. AKAR-AKAR LAPANGAN PEMISAH

Polinomial  $f(x) \in F[x]$ , dimana  $f(x) = 0$ , dengan  $\alpha \in F$  maka  $\alpha$  disebut akar dari  $f(x) = 0$ .

### Teorema 5 [7]

Misalkan  $F$  suatu sublapangan dari lapangan  $E$ ,  $f(x) \in F[x]$  dan  $f(x)$  tak tereduksi serta  $E$  memuat akar dari  $f(x)$ , maka  $f(x)$  tidak mempunyai akar-akar ganda dalam  $E$  jika dan hanya jika  $f'(x) \neq 0$

### Teorema 6 [4]

Misalkan  $E$  suatu lapangan dengan  $p^n$  elemen dengan  $p$  bilangan prima yang termuat dalam penutup aljabar  $\bar{Z}_p$  dari  $Z_p$  maka elemen-elemen  $E$  adalah akar-akar dari polinomial  $x^{p^n} - x \in Z_p[x]$  di  $\bar{Z}_p$  atau  $E = \{a \in \bar{Z}_p / a \text{ akar dari } x^{p^n} - x \in Z_p[x]\}$ .

### Teorema 7[7]

Misalkan  $f(x) \in F[x]$  polinomial tidak konstan atas  $F$  dan  $E$  lapangan perluasan dari  $F$ . Elemen  $\alpha \in E$  adalah akar berlipat dari  $f(x)$  jika dan hanya jika  $\alpha$  adalah akar persekutuan dari  $f(x)$  dan  $f'(x)$ .

#### Bukti:

( $\Rightarrow$ ) Misalkan  $\alpha$  akar berlipat dari  $f(x)$  dan  $m$  adalah multiplisitas dari  $\alpha$ , dengan  $m \geq 2$  maka  $f(x) = (x - \alpha)^m g(x)$ , dengan  $g(x)$  polinomial atas  $E$  sedemikian hingga  $g(\alpha) \neq 0$ , dengan demikian

$$f'(x) = m(x - \alpha)^{m-1} g(x) + (x - \alpha)^m g'(x)$$

dan karena  $m \geq 2$ , maka

$$f'(\alpha) = m(\alpha - \alpha)^{m-1} g(\alpha) + (\alpha - \alpha)^m g'(\alpha) = 0$$

Jadi  $\alpha$  adalah akar persekutuan dari  $f(x)$  dan  $f'(x)$ .

( $\Leftarrow$ ) Misalkan  $\alpha$  adalah akar persekutuan dari  $f(x)$  dan  $f'(x)$  dan andaikan  $\alpha$  bukan akar ganda (akar berlipat) dari  $f(x)$ , dalam hal ini  $f(x) = (x - \alpha)g(x)$ , dengan  $g(x)$  polinomial atas  $E$  sedemikian sehingga  $g(\alpha) \neq 0$ . Untuk  $x = \alpha$ , maka

$$\begin{aligned} f'(x) &= (x - \alpha)g'(x) + g(x) \\ &= (\alpha - \alpha)g'(\alpha) + g(\alpha) \neq 0 \end{aligned}$$

Sehingga dapat disimpulkan bahwa  $\alpha$  bukan akar persekutuan dari  $f(x)$  dan  $f'(x)$ , ini bertentangan dengan yang diketahui. Jadi pengandaian harus diingkar dan  $\alpha$  adalah akar berlipat dari  $f(x)$ .

### Teorema 8 [7]

Jika  $F$  suatu lapangan dengan karakteristik prima  $p \neq 0$  maka polinomial  $f(x) = x^{p^n} - x \in F[X]$ , dengan  $n \geq 1$ , memiliki  $p^n$  akar-akar yang berbeda.

