CIRI-CIRI POLINOMIAL PERMUTASI ATAS *FINITE FIELD*

AINI SURI TALITA

0305017011

UNIVERSITAS INDONESIA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

DEPARTEMEN MATEMATIKA

DEPOK

2008

CIRI-CIRI POLINOMIAL PERMUTASI ATAS *FINITE FIELD*

Skripsi diajukan sebagai salah satu syarat untuk memperoleh gelar Sarjana Sains

Oleh:

AINI SURI TALITA

0305017011

DEPOK

2008

SKRIPSI : CIRI-CIRI POLINOMIAL PERMUTASI ATAS *FINITE FIELD*

NAMA : AINI SURI TALITA

NPM : 0305017011

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

DEPOK, 23 DESEMBER 2008

DR. SRI MARDIYATI, M. KOM	HELEN BURHAN, S.SI., M.SI.
PEMBIMBING I	PEMBIMBING II

Tanggal lulus Ujian Sidang Sarjana: 23 Desember 2008

Penguji I : DR. SRI MARDIYATI, M. KOM

Penguji II : DRA. DENNY RIAMA SILABAN, M. KOM

Penguji III : DRA. RIANTI SETIADI, M.SI

KATA PENGANTAR

Puji syukur saya panjatkan kepada Allah Yang Maha Kuasa, karena atas berkat dan rahmat-Nya, penulisan tugas akhir ini dapat diselesaikan. Penulisan tugas akhir ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Sains Departemen Matematika pada Fakultas Matematika dan Ilmu Pengetahuan Alam. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai penyusunan tugas akhir ini, sangatlah sulit bagi saya untuk menyelesaikan tugas akhir ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

(1) Ibu Lintang Banon Sari dan rekan-rekan;
(2) Dr. Sri Mardiyati, M.Kom dan Helen Burhan S.Si, M.Si. selaku Pembimbing I dan Pembimbing II;
(3) Seluruh sivitas akademika Departemen Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam.

Akhir kata, saya berharap Allah berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga tugas akhir ini membawa manfaat bagi pengembangan ilmu.

Depok, Desember 2008

Penulis

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 $f: GF(q) \to GF(q)$ 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

DAFTAR ISI

BAB 1

PENDAHULUAN

1.1 Latar Belakang

Finite field maupun polinomial atas *finite field* memiliki aplikasi yang cukup luas sehingga menarik untuk dibahas.

Aplikasi tersebut mencakup area seperti *coding theory*, *cryptography*, *combinatoric*, konstruksi dari *error-correcting codes* maupun teknologi terkini seperti telepon seluler CDMA (Blake et al. 1-4).

Area-area di atas sering melibatkan suatu polinomial atas *finite field* dengan sifat khusus yang disebut polinomial permutasi.

Polinomial f atas *finite field* $GF(q)$ merupakan polinomial permutasi jika pemetaan $f: GF(q) \to GF(q)$ adalah pemetaan satu-satu (Mollin and Small 535).

Suatu polinomial yang merupakan polinomial permutasi di suatu *finite field* belum tentu merupakan polinomial permutasi di *finite field* yang lain. Sebagai contoh, $f(x) = x^2$ merupakan polinomial permutasi pada $\mathbb{Z}_2$ karena $f([0]_2) = [0]_2$ dan $f([1]_2) = [1]_2$. Namun, $f(x) = x^2$ bukan polinomial permutasi pada $\mathbb{Z}_3$, karena $f([1]_3) = [1]_3 = f([2]_3)$.

Polinomial permutasi atas *finite field* memiliki beberapa aplikasi khusus seperti *modular enciphering* dan *Imai-Matsumoto system* yang berkaitan dengan *cryptosystem*, *latin square* berkaitan dengan *combinatoric*, maupun pembentukan *key* berkaitan dengan *cryptography* (Lidl and Pilz 243, 252, 398; Koblitz 80).

Untuk menentukan apakah suatu polinomial atas *finite field* merupakan polinomial permutasi dapat digunakan cara yang paling sederhana yaitu dengan mendaftarkan semua hasil peta fungsi polinomial tersebut, kemudian memeriksa apakah himpunan peta yang didapat memuat semua anggota *finite field*. Akan tetapi, hal ini sulit

dilakukan apabila jumlah anggota *finite field* besar. Karena itu, diperlukan suatu kriteria sederhana untuk memeriksa apakah suatu polinomial atas *finite field* merupakan polinomial permutasi atau bukan.

1.2 Permasalahan

Apa ciri-ciri dari suatu polinomial atas *finite field* sehingga polinomial tersebut merupakan polinomial permutasi?

1.3 Tujuan Penulisan

Menentukan ciri-ciri polinomial permutasi atas *finite field*.

1.4 Sistematika Penulisan

Tugas akhir ini terdiri dari empat bab yang dimulai dengan Bab 1 yang menerangkan secara garis besar isi dari tugas akhir ini. Bab 2 berisi landasan teori tentang *group*, *ring*, dan *field* yang akan digunakan pada pembahasan tugas akhir ini. Pembahasan tentang ciri-ciri suatu polinomial permutasi atas suatu *finite field* ditunjukkan pada Bab 3. Bab 4 berisi kesimpulan dari tugas akhir ini.

BAB 2

LANDASAN TEORI

Pada bab ini dibahas landasan teori yang akan digunakan untuk menentukan ciri-ciri dari polinomial permutasi atas *finite field*.

Hal ini dimulai dengan memberikan pengertian dari *group* beserta sifat-sifatnya.

Definisi 2.1

Suatu himpunan tak kosong G dengan operasi $*$, dinotasikan dengan $(G,*)$, disebut *group* apabila memenuhi sifat berikut:

a) $a, b \in G$ mengakibatkan $a * b \in G$.
b) $(a * b) * c = a * (b * c)$ untuk $a, b, c \in G$.
c) Terdapat $\boldsymbol{e} \in G$ sedemikian sehingga $a * \boldsymbol{e} = \boldsymbol{e} * a = a$, untuk setiap $a \in G$. $\boldsymbol{e}$ merupakan elemen identitas pada G.
d) Untuk setiap $a \in G$, terdapat $b \in G$ sedemikian sehingga $a * b = b * a = \boldsymbol{e}$, b biasa dinotasikan dengan $-a$.

(Herstein, *Abstract* 41)

Untuk penyederhanaan tulisan, selanjutnya $(G,*)$ akan ditulis sebagai G saja.

Selanjutnya akan ditampilkan beberapa penamaan atau istilah dari *group* yang berkaitan dengan sifat yang dimiliki oleh anggota *group*.

Definisi 2.2

a) *Finite group* merupakan *group* dengan banyak anggotanya berhingga (Herstein, *Abstract* 42).

b) Untuk G *finite group*, banyaknya anggota G disebut *order* G (Herstein, *Abstract* 42).

c) *Abelian group* merupakan *group* yang memenuhi sifat $a * b = b * a$ untuk setiap a, b anggota *group* (Herstein, *Abstract* 43).

d) Misalkan G suatu *finite group*. $a \in G$. Bilangan bulat positif terkecil m sedemikian sehingga $a^m = \boldsymbol{e}$ disebut *order* a (Herstein, *Abstract* 60).

Berkaitan dengan definisi *finite group* diperoleh teorema berikut.

Teorema 2.3

Misalkan G merupakan *finite group* dengan *order* n, $n \in \mathbb{N}$, maka $a^n = \boldsymbol{e}$, untuk setiap $a \in G$ (Herstein, *Abstract* 60).

Berikut ini diberikan pengertian dari suatu *group* dengan bentuk khusus.

Definisi 2.4

Misalkan G suatu *group*. G disebut *cyclic group* jika terdapat sebuah anggota G, misalkan a, sedemikian sehingga untuk setiap $m \in G$ dapat dinyatakan sebagai $m = a^i$, untuk suatu bilangan bulat i.

Akibat dari Definisi 2.4 diperoleh bahwa *order* dari a adalah banyaknya anggota G dan a disebut *generator* G (Herstein, *Abstract* 55).

Berkaitan dengan sifat dari *cyclic group* diperoleh Lemma 2.5.

Lemma 2.5

Cyclic group merupakan *abelian group* (Herstein, *Abstract* 55).

Suatu *finite abelian group* dapat dikaitkan dengan bilangan prima yang membagi *order group* tersebut. Hal ini ditunjukkan oleh teorema berikut.

Teorema 2.6

Misalkan G adalah suatu *finite abelian group* dan p adalah bilangan prima yang membagi *order* G, maka terdapat suatu anggota G, sebut $a \neq \boldsymbol{e}$, sedemikian sehingga *order a* adalah p (Herstein, *Abstract* 80).

Sebelumnya telah dibahas bahwa *group* adalah suatu struktur aljabar dengan satu operasi, berikut ini akan dibahas suatu struktur aljabar dengan dua operasi yang dikenal dengan sebutan *ring*.

Definisi 2.7

Suatu himpunan tak kosong R dengan operasi $+$ dan $\cdot$, dinotasikan dengan $(R, +, \cdot)$, disebut *ring* apabila memenuhi sifat berikut:

a) $(R, +)$ merupakan *abelian group* dengan elemen identitas $\mathbf{0}$.
b) $a, b \in R$ mengakibatkan $a \cdot b \in R$.
c) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ untuk $a, b, c \in R$.
d) $a \cdot (b + c) = a \cdot b + a \cdot c$ dan $(b + c) \cdot a = b \cdot a + c \cdot a$ untuk $a, b, c \in R$.

(Herstein, *Abstract* 126)

Untuk pembahasan selanjutnya $(R, +, \cdot)$ ditulis sebagai R saja dan $a \cdot b$ ditulis ab saja.

Sifat dari operasi perkalian pada *ring* berkaitan dengan elemen identitas terhadap operasi penjumlahan diberikan pada Lemma 2.8.