#### Bukti:

Diketahui polinomial  $f(x) = x^{p^n} - x$ , maka  $f'(x) = p^n x^{p^n-1} - 1$ . Misalkan  $F$  lapangan dengan karakteristik  $p \neq 0$ , karena  $1 \in F$ , maka  $p = 1 + 1 + \dots + 1 = 0$ , sehingga  $p^n = 0$ . Karena  $p^n = 0$  maka  $f'(x) = -1$ . Sehingga menurut teorema 5  $f(x)$  dan  $f'(x)$  tidak mempunyai akar-akar yang sama lebih dari 1. Dengan kata lain jika  $F$  suatu lapangan berhingga dengan karakteristik  $p \neq 0$  maka polinomial  $f(x) = x^{p^n} - x \in F[X]$ ,  $n \geq 1$  memiliki  $p^n$  akar-akar yang berbeda.

### Teorema 9 [1]

Misal  $p$  bilangan prima dan  $n$  bilangan bulat,  $n \geq 1$ , akar-akar polinomial

$f(x) = x^{p^n} - x \in Z_p[x]$  dalam lapangan pemisah atas  $Z_p$  yang semuanya berbeda membentuk lapangan dengan  $p^n$  elemen.

**Bukti:**

Dari polinomial  $f(x) = x^{p^n} - x$ , maka  $f'(x) = p^n x^{p^n-1} - 1$ . Selanjutnya karena  $p$  bilangan prima dan  $f(x) \in Z_p[x]$ , maka  $f'(x) = 0 \cdot x^{p^n-1} - 1 = -1 \neq 0$  dan menurut Teorema 8,  $f(x)$  memiliki akar-akar yang berbeda. Polinomial  $f(x) = x^{p^n} - x$  berderajat  $p^n$  dan memiliki akar-akar yang semuanya berbeda sehingga jumlah akar-akarnya adalah  $p^n$ . Misal  $F$  himpunan semua akar-akar dari  $f(x)$  atau  $F = \{a \in \bar{Z}_p \mid a \text{ akar dari } f(x) = x^{p^n} - x\}$  akan ditunjukkan  $F$  adalah lapangan.

Ambil  $a, b \in F$  maka  $a^{p^n} - a = 0$  atau  $a^{p^n} = a$  begitu juga  $b^{p^n} - b = 0$  atau  $b^{p^n} = b$ , sehingga  $(a+b)^{p^n} - (a+b) = 0$  dan  $(a+b)^{p^n} = (a+b)$  selanjutnya didapat  $(a \cdot b^{-1})^{p^n} = a^{p^n} (b^{p^n})^{-1}$ . Dengan demikian  $F$  adalah lapangan dan karena jumlah akarnya  $p^n$  maka  $F$  adalah lapangan dengan  $p^n$  elemen atau  $GF_{p^n}$ .

Selanjutnya menurut teorema 6 dan teorema 8, elemen dari  $GF_{p^n}$  adalah akar-akar dari  $f(x) = x^{p^n} - x$ . Akhirnya menurut teorema 7 dan teorema 9,  $F$  lapangan dengan  $p^n$  elemen atau  $GF_{p^n}$  jika dan hanya jika  $F$  adalah lapangan pemisah dari  $f(x) = x^{p^n} - x$ .

**4. MENENTUKAN POLINOMIAL MINIMAL ATAS  $GF_p$  YANG MEMBANGUN  $GF_{p^n}$**

**Definisi 10**

Jika  $E$  lapangan perluasan atas  $F$  dan  $\alpha \in E$  elemen aljabar atas  $F$ , maka polinomial monik  $p(x)$  atas  $F$  dengan

derajat terkecil yang memenuhi  $p(\alpha) = 0$  disebut polinomial minimal atas  $F$ .

Jika derajat dari polinomial minimal atas  $F$  tersebut sama dengan  $n$ , maka  $\alpha$  dikatakan sebagai elemen aljabar atas  $F$  yang berderajat  $n$ .