Lemma 2.8

Misalkan R suatu *ring* dan $a \in R$. Maka $a\mathbf{0} = \mathbf{0}a = \mathbf{0}$ (Herstein, *Abstract* 137).

Istilah-istilah berikut berkaitan dengan *ring* beserta sifat yang dimilikinya.

Definisi 2.9

Misalkan R suatu *ring* dan $u \in R$. u disebut elemen *unit* dari R jika untuk setiap $v \in R$ berlaku $uv = vu = v$.

Untuk selanjutnya, elemen *unit* dinotasikan dengan **1**.

Definisi 2.10

a) Misalkan R suatu *ring*. R disebut *commutative ring* jika berlaku $ab = ba$, untuk $a, b \in R$.
b) Suatu *commutative ring* R disebut *integral domain* jika $ab = \mathbf{0}$ mengakibatkan $a = \mathbf{0}$ atau $b = \mathbf{0}$, untuk $a, b \in R$.
c) Suatu *ring* R dengan elemen *unit* **1** disebut *division ring* jika untuk setiap $a \neq \mathbf{0} \in R$ terdapat $b \in R$ sedemikian sehingga $ab = ba = \mathbf{1}$, dengan b biasa dinotasikan a^{-1}.

(Herstein, *Abstract* 127).

Berdasarkan pengertian *ring* dan sifat-sifat yang berlaku pada *ring*, diperoleh pengertian dari *field* berikut ini.

Definisi 2.11

Suatu *ring* R disebut *field* jika R merupakan *commutative division ring* (Herstein, *Abstract* 127).

Selanjutnya diberikan hubungan antara suatu *field* dengan suatu *integral domain.*

Teorema 2.12

Suatu *field* F merupakan *integral domain* (Herstein, *Abstract* 133).

Suatu *field* yang mempunyai sejumlah berhingga anggota dinamakan *finite field* atau yang dikenal juga sebagai Galois *field*. Suatu *finite field* dengan banyaknya anggota q dinotasikan dengan $GF(q)$.

Pada *field* dikenal suatu istilah karakteristik yang pengertiannya diberikan oleh definisi berikut.

Definisi 2.13

Misalkan F suatu *field*. F memiliki karakteristik $p \neq 0$ jika p merupakan bilangan bulat positif terkecil dimana berlaku $px = \mathbf{0}$, untuk setiap $x \in F$ (Herstein, *Abstract* 178).

Berkaitan dengan karakteristik dari suatu *field* dan jumlah anggotanya diperoleh teorema berikut.

Teorema 2.14

Misalkan F suatu *finite field*. Maka F memiliki p^m anggota, dimana bilangan prima p merupakan karakteristik dari F, untuk suatu bilangan asli m (Herstein, *Topics* 357).

Terdapat suatu sifat dari operasi penjumlahan anggota dari suatu *field* apabila dipangkatkan dengan karakteristik dari *field* yang memuatnya.

Teorema 2.15

Misalkan F suatu *field* dengan karakteristik bilangan prima p. Untuk $a, b \in F$ berlaku:

$(a+b)^p = a^p + b^p$

(Koblitz 58)

Berikut ini diberikan teorema yang menghubungkan suatu *finite field* dengan *cyclic group*.

Teorema 2.16

Misalkan F suatu *finite field*. $F - \{\mathbf{0}\}$ merupakan *cyclic group* terhadap operasi perkalian pada F (Lidl and Pilz 138).

Berdasarkan Teorema 2.16 diperoleh bahwa untuk *finite field* F, $F - \{\mathbf{0}\}$ merupakan *cyclic group*. Sesuai dengan definisi *cyclic group*, diperoleh bahwa $F - \{\mathbf{0}\}$ mempunyai paling sedikit satu *generator*.

Definisi 2.17

Misalkan F suatu *finite field*. *Generator* dari *cyclic group* $F - \{\mathbf{0}\}$ disebut elemen *primitive* dari F (Lidl and Pilz 139).

Sebelum membahas sifat-sifat dari elemen *primitive* suatu *finite field* lebih lanjut, diperlukan Definisi 2.18 yang berkaitan dengan sifat bilangan bulat yaitu apabila diberikan dua buah bilangan bulat maka dapat ditentukan suatu bilangan yang merupakan *greatest common divisor* (*gcd*) dari dua buah bilangan bulat tersebut.

Definisi 2.18

Diberikan dua buah bilangan bulat a, b, tidak keduanya nol, maka *greatest common divisor* (*gcd*) dari a dan b adalah c jika dipenuhi:

a) $c > 0$
b) c membagi a dan c membagi b.
c) Jika d membagi a dan d membagi b maka d membagi c.

(Herstein, *Abstract* 23)

Berkaitan dengan Teorema 2.16 dan Definisi 2.17 diperoleh teorema berikut.

Teorema 2.19

Misalkan α adalah elemen *primitive* dari *finite field* $GF(q)$ dengan banyak anggota q, $q \in \mathbb{N}$. Maka:

a) $F = \{\mathbf{0}, \mathbf{1}, \alpha, \alpha^2, \alpha^3, \dots, \alpha^{q-2}\}$.
b) $\alpha^{q-1} = \mathbf{1}$.

c) α^k juga merupakan elemen *primitive* jika dan hanya jika $gcd(k, q-1) = 1$.

(Lidl and Pilz 139)

Jumlah dari pangkat masing-masing anggota *field* dapat dibatasi menjadi dua kemungkinan nilai saja. Hal ini diberikan pada Lemma 2.20.

Lemma 2.20

Misalkan $GF(q)$ suatu *finite field* dengan banyak anggota q, $q \in \mathbb{N}$, dan $a_0, a_1, \ldots, a_{q-1} \in GF(q)$. Maka

a) $\sum_{i=0}^{q-1} {a_i}^t = \mathbf{0}$, untuk $1 \leq t \leq q-2$.
b) $\sum_{i=0}^{q-1} {a_i}^t = -\mathbf{1}$, untuk $t = q-1$.

(Lidl and Pilz 150).

Salah satu contoh dari *finite field* adalah $\mathbb{Z}_n$, n bilangan prima. Berikut ini diberikan definisinya.

Definisi 2.21

Untuk $a, b \in \mathbb{Z}$, n tertentu di $\mathbb{Z}$, $n > 1$

a) Didefinisikan suatu relasi ekivalen kongruen modulo n pada himpunan bilangan bulat $\mathbb{Z}$. a kongruen modulo n ke b, dinotasikan dengan $a \equiv b \bmod n$, jika n membagi $(a-b)$.
b) Kumpulan semua bilangan bulat yang mempunyai sisa a jika dibagi oleh n disebut kelas ekivalen dari a dan dinotasikan dengan $[a]_n$. $[a]_n = \{b | b = a + nk, k \in \mathbb{Z}\}$.

c) Definisikan $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \cdots, [n-1]_n\}$.

d) Didefinisikan dua buah operasi pada $\mathbb{Z}_n$, operasi $+$ dan $\cdot$ yaitu untuk sembarang $[a]_n, [b]_n \in \mathbb{Z}_n$, $[a]_n + [b]_n = [a \circ b]_n$ dan $[a]_n \cdot [b]_n = [a * b]_n$, dimana $\circ$ merupakan operasi penjumlahan pada bilangan bulat dan $*$ merupakan operasi perkalian pada bilangan bulat.

(Herstein, *Abstract* 60-61)

Berkaitan dengan definisi $\mathbb{Z}_n$, diperoleh Lemma 2.22.

Lemma 2.22

Untuk setiap $[a]_n, [b]_n \in \mathbb{Z}_n$, $[a]_n = [b]_n$ jika dan hanya jika n membagi $(a - b)$ (Herstein, *Abstract* 61).

$\mathbb{Z}_n$ merupakan salah satu contoh *field*, namun hal ini tidak berlaku apabila n bukan bilangan prima.

Teorema 2.23

$\mathbb{Z}_n$ merupakan *field* jika dan hanya jika n merupakan bilangan prima (Herstein, *Abstract* 133).

Berikut ini akan dibahas mengenai definisi polinomial atas *finite field*.

Definisi 2.24

a) Pandang F suatu *field* dan $x \in X \subseteq F$, suatu ekspresi formal $p(x) = \sum_{i=0}^{n} a_i x^i$, $n \geq 0$, dinamakan polinomial dalam x.

b) Jika a_i, $i = 0,1,2,\dots,n$, koefisien dari polinomial $p(x)$ merupakan anggota F maka $p(x)$ disebut polinomial dalam x atas F.

Kumpulan semua polinomial dalam x atas F dinotasikan dengan $F[x]$.

Berikut ini akan didefinisikan suatu anggota *field* dengan sifat khusus.

Definisi 2.25

Misalkan F suatu *field*. $x^n - \mathbf{1} \in F[x]$.

a) Nilai $\alpha \in F$ yang memenuhi $x^n - \mathbf{1} = \mathbf{0}$ disebut *nth root of unity*.
b) *Order* dari suatu *nth root of unity* α adalah bilangan bulat positif terkecil k sedemikian sehingga $\alpha^k = \mathbf{1}$.
c) Suatu *nth root of unity* yang memiliki order n disebut *primitive nth root of unity*.

(Lidl and Pilz 144)

Definisi 2.26 dan Definisi 2.27 diperlukan untuk pendefinisian suatu jenis polinomial yang akan diberikan pada Definisi 2.28.

Definisi 2.26

a) Misalkan M suatu *field* dan F himpunan bagian dari M. F disebut *subfield* dari M jika F merupakan *field* dengan operasi yang berlaku di M.
b) Misalkan α anggota *field* M dan F *subfield* M. $F(\alpha)$ merupakan irisan dari semua *subfield* dari M yang mengandung F dan α (Lidl and Pilz 129).