**Teorema 11 [2]**

Misalkan  $E$  lapangan perluasan atas  $F$  dan  $\alpha \in E$  elemen aljabar atas  $F$ . Misalkan juga  $p(x) \in F[x]$  adalah polinomial dengan derajat terkecil sedemikian hingga  $p(\alpha) = 0$ , maka

- (i).  $p(x)$  adalah polinomial yang tak tereduksi atas  $F$
- (ii). Jika  $g(x) \in F[x]$  sedemikian sehingga  $g(\alpha) = 0$ , maka  $p(x) \mid g(x)$
- (iii). Terdapat dengan tunggal  $p(x) \in F[x]$  dengan derajat terkecil sedemikian sehingga  $p(\alpha) = 0$

**Bukti:**

- (i) Andaikan berlaku sebaliknya yaitu  $p(x)$  adalah polinomial yang tereduksi atas  $F$  maka  $p(x) = h(x)q(x)$ , dimana  $\deg h(x)$  dan  $\deg q(x)$  kurang dari  $\deg p(x)$ . Maka  $p(\alpha) = h(\alpha)q(\alpha) = 0$ , ini berarti  $h(\alpha) = 0$  atau  $q(\alpha) = 0$ . Dengan demikian  $\alpha$  memenuhi sebuah polinomial dengan derajat kurang dari derajat  $p(x)$ . Ini bertentangan dengan keminimalan dari  $p(x)$ , sehingga pengandaian harus diingkar. Jadi,  $p(x)$  adalah polinomial yang tak tereduksi atas  $F$ .
- (ii) Misalkan  $g(x) \in F[x]$  dan  $p(x)$  adalah polinomial seperti pada (i). Berdasarkan algoritma pembagian, terdapat polinomial  $q(x)$  dan  $r(x)$  di  $F[x]$  sedemikian hingga berlaku  $g(x) = p(x)q(x) + r(x)$ ,  $r(x) = 0$  atau  $\deg r(x) < \deg p(x)$ . Karena  $g(\alpha) = 0$ , maka

$$g(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = 0 \Rightarrow r(\alpha) = 0.$$

Karena  $p(x)$  adalah polinomial dengan derajat terkecil sedemikian hingga  $p(\alpha) = 0$ , maka  $r(x)$  haruslah 0. Sehingga  $g(x) = p(x)q(x)$ , yaitu  $p(x) | g(x)$ .

- (iii) Misalkan  $f(x)$  polinomial monik dengan derajat terkecil sedemikian hingga memenuhi  $f(\alpha) = 0$ , maka dari pembuktian (ii) diperoleh  $p(x) | f(x)$  dan  $f(x) | p(x)$ . Karena  $f(x)$  dan  $p(x)$  kedua-duanya adalah polinomial monik, maka dari  $p(x) | f(x)$  dan  $f(x) | p(x)$  diperoleh  $f(x) = p(x)$ . Ini memperlihatkan bahwa polinomial  $p(x)$  tunggal.

**Teorema 12 [9]**

Misalkan  $p$  adalah bilangan prima dengan  $p > 0$  dan  $n \in \mathbb{N}$ , maka polinomial  $x^{p^n} - x$  merupakan hasil kali semua polinomial monik yang tak tereduksi dalam  $Z_p[x]$  yang derajatnya membagi  $n$ .

**Bukti:**

Jika polinomial monik  $x^{p^n} - x$  difaktorkan dalam  $Z_p[x]$  maka akan diperoleh

$$x^{p^n} - x = f_1^{e_1} f_2^{e_2} \cdots f_s^{e_s}$$

dimana  $f_1^{e_1}, f_2^{e_2}, \dots, f_s^{e_s}$  adalah polinomial polinomial monik yang tak tereduksi dan berbeda dalam  $Z_p[x]$  dan  $e_1, e_2, \dots, e_s \in \mathbb{N}$

Untuk membuktikan teorema di atas akan akan ditunjukkan beberapa hal berikut

- (a) Tidak ada faktor dari  $x^{p^d} - x$  yang membagi  $x^{p^n} - x$  lebih dari sekali
- (b) Jika  $f$  polinomial monik yang tak tereduksi dalam  $Z_p[x]$  dengan derajat yang membagi  $n$  maka  $f$  adalah faktor dari  $x^{p^n} - x$  (dengan kata lain  $f$  sama dengan salah satu dari  $f_i$ )
- (c) Derajat dari setiap faktor dari  $x^{p^n} - x$  dalam  $Z_p[x]$  harus membagi  $n$

(dengan kata lain setiap derajat dari  $f_i$  membagi  $d$ ).