Definisi 2.27

Fungsi Euler $\varphi(n)$ didefinisikan dengan $\varphi(1) = 1$, dan untuk $n > 1 \in \mathbb{N}, \varphi(n)$ adalah banyaknya bilangan bulat positif m dengan $1 \leq m < n$ sedemikian sehingga m dan n saling relatif prima yaitu $gcd(m, n) = 1$ (Herstein, *Abstract* 62).

Berikut ini diberikan definisi dari suatu polinomial yang berkaitan dengan *nth root of unity*. Pada bab 3 akan dibahas ciri-ciri dari polinomial tersebut sehingga menjadi polinomial permutasi atas *finite field*.

Definisi 2.28

Misalkan n adalah suatu bilangan bulat positif dan F suatu *field* yang karakteristiknya tidak membagi n. Misalkan α merupakan *primitive nth root of unity* dan $\varphi(n)$ merupakan Fungsi Euler. Polinomial

$$Q_n \coloneqq (x - \alpha_1) \dots (x - \alpha_{\varphi(n)}) \in F(\alpha)[x]$$

dengan $\alpha_1, \alpha_2, \dots, \alpha_{\varphi(n)}$ adalah *primitive nth root of unity* pada $F(\alpha)$, disebut *nth cyclotomic polynomial* atas F (Lidl and Pilz 145).

Berikut beberapa teorema yang berkaitan dengan *cyclotomic polynomial*.

Teorema 2.29

Misalkan Q_n merupakan *nth cyclotomic polynomial* atas *field* F yang karakteristiknya bukan p.

Jika p prima dan p tidak membagi m, maka

a) $Q_{mp^k} = Q_{pm} \circ (x^{p^{k-1}})$

b) $Q_{pm} = \frac{Q_m \circ (x^p)}{Q_m}$

(Lidl and Pilz 151)

Teorema 2.30

Misalkan p prima dan Q_n merupakan *nth cyclotomic polynomial* atas *field F* yang karakteristiknya bukan p. Misalkan pula m bilangan bulat positif. Maka

a) $Q_{p^m} = \mathbf{1} + x^{p^{m-1}} + \cdots + x^{(p-1)p^{m-1}}$

b) $Q_{p^m} = \frac{x^{p^m}-\mathbf{1}}{x^{p^{m-1}}-\mathbf{1}}$

(Lidl and Pilz 146)

Pada Definisi 2.18 diberikan definisi dari gcd dari dua buah bilangan bulat. Teorema 2.31 berikut ini berisi jaminan bahwa gcd dari dua bilangan dapat dinyatakan sebagai kombinasi linier dari dua bilangan tersebut.

Teorema 2.31

Jika a, b merupakan bilangan bulat yang tidak keduanya 0, maka terdapat tepat satu *greatest common divisor* (*gcd*) dari a dan b, misal c, dimana $c = ma + nb$, untuk suatu bilangan bulat m dan n (Herstein, *Abstract* 23).

Karena pada tulisan ini akan dibahas ciri-ciri polinomial permutasi atas *finite field* yang membutuhkan fungsi satu-satu, maka berikut ini diberikan *lemma* mengenai sifat dari komposisi fungsi satu-satu.

Lemma 2.32

Jika $g: S \to T$ dan $f: T \to U$ merupakan fungsi satu-satu maka $f \circ g: S \to U$ juga fungsi satu-satu (Herstein, *Abstract* 12).

Teorema 2.33 berisikan jaminan bahwa setiap bilangan asli yang lebih dari satu dapat dinyatakan sebagai perkalian dari pangkat bilangan prima.

Teorema 2.33

Diberikan $n \in \mathbb{Z}, n > 1$. Maka terdapat tepat satu cara untuk menyatakan n dalam bentuk $n = {p_1}^{a_1} {p_2}^{a_2} \dots {p_k}^{a_k}$, dengan $p_1 < p_2 < p_3 \dots < p_k$ bilangan-bilangan prima, dan $a_1, a_2, \dots, a_k$ bilangan bulat positif (Herstein, *Abstract* 27).

Teorema 2.34 menerangkan bentuk dari koefisien penjumlahan anggota *commutative ring* apabila dipangkatkan dengan bilangan bulat nonnegatif.

Teorema 2.34

Jika x, y anggota *commutative ring* dan n bilangan bulat nonnegatif. Maka

$$(x + y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$$

(Rotman 118)

BAB 3

CIRI-CIRI POLINOMIAL PERMUTASI ATAS *FINITE FIELD*

Pada bab ini akan dibahas ciri-ciri dari polinomial permutasi atas suatu *finite field.*

Pembahasan ini dimulai dengan pengertian polinomial permutasi atas suatu *finite field.*

Definisi 3.1

Suatu polinomial $f(x) \in GF(q)[x]$ merupakan polinomial permutasi jika pemetaan $f: GF(q) \to GF(q)$ adalah pemetaan satu-satu (Mollin and Small 535).

Sebagai contoh, diambil polinomial $f(x) = x^2$ atas *finite field* $\mathbb{Z}_n$, n bilangan prima. Untuk $n = 2$, $f(x) = x^2$ merupakan polinomial permutasi pada $\mathbb{Z}_2$ karena $f([0]_2) = [0]_2$ dan $f([1]_2) = [1]_2$. Sedangkan untuk $n = 3$, $f(x) = x^2$ bukan polinomial permutasi pada $\mathbb{Z}_3$, karena $f([1]_3) = [1]_3 = f([2]_3)$.

Selanjutnya akan dicari syarat agar suatu monomial $f(x) = x^m \in GF(q)[x], m \in \mathbb{N}, m < q$, menjadi polinomial permutasi atas $GF(q)$.

Teorema 3.2

$f(x) = x^k \in GF(q)[x]$, $k < q$, adalah polinomial permutasi jika dan hanya jika $gcd(k, q-1) = 1$.

Bukti

(→)

Jika $f(x) = x^k$ adalah polinomial permutasi maka akan dibuktikan $gcd(k, q-1) = 1$. Pembuktian dilakukan dengan kontradiksi. Andaikan $gcd(k, q-1) \neq 1$ maka terdapat bilangan prima p yang membagi $gcd(k, q-1)$. Hal ini mengakibatkan p membagi $q-1$ dan p membagi k. Karena p membagi k maka $k = pu$, untuk suatu bilangan bulat u. Berdasarkan Teorema 2.16 dan Lemma 2.5, $GF(q) - \{\mathbf{0}\}$ merupakan *finite abelian group* terhadap operasi perkalian di $GF(q)$, dengan $q-1$ buah anggota. Berdasarkan Teorema 2.6, terdapat $a \neq \mathbf{1}$ anggota $GF(q) - \{\mathbf{0}\}$ sedemikian sehingga $a^p = \mathbf{1}$. Maka $a^k = a^{pu} = (a^p)^u = \mathbf{1}^u = \mathbf{1} = \mathbf{1}^k$. Akan tetapi $a \neq \mathbf{1}$. Sehingga didapat $a \neq \mathbf{1} \in GF(q)$ dan $\mathbf{1}$ yang dipetakan ke $\mathbf{1}$. Didapat f bukan fungsi satu-satu. Hal ini kontradiksi dengan yang diketahui bahwa $f(x)$ polinomial permutasi. Jadi, pengandaian bahwa $gcd(k, q-1) \neq 1$ salah. Terbukti bahwa jika $f(x) = x^k$ adalah polinomial permutasi maka $gcd(k, q-1) = 1$.

(←)

Jika diketahui $gcd(k, q-1) = 1$ maka akan dibuktikan bahwa $f(x) = x^k$ adalah polinomial permutasi. Karena $gcd(k, q-1) = 1$ maka berdasarkan Teorema 2.31 terdapat bilangan bulat m dan n, sedemikian sehingga $nk + m(q-1) = 1$. Untuk x_1, x_2 anggota $GF(q)$, jika berlaku $f(x_1) = f(x_2)$ maka akan dibuktikan $x_1 = x_2$.

Pembuktian dibagi menjadi dua kasus yaitu jika $f(x_1) = f(x_2) = \mathbf{0}$ dan jika $f(x_1) = f(x_2) \neq \mathbf{0}$.

Kasus 1:

Jika $f(x_1) = f(x_2) = \mathbf{0}$. ${x_1}^k = {x_2}^k = \mathbf{0}$. Karena $GF(q)$ merupakan *integral domain* maka didapat $x_1 = \mathbf{0} = x_2$.

Kasus 2:

Untuk kasus kedua, jika $f(x_1) = f(x_2) \neq \mathbf{0}$. Jelas x_1 dan x_2 keduanya bukan $\mathbf{0}$. Karena berlaku $f(x_1) = f(x_2)$.

$x_1{}^k = x_2{}^k$

$x_1{}^{nk} = x_2{}^{nk}$

$x_1{}^{nk}\mathbf{1} = x_2{}^{nk}\mathbf{1}$

Karena $x_1, x_2 \neq \mathbf{0} \in GF(q) - \{\mathbf{0}\}$, berdasarkan Teorema 2.16 dan Teorema 2.3, $x_1{}^{(q-1)} = \mathbf{1} = x_2{}^{(q-1)}$. Sehingga $x_1{}^{m(q-1)} = \mathbf{1} = x_2{}^{m(q-1)}$. Didapat

$x_1{}^{nk} x_1{}^{m(q-1)} = x_2{}^{nk} x_2{}^{m(q-1)}$

$x_1{}^{nk+m(q-1)} = x_2{}^{nk+m(q-1)}$

Karena $nk + m(q-1) = 1$ maka

$x_1 = x_2$

Didapat $x_1 = x_2$. Sehingga f adalah fungsi satu-satu. Terbukti $f(x)$ polinomial permutasi.

Berikut ini akan ditunjukkan suatu syarat yang harus dipenuhi oleh suatu polinomial derajat m_n agar menjadi polinomial permutasi. Syarat tersebut adalah syarat dari fungsi-fungsi yang apabila dikomposisi menghasilkan polinomial derajat m_n.