Bukti dari (a):

Misalkan  $F = Z_p$  lapangan dan  $f = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in F[x]$ , maka turunan pertama dari  $f$  adalah  $f' = a_1 + 2a_2x + \dots + na_nx^{n-1}$ . Perlu diperhatikan bahwa untuk setiap polinomial  $f$  dan  $g$  di dalam  $F[x]$  dan sebarang  $a \in F$  senantiasa berlaku hal-hal berikut :

- $(f + g)' = f' + g'$
- $(fg)' = f'g + fg'$
- $(af)' = af'$

Misalkan  $f = g^2h$  untuk untuk sebarang polinomial  $g$  dengan derajat  $\geq 1$ . Dari fungsi  $f$  di atas menghasilkan

$$f' = 2gg'h + g^2h' = g(2g'h + gh')$$

Sehingga  $f$  dan  $f'$  mempunyai faktor bersama, yaitu  $g$ , dengan derajat  $\geq 1$ . Dalam kasus ini  $P = x^{p^n} - x$  sehingga  $P' = p^n x^{p^n-1} - 1 \neq 0$ . Sesuai teorema 3  $P$  tidak mempunyai akar berlipat dalam perluasan  $Z_p$ . Itu artinya bahwa  $P$  tidak mempunyai faktor yang berulang atau  $P$  tidak mempunyai faktor yang membagi  $x^{p^n} - x$  lebih dari sekali.

Bukti (b):

Misalkan  $f$  suatu polinomial monik yang tak tereduksi dalam  $Z_p[x]$  dengan derajat  $d$  membagi  $n$ . Akan ditunjukkan  $f$  membagi  $x^{p^n} - x$ . Karena  $d$  membagi  $n$  maka  $p^d - 1$  membagi  $p^n - 1$  dalam  $\mathbb{Z}$ . Dengan demikian  $x^{p^d-1} - 1$  membagi  $x^{p^n-1} - 1$  dalam  $Z_p[x]$ . Dan jika kedua polinomial di atas dikalikan dengan  $x$ , diperoleh  $x^{p^d} - x$  membagi  $x^{p^n} - x$  dalam  $Z_p[x]$ .

Sekarang  $f$  tak tereduksi dalam  $Z_p[x]$  dengan derajat  $d$ , sehingga  $K = Z_p[X]/f$  adalah lapangan dengan  $p^d$  elemen. Selanjutnya, polinomial minimal dari  $\alpha = x + (f) \in K$  atas  $Z_p$  adalah  $f$ . Karena  $K^*$  adalah grup dengan  $p^d - 1$  elemen maka dipunyai  $\alpha^{p^d-1} = 1$  dan jika bentuk ini dikalikan dengan  $\alpha$  diperoleh  $\alpha^{p^d} - \alpha = 0$ , yaitu  $\alpha$  adalah akar dari polinomial  $x^{p^d} - x \in Z_p[x]$  karena polinomial minimal  $\alpha$  atas  $Z_p$  adalah  $f$  maka  $f$  harus membagi  $x^{p^d} - x$ . Sementara polinomial terakhir membagi  $x^{p^n} - x$ . Jadi  $f$  juga membagi  $x^{p^n} - x$ .