Lemma 3.3

Misalkan $f(x) = \sum_{i=1}^{n} c_i x^{m_i}$ anggota dari $GF(q)[x]$ dimana $m_n > m_{n-1} > \cdots > m_1 \geq 1$ dan $\prod_{i=1}^{n} c_i \neq \mathbf{0}$ dan misalkan pula $e = gcd\{m_i,\ 1 \leq i \leq n\}$.

Maka $f(x)$ polinomial permutasi pada $GF(q)[x]$ jika dan hanya jika $gcd\ (e, q-1) = 1$ dan $\sum_{i=1}^{n} c_i x^{m_i/e}$ adalah polinomial permutasi.

Bukti

Sebut:

$g(x) = x^e$

$h(x) = \sum_{i=1}^{n} c_i x^{m_i/e}$

(←)

Jika diketahui $gcd\ (e, q-1) = 1$ dan $h(x)$ polinomial permutasi maka akan dibuktikan $f(x)$ merupakan polinomial permutasi pada $GF(q)[x]$.

Karena $gcd(e, q-1) = 1$ maka berdasarkan Teorema 3.2, $g(x)$ merupakan polinomial permutasi sehingga g adalah fungsi satu-satu. Karena $h(x)$ polinomial permutasi maka h fungsi satu-satu. Sesuai Lemma 2.32, $h(x) \circ g(x)$ merupakan fungsi satu-satu. Karena $h \circ g = f$, didapat f juga fungsi satu-satu. Didapat $f(x)$ polinomial permutasi.

(→)

Jika diketahui $f(x)$ polinomial permutasi maka akan ditunjukkan bahwa $gcd(e, q-1) = 1$ dan $h(x)$ polinomial permutasi. Pembuktian dilakukan dengan menggunakan bantuan logika proposisi.

Misalkan proposisi:

p: $f(x)$ merupakan polinomial permutasi,

s: $gcd(e, q-1) = 1$,

r: $h(x)$ merupakan polinomial permutasi.

Akan dibuktikan $p \rightarrow s \wedge r$, dimana $p \rightarrow s \wedge r \equiv (\sim s \rightarrow \sim p) \wedge (\sim r \rightarrow \sim p)$.

Akan ditunjukkan $(\sim s \rightarrow \sim p)$. Diketahui $gcd(e, q-1) \neq 1$. Akan dibuktikan $f(x)$ bukan polinomial permutasi. Karena $gcd(e, q-1) \neq 1$ maka berdasarkan Teorema 3.2, $g(x)$ bukan polinomial permutasi. Sehingga g bukan fungsi satu-satu. Diketahui $h(x) \circ g(x) = f(x)$. Karena g bukan fungsi satu-satu maka terdapat z, y anggota $GF(q)$, dengan $z \neq y$, sedemikian sehingga $g(z) = g(y)$. Didapat $h\big(g(z)\big) = h(g(y))$ karena h merupakan fungsi. Maka $f(z) = f(y)$, dimana $z \neq y$, sehingga f bukan fungsi satu-satu. Terbukti $f(x)$ bukan polinomial permutasi.

Berikutnya akan ditunjukkan $(\sim r \rightarrow \sim p)$. Jika diketahui $h(x)$ bukan polinomial permutasi maka akan ditunjukkan bahwa $f(x)$ bukan polinomial permutasi. Karena $h(x)$ bukan polinomial permutasi maka h bukan fungsi satu-satu. Pembuktian dibagi menjadi dua kasus, jika $g(x)$ polinomial permutasi dan jika $g(x)$ bukan polinomial permutasi.

Kasus 1:

Bila $g(x)$ polinomial permutasi. Pembuktian dilakukan dengan kontradiksi. Andaikan $f(x)$ polinomial permutasi. Diketahui $f(x) = h(x) \circ g(x)$, karena g fungsi satu-satu, maka terdapat $g^{-1}(x)$ sedemikian sehingga $f(x) \circ g^{-1}(x) = h(x)$. Berdasarkan Lemma 2.32 didapat h fungsi satu-satu, hal ini kontradiksi dengan yang diketahui bahwa $h(x)$ bukan polinomial permutasi. Jadi pengandaian bahwa $f(x)$ adalah polinomial permutasi salah. Dapat disimpulkan $f(x)$ bukan polinomial permutasi.

Kasus 2:

Bila $g(x)$ bukan polinomial permutasi. Diketahui $f(x) = h(x) \circ g(x)$. Karena g bukan fungsi satu-satu maka terdapat z, y anggota $GF(q)$, dengan $z \neq y$, sedemikian sehingga $g(z) = g(y)$. Karena h adalah fungsi maka $h\big(g(z)\big) = h(g(y))$. Didapat $f(z) = f(y)$, padahal $z \neq y$. Sehingga f bukan fungsi satu-satu. Dapat disimpulkan $f(x)$ bukan polinomial permutasi.

Dari pembuktian $(\sim s \rightarrow \sim p)$ dan $(\sim r \rightarrow \sim p)$ maka $p \rightarrow s \wedge r$ terbukti. Dengan kata lain terbukti:

Jika $f(x)$ adalah polinomial permutasi maka $gcd(e, q-1) = 1$ dan $h(x)$ adalah polinomial permutasi.

Pembahasan selanjutnya adalah pembahasan ciri-ciri dari suatu trinomial derajat k untuk tidak menjadi polinomial permutasi.

Teorema 3.4

Misalkan k, j bilangan bulat positif sedemikian sehingga $q > k > j \geq 1$ dan $gcd(k-j, q-1) = 1$. Maka $ax^k + bx^j + c$ dengan $a \neq \mathbf{0}$ adalah polinomial permutasi atas $GF(q)$ jika dan hanya jika $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

Bukti

Sebut:

$$f(x) = ax^k + bx^j + c$$

$$g(x) = x^k + a^{-1}bx^j$$

Pembuktian dilakukan dengan menggunakan bantuan logika proposisi.

Misalkan proposisi:

p: $f(x)$ adalah polinomial permutasi,

s: $g(x)$ adalah polinomial permutasi,

r: $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

Karena $p \leftrightarrow s$ dan $s \leftrightarrow r$ mengakibatkan $p \leftrightarrow r$, maka pembuktian $p \leftrightarrow r$ dimulai dengan pembuktian $p \leftrightarrow s$.

Dengan perkataan lain akan dibuktikan bahwa $f(x)$ polinomial permutasi jika dan hanya jika $g(x)$ polinomial permutasi.

($\rightarrow$)

Jika diketahui $f(x)$ polinomial permutasi. Akan dibuktikan $g(x)$ polinomial permutasi. Karena $f(x)$ polinomial permutasi maka f fungsi satu-satu. Jika terdapat z, y anggota $GF(q)$ sedemikian sehingga $g(z) = g(y)$, maka $a^{-1}(f(z) - c) = a^{-1}(f(y) - c)$, $(f(z) - c) = (f(y) - c)$, sehingga $f(z) = f(y)$. Karena f fungsi satu-satu maka $z = y$. Sehingga didapat g fungsi satu-satu. Terbukti $g(x)$ polinomial permutasi.

($\leftarrow$)

Jika diketahui $g(x)$ adalah polinomial permutasi. Maka g fungsi satu-satu. Jika terdapat z, y anggota $GF(q)$ sedemikian sehingga $f(z) = f(y)$, didapat $a^{-1}(f(z) - c) = a^{-1}(f(y) - c)$, atau $g(z) = g(y)$. Karena g fungsi satu-satu maka $z = y$. Dapat disimpulkan bahwa f fungsi satu-satu. Terbukti $f(x)$ polinomial permutasi.

Terbukti $p \leftrightarrow s$.

Selanjutnya akan dibuktikan $s \leftrightarrow r$. Dengan perkataan lain akan dibuktikan $g(x)$ polinomial permutasi jika dan hanya jika $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

(←)

Jika diketahui $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$ maka akan dibuktikan $g(x)$ polinomial permutasi. Berdasarkan Teorema 3.2, $g(x)$ adalah polinomial permutasi.

(→)

Jika diketahui $g(x)$ adalah polinomial permutasi akan ditunjukkan $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

Pembuktian dilakukan dengan menggunakan bantuan logika proposisi.

Misalkan proposisi:

t: $gcd(k, q-1) = 1$,

u: $b = \mathbf{0}$.

Akan ditunjukkan $s \to t \wedge u$. Karena

$s \to t \wedge u \equiv (\sim t \to \sim s) \wedge (\sim u \to \sim s)$

maka akan dibuktikan $(\sim t \to \sim s) \wedge (\sim u \to \sim s)$.

Untuk bagian pertama $(\sim t \to \sim s)$

Jika diketahui $gcd(k, q-1) \neq 1$, akan ditunjukkan $g(x)$ bukan polinomial permutasi. Pembuktian dibagi menjadi dua kasus yaitu jika $b = \mathbf{0}$ dan $b \neq \mathbf{0}$.

Kasus 1:

Jika $b = \mathbf{0}$. Untuk kasus pertama jelas dari Teorema 3.2 bahwa jika $gcd(k, q-1) \neq 1$ dan $b = \mathbf{0}$ maka $g(x)$ bukanlah polinomial permutasi.

Kasus 2:

Jika $b \neq \mathbf{0}$. Misalkan $\alpha = -a^{-1}b \neq \mathbf{0}$. Maka $g(x) = x^k - \alpha x^j$, dengan $\alpha \in GF(q)$. Dari premis diketahui bahwa $gcd(k-j, q-1) = 1$, maka berdasarkan Teorema 2.31, terdapat $m, n \in \mathbb{Z}$ sedemikian sehingga $m(k-j) + n(q-1) = 1$.