Bukti (c):

Misalkan  $f$  polinomial monik yang tak tereduksi dalam  $Z_p[x]$  yang membagi  $x^{p^n} - x$  dan berderajat  $d$ . Sebagaimana pada pembuktian (b), dapat dilihat bahwa  $f$  adalah faktor dari  $x^{p^d} - x$ . Dengan mengasumsikan  $f$  juga faktor dari  $x^{p^n} - x$ , maka  $f$  adalah faktor dari  $\gcd(x^{p^n} - x, x^{p^d} - x)$ . Sehingga diperoleh  $\gcd(x^{p^n-1} - 1, x^{p^d-1} - 1) = x^{\gcd(p^n-1, p^d-1)} = x^{p^{\gcd(n,d)-1}} - 1$ . Dari sini diperoleh  $x$  prima relatif terhadap semua polinomial yang ditunjukkan, mengalikan dengan  $x$  diperoleh

$$D = \gcd(x^{p^n} - x, x^{p^d} - x) = x^{p^{\gcd(n,d)}} - x$$

Sebagaimana pada pembuktian (b), dengan

$$K = Z[x]/f \text{ dan } \alpha = x + (f), \text{ maka}$$

$$K = Z_p[\alpha]. \text{ Kita ketahui bahwa } K$$

mempunyai  $p^d$  elemen, dan setiap elemen

dari  $K$  adalah akar dari  $x^{p^d} - x$ .

Diberikan  $e = \gcd(n, d)$ , dari uraian di atas

$x^{p^e} - x$  adalah faktor dari  $x^{p^d} - x$ , jadi  $x^{p^d} - x$  mempunyai  $p^e$  akar yang berbeda dalam  $K$ . Akar-akar tersebut membentuk sebuah lapangan bagian  $L$  dari  $K$ . Tetapi  $f$  membagi  $x^{p^e} - x$ , jadi  $\alpha \in L$ . Lagipula,

$Z_p$  termuat dalam  $L$ . Oleh karena itu,  $K = Z_p[\alpha]$  termuat dalam  $L$ , sehingga  $L = K$  karena itu,  $p^e = p^d$ , jadi  $e = d$ .  
Sehingga terbukti  $d$  membagi  $n$ .

Dari pengertian polinomial minimal dan uraian sebelumnya diketahui bahwa polinomial yang akan ditentukan adalah faktor (yang merupakan polinomial tak tereduksi) dari  $f(x) = x^{p^n} - x$ . Sehingga untuk mendapatkan polinomial minimal atas  $GF_p$  yang membangun  $GF_{p^n}$  dengan  $p$  dan  $n$  diketahui, terlebih dahulu dibentuk polinomial  $f(x) = x^{p^n} - x$ . Polinomial ini difaktorkan dengan menentukan koset-koset siklotomiknya dan menggunakan metode faktor persekutuan terbesar (gcd).

### Definisi 13 [8]

Misalkan  $i$  suatu bilangan bulat tertentu,  $0 \leq i \leq m-1$ . Koset-koset siklotomik ( $p$  modulo  $m$ ) yang memuat  $i$ ,  $p$  bilangan prima dan  $m$  bilangan bulat positif, dinyatakan sebagai berikut:

$$C_i = \{i, ip, ip^2, \dots, ip^{s-1}\}$$

dengan elemen-elemen himpunan diambil dari mod  $m$ , dan  $s$  bilangan bulat terkecil sedemikian sehingga  $ip^s \equiv i \pmod{m}$ .

$C = \{C_i / 0 \leq i \leq m-1\}$  adalah himpunan koset-koset siklotomik dari  $p$  modulo  $m$ .

### Teorema 14 [8]

Jika  $f(x)$  suatu polinomial monik berderajat  $m$  atas  $F = GF_p$ , dan  $g(x)$  suatu polinomial atas  $F$  dengan  $\deg g(x) \leq m-1$  serta memenuhi  $[g(x)]^p \equiv g(x) \pmod{f(x)}$ , maka  $f(x) = \prod_{i=1}^r \gcd(f(x), g(x) - s)$ .