$\alpha^1 = \alpha$

$\alpha^{m(k-j)+n(q-1)} = \alpha$

$\alpha^{m(k-j)}\alpha^{n(q-1)} = \alpha$

Karena $\alpha \in GF(q) - \{\mathbf{0}\}$, berdasarkan Teorema 2.3 dan Teorema 2.16 maka $\alpha^{n(q-1)} = \mathbf{1}$, sehingga

$\alpha^{m(k-j)} = \alpha$

$(\alpha^m)^{k-j} = \alpha$

Sebut $\alpha^m = y \in GF(q)$. Maka terdapat $y \in GF(q)$ sedemikian sehingga $\alpha = y^{k-j}, y \neq \mathbf{0}$. Diketahui $g(x) = x^k - \alpha x^j = x^j\left(x^{k-j} - \alpha\right) = x^j\left(x^{k-j} - y^{k-j}\right)$. Jadi $g(y) = \mathbf{0} = g(\mathbf{0})$, padahal $y \neq \mathbf{0}$. Jadi, g bukan fungsi satu-satu. Dapat disimpulkan bahwa $g(x)$ bukan polinomial permutasi.

Untuk bagian kedua $(\sim u \rightarrow \sim s)$.

Untuk $b \neq \mathbf{0}$ telah dibuktikan di atas bahwa $g(x)$ bukan polinomial permutasi.

Telah terbukti $(\sim t \rightarrow \sim s) \wedge (\sim u \rightarrow \sim s)$. Maka $s \rightarrow t \wedge u$ terbukti. Dimana $t \wedge u \equiv r$. Sebelumnya telah dibuktikan $r \rightarrow s$. Jadi terbukti pula $s \leftrightarrow r$.

Sebelumnya telah dibuktikan $p \leftrightarrow s$. Sehingga terbukti $p \leftrightarrow r$. Dengan perkataan lain terbukti $f(x) = ax^k + bx^j + c$ adalah polinomial permutasi jika dan hanya jika $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

Berdasarkan Teorema 3.4 didapat Akibat 3.5 yang membahas ciri-ciri polinomial derajat dua untuk menjadi polinomial permutasi.

Akibat 3.5

$ax^2 + bx + c, (a \neq \mathbf{0})$ adalah polinomial permutasi atas $GF(q)$ jika dan hanya jika $b = \mathbf{0}$ dan karakteristik dari $GF(q)$ adalah 2.

Bukti

Analog dengan Teorema 3.4 untuk $k = 2$ dan $j = 1$. $gcd(1, q-1) = 1$. Maka $ax^2 + bx + c$, dengan $a \neq \mathbf{0}$, merupakan polinomial permutasi jika dan hanya jika $b = \mathbf{0}$ dan $gcd(2, q-1) = 1$. Haruslah $q - 1$ ganjil. Atau q genap. Berdasarkan Teorema 2.14, maka karakteristik $GF(q)$ adalah 2.

Akibat 3.6 merupakan akibat lain dari Teorema 3.4 yang berisikan ciri-ciri dari suatu binomial derajat 8 dengan syarat tertentu untuk menjadi polinomial permutasi.

Akibat 3.6

Misalkan $q - 1$ tidak habis dibagi 3, 5, atau 7. Maka $x^8 + ax^t$ untuk t ganjil dan $t < 8$, adalah polinomial permutasi pada $GF(q)$ jika dan hanya jika $a = \mathbf{0}$ dan $GF(q)$ memiliki karakteristik 2.

Bukti

$gcd(8-t, q-1) = 1$ karena $q-1$ tidak habis dibagi 3, 5, 7. Maka syarat Teorema 3.4 terpenuhi. Didapat $x^8 + ax^t$ polinomial permutasi jika dan hanya jika $a = \mathbf{0}$ dan $gcd(8, q-1) = 1$ yaitu $q-1$ ganjil atau q genap. Berdasarkan Teorema 2.14, maka karakteristik $GF(q)$ adalah 2.

Ciri-ciri dari suatu trinomial derajat k untuk tidak menjadi polinomial permutasi telah dibahas pada Teorema 3.4. Teorema 3.7 membahas ciri-ciri dari suatu trinomial derajat k yang memenuhi syarat tambahan tertentu untuk menjadi polinomial permutasi.

Teorema 3.7

Misalkan $f(x) = ax^k + bx^j + c$ merupakan polinomial atas $GF(q)$ dengan $a \neq \mathbf{0}$ dan $-ba^{-1}$ merupakan pangkat ke $(k-j)$ dari suatu anggota dalam $GF(q)$. Maka $f(x)$ polinomial permutasi jika dan hanya jika $b = \mathbf{0}$ pada $GF(q)$ dan $gcd(k, q-1) = 1$.

Bukti

Sebut:

$$g(x) = x^k + a^{-1}bx^j$$

Pembuktian dilakukan dengan menggunakan bantuan logika proposisi.

Misalkan proposisi:

p: $f(x)$ adalah polinomial permutasi,

s: $g(x)$ adalah polinomial permutasi,

r: $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

Karena $p \leftrightarrow s$ dan $s \leftrightarrow r$ mengakibatkan $p \leftrightarrow r$, maka pembuktian $p \leftrightarrow r$ dimulai dengan pembuktian $p \leftrightarrow s$.

Pada pembuktian Teorema 3.4 telah dibuktikan $f(x)$ adalah polinomial permutasi jika dan hanya jika $g(x)$ adalah polinomial permutasi. Dengan demikian $p \leftrightarrow s$ telah terbukti.

Selanjutnya akan dibuktikan $s \leftrightarrow r$.

($\leftarrow$)

Jika diketahui $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$. Berdasarkan Teorema 3.2, $g(x)$ adalah polinomial permutasi.

($\rightarrow$)

Sebaliknya jika diketahui $g(x)$ adalah polinomial permutasi. Akan ditunjukkan $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

Pembuktian dilakukan dengan menggunakan bantuan logika proposisi.

Misalkan proposisi:

t: $gcd(k, q-1) = 1$,

u: $b = \mathbf{0}$.

Maka akan ditunjukkan $s \rightarrow t \wedge u$. Karena

$s \rightarrow t \wedge u \equiv (\sim t \rightarrow \sim s) \wedge (\sim u \rightarrow \sim s)$

maka akan dibuktikan $(\sim t \rightarrow \sim s) \wedge (\sim u \rightarrow \sim s)$.

Untuk bagian pertama $(\sim t \rightarrow \sim s)$

Jika diketahui $gcd(k, q-1) \neq 1$ maka akan ditunjukkan $g(x)$ bukan polinomial permutasi. Akan dibagi menjadi dua kasus yaitu jika $b = \mathbf{0}$ dan $b \neq \mathbf{0}$.

Kasus 1:

Jika $b = \mathbf{0}$. Berdasarkan Teorema 3.2, didapat jika $gcd(k, q-1) \neq 1$ dan $b = \mathbf{0}$ maka $g(x)$ bukanlah polinomial permutasi.

Kasus 2:

Untuk $b \neq \mathbf{0}$. Misalkan $\alpha = -ba^{-1} \neq \mathbf{0}$. Maka $g(x) = x^k - \alpha x^j$, dengan $\alpha \in GF(q)$. Dari premis diketahui bahwa $\alpha = -ba^{-1}$ merupakan pangkat ke $(k-j)$ dari suatu anggota dalam $GF(q)$. Maka terdapat $y \in GF(q)$ sedemikian sehingga $\alpha = y^{k-j}$, $y \neq \mathbf{0}$. Diketahui, $g(x) = x^k - \alpha x^j = x^j(x^{k-j} - \alpha) = x^j(x^{k-j} - y^{k-j})$. Jadi $g(y) = \mathbf{0} = g(\mathbf{0})$, padahal $y \neq \mathbf{0}$. Jadi, g bukan fungsi satu-satu. Dapat disimpulkan bahwa $g(x)$ bukan polinomial permutasi.

Untuk bagian kedua $(\sim u \rightarrow \sim s)$

Untuk $b \neq \mathbf{0}$ telah dibuktikan di atas bahwa $g(x)$ bukan polinomial permutasi.

Telah terbukti $(\sim t \rightarrow \sim s) \wedge (\sim u \rightarrow \sim s)$. Maka $s \rightarrow t \wedge u$ terbukti. Dimana $t \wedge u \equiv r$. Sebelumnya telah dibuktikan $r \rightarrow s$. Jadi terbukti pula $s \leftrightarrow r$.

Juga telah dibuktikan $p \leftrightarrow s$. Jadi terbukti $p \leftrightarrow r$. Dengan perkataan lain terbukti $f(x) = ax^k + bx^j + c$ adalah polinomial permutasi jika dan hanya jika $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

Akibat 3.8 merupakan akibat dari Teorema 3.7. Terdapat sedikit perbedaan dalam premis yang harus dipenuhi pada Akibat 3.8 dibandingkan dengan Teorema 3.7.

Akibat 3.8

Misalkan $f(x) = ax^k + bx^j + c$ merupakan polinomial atas $GF(q)$ dengan $a \neq \mathbf{0}$ dan $-ba^{-1}$ merupakan pangkat ke d dari suatu anggota dalam $GF(q)$, dimana $d = gcd(q-1, k-j)$, maka $f(x)$ merupakan polinomial permutasi jika dan hanya jika $b = \mathbf{0}$ dan $gcd(k, q-1) = 1$.

Bukti

Karena $-ba^{-1}$ merupakan pangkat ke d dari suatu anggota dalam $GF(q)$, dimana $d = gcd(q-1, k-j)$, maka terdapat $y \in GF(q)$ sedemikian sehingga $y^d = -ba^{-1}$. Pembuktian dibagi 2 kasus yaitu jika $y = \mathbf{0}$ dan $y \neq \mathbf{0}$.

Kasus 1:

Jika $y = \mathbf{0}$. Didapat $-ba^{-1} = \mathbf{0}$. Karena $a \neq \mathbf{0}$ dan $GF(q)$ *integral domain* maka $b = \mathbf{0}$. Sehingga $f(x) = ax^k + c$. Namun $f(x)$ polinomial permutasi jika dan hanya jika x^k polinomial permutasi. Berdasarkan Teorema 3.2, $f(x)$ polinomial permutasi jika dan hanya jika $gcd(k, q-1) = 1$.

Kasus 2 :

Jika $y \neq \mathbf{0}$. Karena $d = gcd(q-1, k-j)$, berdasarkan Teorema 2.31, terdapat bilangan bulat m, n sedemikian sehingga $d = m(q-1) + n(k-j)$. Didapat

$$-ba^{-1} = y^d$$

$$-ba^{-1} = y^{m(q-1)+n(k-j)}$$

$$-ba^{-1} = y^{m(q-1)} y^{n(k-j)}$$

Karena $y \in GF(q) - \{\mathbf{0}\}$ dan berdasarkan Teorema 2.3 dan Teorema 2.16, maka $y^{(q-1)} = \mathbf{1}$. Sehingga

$$-ba^{-1} = y^{n(k-j)}$$

$$-ba^{-1} = (y^n)^{(k-j)}$$

Sebut $y^n = z \in GF(q)$. Maka $-ba^{-1} = z^{(k-j)}$, $z \in GF(q)$. Berdasarkan Teorema 3.7, $f(x)$ polinomial permutasi jika dan hanya jika $b = \mathbf{0}$ dan $gcd(k, q-1) = 1$.

Seperti Teorema 3.7 maupun Akibat 3.8, Teorema 3.9 membahas ciri-ciri trinomial derajat k agar menjadi polinomial permutasi. Namun pada Teorema 3.9, pangkat tertinggi kedua dari trinomial membagi derajat trinomial tersebut.

Teorema 3.9

Misalkan $f(x) = ax^k + bx^j + c \in GF(q)[x]$ dimana j membagi k, $a \neq \mathbf{0}$, $gcd\left(\left(\frac{k}{j}\right) - 1, q-1\right) = d$, dan $gcd(j, q-1) = 1$. Misalkan pula $-ba^{-1}\beta^{-1}$ merupakan pangkat ke d dari suatu anggota pada $GF(q)$, dimana $\beta = z^{\left(\frac{k}{j}\right)-1} + z^{\left(\frac{k}{j}\right)-2} + \cdots + \mathbf{1}$ untuk suatu $z \in GF(q), z \neq \mathbf{1}$. Maka $f(x)$ merupakan polinomial permutasi jika dan hanya jika $b = \mathbf{0}$ dan $gcd(k, q-1) = 1$.

Bukti

Sebut:

$$g(x) = x^k + a^{-1}bx^j$$

Pembuktian dilakukan dengan menggunakan bantuan logika proposisi.

Misalkan proposisi:

p: $f(x)$ adalah polinomial permutasi,

s: $g(x)$ adalah polinomial permutasi,

r: $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

Karena $p \leftrightarrow s$ dan $s \leftrightarrow r$ mengakibatkan $p \leftrightarrow r$ maka pembuktian $p \leftrightarrow r$ dimulai dengan pembuktian $p \leftrightarrow s$.

Pada pembuktian Teorema 3.4 telah dibuktikan $f(x)$ adalah polinomial permutasi jika dan hanya jika $g(x)$ adalah polinomial permutasi. Dengan demikian $p \leftrightarrow s$ telah terbukti.

Selanjutnya akan dibuktikan $s \leftrightarrow r$.

($\leftarrow$)

Jika diketahui $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$. Berdasarkan Teorema 3.2, didapat $g(x)$ adalah polinomial permutasi.

($\rightarrow$)

Jika diketahui $g(x)$ adalah polinomial permutasi maka akan dibuktikan $gcd(k, q-1) = 1$ dan $b = \mathbf{0}$.

Pembuktian akan dilakukan dengan bantuan logika proposisi.

Misalkan proposisi:

t: $gcd(k, q-1) = 1$,

u: $b = \mathbf{0}$.

Maka akan ditunjukkan $s \rightarrow t \wedge u$. Karena

$s \rightarrow t \wedge u \equiv (\sim t \rightarrow \sim s) \wedge (\sim u \rightarrow \sim s)$

maka akan ditunjukkan $(\sim t \rightarrow \sim s) \wedge (\sim u \rightarrow \sim s)$.

Untuk bagian pertama $(\sim t \rightarrow \sim s)$

Jika diketahui $gcd(k, q-1) \neq 1$, akan ditunjukkan $g(x)$ bukan polinomial permutasi. Pembuktian dibagi menjadi dua kasus yaitu jika $b = \mathbf{0}$ dan $b \neq \mathbf{0}$.

Kasus 1:

Jika $b = \mathbf{0}$. Berdasarkan Teorema 3.2, didapat bahwa jika $gcd(k, q-1) \neq 1$ dan $b = \mathbf{0}$ maka $g(x)$ bukanlah polinomial permutasi.

Kasus 2:

Jika $b \neq \mathbf{0}$.

Sebut:

$h(x) = x^{\frac{k}{j}} + a^{-1}bx$

$i(x) = x^j$

Dari premis diketahui bahwa $gcd(j, q-1) = 1$, maka berdasarkan Teorema 3.2, $i(x)$ merupakan polinomial permutasi. Sehingga i merupakan fungsi satu-satu.

Misalkan proposisi:

v: $h(x)$ adalah polinomial permutasi.

Akan dibuktikan bahwa $g(x)$ polinomial permutasi jika dan hanya jika $h(x)$ polinomial permutasi. Atau akan dibuktikan $s \leftrightarrow v$.

($\rightarrow$)

Jika diketahui $g(x)$ merupakan polinomial permutasi. Akan dibuktikan bahwa $h(x)$ merupakan polinomial permutasi. Telah diketahui bahwa $i(x)$ merupakan fungsi satu-satu, dimana $g(x) = h(x) \circ i(x)$. Karena $i(x)$ fungsi satu-satu maka terdapat $i^{-1}(x)$ fungsi invers dari $i(x)$ yang merupakan fungsi satu-satu pula. Sehingga didapat $g(x) \circ i^{-1}(x) = h(x)$. Dimana $g(x)$ dan $i^{-1}(x)$ merupakan fungsi satu-satu. Sehingga berdasarkan Lemma 2.32, $h(x)$ merupakan fungsi satu-satu. Terbukti bahwa $h(x)$ merupakan polinomial permutasi.

($\leftarrow$)

Jika diketahui $h(x)$ adalah polinomial permutasi maka akan dibuktikan bahwa $g(x)$ merupakan polinomial permutasi pula. Telah diketahui bahwa i merupakan fungsi satu-satu, dimana $g(x) = h(x) \circ i(x)$. Sehingga berdasarkan Lemma 2.32, g merupakan fungsi satu-satu pula.

Terbukti $s \leftrightarrow v$. Atau terbukti $g(x)$ polinomial permutasi jika dan hanya jika $h(x)$ polinomial permutasi.

Karena telah terbukti $g(x)$ polinomial permutasi jika dan hanya jika $h(x)$ polinomial permutasi maka selanjutnya untuk membuktikan $g(x)$ bukan polinomial permutasi jika diketahui $gcd(k, q-1) \neq 1$ dan $b \neq \mathbf{0}$, cukup dibuktikan $h(x)$ bukan polinomial permutasi jika diketahui $gcd(k, q-1) \neq 1$ dan $b \neq \mathbf{0}$.

Akan dibuktikan $h(x)$ bukan polinomial permutasi jika diketahui $gcd(k, q-1) \neq 1$ dan $b \neq \mathbf{0}$.

Misalkan $\frac{k}{j} = k'$. Dimana k' merupakan bilangan bulat karena dari premis diketahui bahwa j membagi k. Dari premis diketahui $-ba^{-1}\beta^{-1}$ merupakan

pangkat ke d dari suatu anggota pada $GF(q)$, dimana $\beta = z^{\left(\frac{k}{j}\right)-1} + z^{\left(\frac{k}{j}\right)-2} + \cdots + \mathbf{1}$ untuk suatu $z \in GF(q), z \neq \mathbf{1}$. Misalkan $\alpha = -ba^{-1} \neq \mathbf{0}$. Maka didapat $\alpha\beta^{-1} = {y_1}^d \neq \mathbf{0}$, untuk y_1 suatu anggota $GF(q) - \{\mathbf{0}\}$ dan $d = gcd(k' - 1, q - 1)$. Berdasarkan Teorema 2.31, terdapat bilangan bulat m, n sedemikian sehingga $m(k' - 1) + n(q - 1) = d$. Sehingga

$$\alpha\beta^{-1} = {y_1}^{m(k'-1)+n(q-1)}$$

$$\alpha\beta^{-1} = {y_1}^{m(k'-1)}{y_1}^{n(q-1)}$$

Karena $y_1 \in GF(q) - \{\mathbf{0}\}$ maka berdasarkan Teorema 2.3 dan Teorema 2.16, didapat ${y_1}^{n(q-1)} = \mathbf{1}$. Sehingga

$$\alpha\beta^{-1} = {y_1}^{m(k'-1)}$$

$$\alpha\beta^{-1} = (y_1^m)^{(k'-1)}$$

Misalkan $y_1^m = y \neq \mathbf{0}$ suatu anggota $GF(q)$. Sehingga $\alpha = y^{k'-1}\beta$.