### Bukti:

Misalkan  $\gcd(f(x), g(x) - s)$  membagi habis  $f(x)$  untuk setiap  $s \in F$ . Selanjutnya karena

$$\begin{aligned} \gcd(a, b) &= \gcd(a, b - a) \\ \gcd(g(x) - s, g(x) - t) &= 1 \text{ dan} \\ \gcd(g(x) - s, s - t) &= 1 \end{aligned}$$

untuk  $s \neq t$ , dengan  $t \in F$  maka  $\gcd(\gcd(f(x), g(x) - s), \gcd(f(x), g(x) - t)) = 1$ , untuk  $s \neq t$ . Dengan demikian  $\prod_{s \in F} \gcd(f(x), g(x) - s)$  membagi habis  $f(x)$ . Dari pendefinisian  $g(x)$ , maka  $f(x)$  membagi habis  $[g(x)]^p - g(x)$ . Sehingga didapat  $y^p - y = \prod_{s \in F} (y - s)$ ,  $[g(x)]^p - g(x) = \prod_{s \in F} g(x) - s$  dan  $f(x)$  membagi habis  $\prod_{s \in F} g(x) - s$ . Dengan demikian  $f(x)$  membagi habis  $\prod_{s \in F} \gcd(f(x), g(x) - s)$ . Terakhir karena  $f(x)$  dan  $\prod_{s \in F} \gcd(f(x), g(x) - s)$  keduanya polinomial monik, dapat disimpulkan  $f(x) = \prod_{s \in F} \gcd(f(x), g(x) - s)$ .

Dari teorema 12 diketahui bahwa faktor atau polinomial yang dicari adalah polinomial yang berderajat  $n$ . Kemudian satu ciri lagi dari polinomial yang dapat mengkonstruksi  $GF_{p^n}$  secara *implisit* dapat dilihat pada proposisi dan definisi elemen primitif berikut.

**Proposisi 15 [10]**

Misalkan  $F$  lapangan berhingga dengan  $p^n$  elemen. Misalkan  $\theta$  elemen primitif dari  $F$  dan  $M(x)$  polinomial minimal atas  $Z_p$ . Maka  $F$  isomorfis dengan  $Z_p[x]/M(x)$ . Dalam hal ini  $\deg M(x) = n$ .

**Definisi 16 [2]**

Misalkan  $\theta \neq 0$ ,  $\theta \in GF_{p^n}$  dan memenuhi persamaan  $\theta^{p^n-1} = 1$ , maka  $\theta$  dikatakan elemen primitif dari  $GF_{p^n}$  jika hasil perpangkatan  $\theta$  dengan pangkat kurang

dari  $p^n - 1$  ( $\theta^i, 0 \leq i < p^n - 1$ ) semuanya berbeda.

Dengan demikian jika  $\theta$  adalah elemen primitif, maka

$$\theta^0 (= 1), \theta, \theta^2, \theta^3, \dots, \theta^{p^n-2}$$

kesemuanya berbeda dan semua elemen tersebut di dalam  $GF_{p^n}$  serta  $\theta^i \neq 1$  untuk  $0 < i < p^n - 1$ .

**Contoh 2**

Misal diberikan  $GF_p$ , dengan  $p = 3$ , maka dapat dikonstruksi lapangan  $GF_{3^2}$  dari polinomial  $x^2 + 2x + 2$  yang merupakan polinomial yang tak tereduksi atas  $GF_3$ . Dapat dilihat bahwa kelas residu  $x$  dari  $x^2 + 2x + 2$  mempunyai elemen primitif  $x^2 = -2x - 2 = x + 1$ . Kelas-kelas residu tersebut adalah

$$\begin{aligned} [x^0] &= 1 & [x^5] &= 2x \\ [x^1] &= x & [x^6] &= 2x + 2 \\ [x^2] &= x + 1 & [x^7] &= x + 2 \\ [x^3] &= 2x + 1 & [x^8] &= 1 \\ [x^4] &= 2 \end{aligned}$$

Karena  $\theta^i, 0 \leq i < p^n - 1$  semuanya berbeda maka kelas residu  $x$  mempunyai elemen primitif.