Diketahui

$$\beta = z^{k'-1} + z^{k'-2} + z^{k'-3} + \cdots + \mathbf{1}.$$

Misalkan $x = yz$. ($x \neq y$ karena $z \neq \mathbf{1}$)

$$\alpha = y^{k'-1}\beta$$

$$\alpha = y^{k'-1}(z^{k'-1} + z^{k'-2} + z^{k'-3} + \cdots + \mathbf{1})$$

$$\alpha = y^{k'-1}z^{k'-1} + y^{k'-1}z^{k'-2} + y^{k'-1}z^{k'-3} + \cdots + y^{k'-1}$$

$$\alpha = x^{k'-1} + x^{k'-2}y + x^{k'-3}y^2 + \cdots + y^{k'-1} \qquad (3.1)$$

$$\alpha(x-y) = \alpha x - \alpha y \qquad (3.2)$$

Substitusi (3.1) pada (3.2):

$$\alpha(x-y) = \left[\left(x^{k'-1} + x^{k'-2}y + x^{k'-3}y^2 + \cdots + y^{k'-1}\right)x\right] - \left[\left(x^{k'-1} + x^{k'-2}y + x^{k'-3}y^2 + \cdots + y^{k'-1}\right)y\right]$$

$$\alpha(x-y) = \left[x^{k'} + x^{k'-1}y + x^{k'-2}y^2 + \cdots + xy^{k'-1}\right] - \left[x^{k'-1}y + x^{k'-2}y^2 + x^{k'-3}y^3 + \cdots + y^{k'}\right]$$

$$\alpha(x-y) = x^{k'} - y^{k'}$$

$$\alpha x - \alpha y = x^{k'} - y^{k'}$$

$$y^{k'} - \alpha y = x^{k'} - \alpha x$$

Karena $k' = \frac{k}{j}$ dan $\alpha = -a^{-1}b$ maka didapat

$$y^{\frac{k}{j}} + a^{-1}by = x^{\frac{k}{j}} + a^{-1}bx$$

$$h(y) = h(x)$$

Didapat $h(y) = h(x)$ padahal $x \neq y$. Jadi h bukanlah fungsi satu-satu. Terbukti $h(x)$ bukan polinomial permutasi. Sebelumnya telah dibuktikan $g(x)$ polinomial permutasi jika dan hanya jika $h(x)$ polinomial permutasi. Sehingga terbukti $g(x)$ bukan polinomial permutasi jika diketahui $gcd(k, q-1) \neq 1$. Atau terbukti bagian pertama yaitu $(\sim t \rightarrow \sim s)$.

Untuk bagian kedua $(\sim u \rightarrow \sim s)$.

Untuk $b \neq \mathbf{0}$ telah dibuktikan di atas bahwa g bukan polinomial permutasi.

Telah terbukti $(\sim t \rightarrow \sim s) \wedge (\sim u \rightarrow \sim s)$. Maka $s \rightarrow t \wedge u$ terbukti. Dimana $t \wedge u \equiv r$. Sebelumnya telah dibuktikan $r \rightarrow s$. Jadi terbukti pula $s \leftrightarrow r$.

Juga telah dibuktikan $p \leftrightarrow s$. Jadi terbukti $p \leftrightarrow r$. Dengan perkataan lain terbukti $f(x) = ax^k + bx^j + c$ adalah polinomial permutasi jika dan hanya jika $gcd(k, q - 1) = 1$ dan $b = \mathbf{0}$.

Teorema 3.10 membahas syarat perlu dari suatu trinomial agar menjadi polinomial permutasi. Namun trinomial pada Teorema 3.10 dibatasi pada trinomial yang selisih antara derajatnya dengan pangkat tertinggi keduanya adalah dua.

Teorema 3.10

Jika $f(x) = ax^k + bx^{k-2} + c$ (dimana $a \neq \mathbf{0}$ dan $k \geq 2$) merupakan polinomial permutasi pada $GF(q)$ maka $q \not\equiv \pm 1 \ (mod\ k)$ atau $b = \mathbf{0}$.

Bukti

Sebut:

$$g(x) = x^k + a^{-1}bx^{k-2}$$

Pada pembuktian Teorema 3.4 telah dibuktikan $ax^k + bx^j + c$ adalah polinomial permutasi jika dan hanya jika $x^k + a^{-1}bx^j$ adalah polinomial permutasi. Misalkan $k - 2 = j$, maka terbukti bahwa $f(x)$ merupakan polinomial permutasi jika dan hanya jika $g(x)$ merupakan polinomial permutasi. Sehingga selanjutnya akan dibuktikan jika $g(x)$ merupakan polinomial permutasi pada $GF(q)$ maka $q \not\equiv \pm 1 \ (mod\ k)$ atau $b = \mathbf{0}$. Pembuktian dilakukan dengan kontradiksi. Sebut $\alpha = -a^{-1}b$, maka

$$g(x) = x^k - \alpha x^{k-2}$$

Pembuktian dilakukan dengan menggunakan bantuan logika proposisi.

Misalkan proposisi:

r: $g(x)$ polinomial permutasi atas $GF(q)$

s: $q \not\equiv \pm 1 \ (mod\ k)$ atau $b = \mathbf{0}$

Akan dibuktikan $r \rightarrow s$

Diketahui $g(x)$ polinomial permutasi, andaikan $q \equiv \pm 1 \ (mod\ k)$ dan $b \neq \mathbf{0}$. Misalkan $n = \frac{q \pm 1}{k}$. Akan dibuktikan $n \neq q - 1$. Pembuktian dengan kontradiksi dibagi menjadi dua kasus.

Kasus 1:

Jika $n = \frac{q-1}{k}$. Andaikan $n = q - 1$. Maka $k = 1$. Kontradiksi dengan premis bahwa $k \geq 2$.

Kasus 2:

Kasus kedua jika $n = \frac{q+1}{k}$. Andaikan $n = q - 1$. Maka

$$q - 1 = \frac{q + 1}{k}$$

$$k(q - 1) = q + 1$$

$$kq - k = q + 1$$

$$kq - q = k + 1$$

$$q(k - 1) = k + 1$$

$$q = \frac{k - 1 + 2}{k - 1}$$

$$q = 1 + \frac{2}{k - 1}$$

Karena q merupakan bilangan bulat positif, maka haruslah $k = 2$ atau $k = 3$. Untuk kasus pertama jika $k = 2$ maka $q = 3$. Sehingga $g(x) = x^k - \alpha x^{k-2} = x^2 - \alpha$. $g(x)$ polinomial permutasi jika dan hanya jika x^2 polinomial permutasi. Namun berdasarkan Teorema 3.2, x^2 polinomial permutasi jika dan hanya jika $gcd(2, q - 1) = 1$. Namun, jika $k = 2$ maka $q = 3$ sehingga $gcd(2, 3 - 1) = 2$. Sehingga, x^2 bukan polinomial permutasi. Didapat $g(x)$ bukan polinomial permutasi. Hal ini kontradiksi dengan yang diketahui di premis bahwa $g(x)$ polinomial permutasi. Untuk kasus kedua jika $k = 3$. Didapat $q = 2$. Maka anggota dari $GF(q)$ hanyalah $\mathbf{1}$ dan $\mathbf{0}$. Dan $g(x) = x^k - \alpha x^{k-2} = x^3 - \alpha x$. $g(\mathbf{0}) = \mathbf{0} = g(\mathbf{1})$, sehingga $g(x)$ bukan polinomial permutasi. Hal ini kontradiksi dengan yang diketahui di premis bahwa $g(x)$ polinomial permutasi.

Karena pada kedua kasus terjadi kontradiksi, maka $n \neq q - 1$.

Karena $g(x) = x^k - \alpha x^{k-2}$ merupakan polinomial permutasi maka g fungsi satu-satu, sehingga $\sum_{x \in GF(q)} g(x) = \sum_{x \in GF(q)} x$. Karena $n \neq q - 1$, berdasarkan Lemma 2.20, $\sum_{x \in GF(q)} g(x)^n = \sum_{x \in GF(q)} (x^k - \alpha x^{k-2})^n = \sum_{x \in GF(q)} x^n = \mathbf{0}$. Berdasarkan Teorema 2.34, didapat

$$\mathbf{0} = \sum_{x \in GF(q)} \sum_{i=0}^{n} \binom{n}{i} x^{k(n-i)} (-\alpha x^{k-2})^i$$

$$\mathbf{0} = \sum_{x \in GF(q)} \sum_{i=0}^{n} \binom{n}{i} x^{k(n-i)+(k-2)i} (-\alpha)^i$$

$$\mathbf{0} = \sum_{x \in GF(q)} \sum_{i=0}^{n} \binom{n}{i} x^{kn-2i} (-\alpha)^i$$

$$\mathbf{0} = \sum_{i=0}^{n} \binom{n}{i} (-\alpha)^i \sum_{x \in GF(q)} x^{kn-2i}$$

Berdasarkan Lemma 2.20, $\sum_{x\in GF(q)} x^{kn-2i} = \mathbf{0}$ kecuali jika $kn-2i = q-1$. $kn-2i = q-1$ terjadi ketika $i = 0$ (ketika $nk = q-1$) atau $i = 1$ (ketika $nk = q+1$). Akan dilihat nilai dari $\sum_{i=0}^{n} \binom{n}{i} (-\alpha)^i \sum_{x\in GF(q)} x^{kn-2i}$ pada kedua kasus tersebut.

Kasus 1:

Jika $nk = q-1$ ketika $i = 0$.

$$\mathbf{0} = \sum_{i=0}^{n} \binom{n}{i} (-\alpha)^i \sum_{x\in GF(q)} x^{kn-2i} = \binom{n}{0} (-\alpha)^0 \sum_{x\in GF(q)} x^{kn-0} = \sum_{x\in GF(q)} x^{q-1}$$

Hal ini kontradiksi dengan $\sum_{x\in GF(q)} x^{q-1} = -\mathbf{1}$ berdasarkan Lemma 2.20.