Jika yang digunakan adalah  $x^2 + 1$ , yang juga tak tereduksi atas  $GF_3$ , maka masih akan didapatkan sebuah lapangan dengan 9 elemen. Namun  $x^2 + 1$  tidak mempunyai elemen primitif, sebab akar dari  $x^2 + 1$  hanya mempunyai order 4 sebagaimana yang ditunjukkan berikut ini

Dari  $x^2 = -1 = 2$  diperoleh

$$\begin{aligned} [x^0] &= 1 & [x^3] &= 2x \\ [x^1] &= x & [x^4] &= 1 \\ [x^2] &= 2 \end{aligned}$$

Karena  $\theta$  adalah elemen dari  $GF_{p^n}$ , yaitu  $\theta$  merupakan akar dari salah satu polinomial tak tereduksi yang merupakan faktor dari  $f(x) = x^{p^n} - x$ ,

maka polinomial minimal atas  $GF_p$  yang membangun  $GF_{p^n}$  haruslah mempunyai akar yang merupakan elemen primitif. Dengan perkataan lain, polinomial tersebut harus mengandung elemen primitif.

## 5. KESIMPULAN

Dari uraian di atas dapat disimpulkan bahwa polinomial minimal atas  $GF_p$  yang membangun  $GF_{p^n}$  dapat diperoleh dengan prosedur berikut :

Misal diberikan  $GF_{p^n}$  dengan  $p$  dan  $n$  diketahui, maka dapat dibentuk polinomial  $f(x) = x^{p^n} - x$  yang mempunyai faktor-faktor berupa polinomial monik yang tak tereduksi atas  $GF_p$ .

Dengan menentukan koset-koset siklotomik dari polinomial tersebut dan menggunakan metode faktor persekutuan terbesar (gcd) akan diperoleh  $p_i(x)$ , faktor-faktor yang tak tereduksi dari  $f(x)$ , dimana derajat dari  $p_i(x)$  pasti membagi  $n$  untuk setiap  $i$ , dimana  $i$  menunjukkan faktor yang ke- $i$ ., dan  $p_i(x)$  semuanya berbeda.

Polinomial minimal yang dimaksud adalah  $p_i(x)$  yang berderajat  $n$  dan mempunyai elemen primitif.

## 6. DAFTAR PUSTAKA

[1]. Bambang Irawanto, (2001), *Galois Field*, Program Studi Matematika Jurusan Ilmu-ilmu Matematika dan Pengetahuan Alam Universitas Gajah Mada, Yogyakarta.

- [2]. Bhattacharya, P. B., (1984), *Basic Abstract Algebra*, Cambridge University Press, New York.
- [3]. Fraleigh, J. B., (1994), *A First Course in Abstract Algebra*, Addison-Wesley Publishing Company, USA.
- [4]. Gallian, Joseph, (1990), *A Contemporary Abstract Algebra, Second Edition*, D.C. Heath and Company, Massachusetts.
- [5]. Gilbert, Jimmi & Linda., (1998), *Elements of Modern Algebra : Second edition*, PWS-KENT Publishing Co., Boston.
- [6]. Raisinghanian, M.D. and R.S. Aggarwal, (1980), *Modern Algebra*, S. Chand and Company Ltd., New Delhi.
- [7]. Sudibyo, (2001), *Faktorisasi Polinomial  $x^n - 1$  atas Lapangan Berhingga*, Jurusan Matematika FMIPA Universitas Diponegoro, Semarang.
- [8]. \_\_\_\_\_, *On Finite Fields*, [www.math.uregina.ca/~szechtf/finitefields.pdf](http://www.math.uregina.ca/~szechtf/finitefields.pdf). Diakses: 8 Mei 2007, 20.38 WIB.
- [9]. \_\_\_\_\_, *Commutative Rings and Finite Fields*, [www-rohan.sdsu.edu/~mosulliv/coding04/FF.pdf](http://www-rohan.sdsu.edu/~mosulliv/coding04/FF.pdf). Diakses : 8 Mei 2007, 20.38 WIB.