Kasus 2:

Jika $nk = q+1$ ketika $i = 1$.

$$\mathbf{0} = \sum_{i=0}^{n} \binom{n}{i} (-\alpha)^i \sum_{x\in GF(q)} x^{kn-2i} = \binom{n}{1} (-\alpha)^1 \sum_{x\in GF(q)} x^{kn-2} = n(-\alpha) \sum_{x\in GF(q)} x^{q-1} \quad (3.3)$$

Karena $\alpha \neq \mathbf{0}$ maka

$$\mathbf{0} + \alpha \neq \mathbf{0}$$

Berdasarkan Teorema 2.3 dan fakta bahwa *finite field* $GF(q)$ merupakan *finite group* terhadap operasi penjumlahan pada $GF(q)$, maka

$$q\alpha + \alpha \neq \mathbf{0}$$

$$(q+1)\alpha \neq \mathbf{0}$$

$$nk\alpha \neq \mathbf{0}$$

$n\alpha \neq \mathbf{0}$

Karena $n\alpha \neq \mathbf{0}$ maka $n(-\alpha) \neq \mathbf{0}$. Dari (3.3):

$$\mathbf{0} = n(-\alpha) \sum_{x \in GF(q)} x^{q-1}$$

Karena $n(-\alpha) \neq \mathbf{0}$ dan $GF(q)$ merupakan *integral domain* maka haruslah $\sum_{x \in GF(q)} x^{q-1} = \mathbf{0}$. Hal ini kontradiksi dengan $\sum_{x \in GF(q)} x^{q-1} = -\mathbf{1}$, berdasarkan Lemma 2.20.

Telah dibuktikan terjadi kontradiksi pada kasus kedua yaitu kasus jika $nk = q + 1$ ketika $i = 1$. Telah dibuktikan pula terjadi kontradiksi pada kasus pertama yaitu kasus jika $nk = q - 1$ ketika $i = 0$. Maka terbukti pengandaian awal $q \equiv \pm 1 \ (mod\ k)$ dan $b \neq \mathbf{0}$ salah. Jadi, apabila diketahui $g(x) = x^k - \alpha x^{k-2}$, dengan $\alpha = -a^{-1}b$, polinomial permutasi atas $GF(q)$ maka $q \not\equiv \pm 1 \ (mod\ k)$ atau $b = \mathbf{0}$. Dengan kata lain terbukti $r \rightarrow s$. Karena telah terbukti $f(x) = ax^k + bx^{k-2} + c$ merupakan polinomial permutasi jika dan hanya jika $g(x) = x^k + a^{-1}bx^{k-2}$ merupakan polinomial permutasi maka terbukti pula jika $f(x) = ax^k + bx^{k-2} + c$ merupakan polinomial permutasi atas $GF(q)$ maka $q \not\equiv \pm 1 \ (mod\ k)$ atau $b = \mathbf{0}$.

Akibat 3.11 merupakan akibat dari Teorema 3.10, yaitu kasus khusus untuk polinomial derajat 3 atas *finite field* yang karakteristiknya bukan 3.

Akibat 3.11

Misalkan $GF(q)$ *field* dengan karakteristik tidak sama dengan 3. Maka $f(x) = ax^3 + bx^2 + cx + d$ dimana $a \neq \mathbf{0}$ merupakan polinomial permutasi pada $GF(q)$ jika dan hanya jika $b^2 = 3ac$ dan $q \equiv 2 \ (mod\ 3)$.

Bukti

Sebut:

$$g(x) = x^3 + a^{-1}bx^2 + a^{-1}cx$$

Pembuktian dilakukan dengan menggunakan bantuan logika proposisi.

Misalkan proposisi:

p: $f(x)$ merupakan polinomial permutasi,

r: $g(x)$ merupakan polinomial permutasi.

Akan dibuktikan bahwa $f(x)$ merupakan polinomial permutasi jika dan hanya jika $g(x)$ merupakan polinomial permutasi. Atau akan dibuktikan $p \leftrightarrow r$.

($\rightarrow$)

Jika diketahui $f(x)$ merupakan polinomial permutasi maka akan dibuktikan bahwa $g(x)$ polinomial permutasi.

Misalkan terdapat w, z anggota $GF(q)$, sedemikian sehingga $g(w) = g(z)$. Maka $ag(w) = ag(z)$. Dan $ag(w) + d = ag(z) + d$. Sehingga didapat $f(w) = f(z)$. Karena $f(x)$ merupakan polinomial permutasi, maka f fungsi satu-satu. Karena f fungsi satu-satu maka $w = z$. Terbukti jika terdapat w, z anggota $GF(q)$,sedemikian sehingga $g(w) = g(z)$ maka $w = z$. Terbukti bahwa g fungsi satu-satu, sehingga $g(x)$ merupakan polinomial permutasi.

($\leftarrow$)

Jika diketahui $g(x)$ merupakan polinomial permutasi akan dibuktikan bahwa $f(x)$ polinomial permutasi.

Misalkan terdapat w, z anggota $GF(q)$, sedemikian sehingga $f(w) = f(z)$. Maka $f(w) - d = f(z) - d$. Dan $a^{-1}(f(w) - d) = a^{-1}(f(z) - d)$. Sehingga didapat $g(w) = g(z)$. Karena $g(x)$ polinomial permutasi maka g

fungsi satu-satu. Karena g fungsi satu-satu maka $w = z$. Terbukti jika terdapat w, z anggota $GF(q)$, sedemikian sehingga $f(w) = f(z)$ maka $w = z$. Terbukti bahwa f fungsi satu-satu, sehingga $f(x)$ merupakan polinomial permutasi.

Telah dibuktikan bahwa $f(x)$ merupakan polinomial permutasi jika dan hanya jika $g(x)$ polinomial permutasi. Atau terbukti $p \leftrightarrow r$.

Rubah bentuk $g(x) = x^3 + a^{-1}bx^2 + a^{-1}cx$ menjadi bentuk $g(x) = x(x^2 + a^{-1}bx + a^{-1}c)$. Pilih $y = x + b(3a)^{-1}$ maka $x = y - b(3a)^{-1}$. Substitusi $x = y - b(3a)^{-1}$ pada $x(x^2 + a^{-1}bx + a^{-1}c)$. Didapat

$$x(x^2 + a^{-1}bx + a^{-1}c) = y - b(3a)^{-1}[(y - b(3a)^{-1})^2 + a^{-1}b(y - b(3a)^{-1}) + a^{-1}c]$$

Misal $g(x) = L$. Karena $x(x^2 + a^{-1}bx + a^{-1}c) = g(x)$. Maka

$$L = y - b(3a)^{-1}[(y - b(3a)^{-1})^2 + a^{-1}b(y - b(3a)^{-1}) + a^{-1}c]$$

$$L = y - b(3a)^{-1}[y^2 - 2yb(3a)^{-1} + b^2(3a)^{-2} + a^{-1}by - a^{-1}b^2(3a)^{-1} + a^{-1}c]$$

$$L = \{y^3 - 2y^2b(3a)^{-1} + yb^2(3a)^{-2} + a^{-1}by^2 - ya^{-1}b^2(3a)^{-1} + ya^{-1}c\} + \{-b(3a)^{-1}y^2 + 2yb^2(3a)^{-2} - b^3(3a)^{-3} - a^{-1}b^2y(3a)^{-1} + a^{-1}b^3(3a)^{-2} - b(3a)^{-1}a^{-1}c\}$$

$$L = y^3 + y^2\{-2b(3a)^{-1} + a^{-1}b - b(3a)^{-1}\} + y\{b^2(3a)^{-2} - a^{-1}b^2(3a)^{-1} + a^{-1}c + 2b^2(3a)^{-2} - a^{-1}b^2(3a)^{-1}\} + \{-b^3(3a)^{-3} + a^{-1}b^3(3a)^{-2} - b(3a)^{-1}a^{-1}c\}$$

Sebut $-b^3(3a)^{-3} + a^{-1}b^3(3a)^{-2} - b(3a)^{-1}a^{-1}c = d'$, maka

$$L = y^3 + y^2\{-2b(3a)^{-1} + a^{-1}b - b(3a)^{-1}\} + y\{b^2(3a)^{-2} - a^{-1}b^2(3a)^{-1} + a^{-1}c + 2b^2(3a)^{-2} - a^{-1}b^2(3a)^{-1}\} + d' \qquad (3.4)$$

Pandang koefisien dari y. Sebut $b^2(3a)^{-2} - a^{-1}b^2(3a)^{-1} + a^{-1}c + 2b^2(3a)^{-2} - a^{-1}b^2(3a)^{-1} = W$. Maka

$$W = b^2(3a)^{-2} - a^{-1}b^2(3a)^{-1} + a^{-1}c + 2b^2(3a)^{-2} - a^{-1}b^2(3a)^{-1}$$

$$W = 3b^2(3a)^{-2} - 2a^{-1}b^2(3a)^{-1} + a^{-1}c$$

$$W = 3b^2(3a)^{-2} - 2b^2a^{-1}(a + a + a)^{-1} + a^{-1}c$$

$$W = 3b^2(3a)^{-2} - 2b^2((a + a + a)a)^{-1} + a^{-1}c$$

$$W = 3b^2(3a)^{-2} - 2b^2(a^2 + a^2 + a^2)^{-1} + a^{-1}c$$

$$W = 3b^2(3a)^{-2} - 2b^2(3a^2)^{-1} + a^{-1}c$$

$$W = 3b^2((a + a + a)^2)^{-1} - 2b^2(3a^2)^{-1} + a^{-1}c$$

$$W = 3b^2(9a^2)^{-1} - 2b^2(3a^2)^{-1} + a^{-1}c \quad (3.5)$$

Pandang bentuk $3b^2(9a^2)^{-1}$. Akan dibuktikan $3b^2(9a^2)^{-1} = b^2(3a^2)^{-1}$.

$$3b^2 = 3b^2$$

$$3b^2 = b^2 + b^2 + b^2$$

$$3b^2 = b^2[\mathbf{1} + \mathbf{1} + \mathbf{1}]$$

$$3b^2 = b^2[(a^2 + a^2 + a^2)^{-1}(a^2 + a^2 + a^2) + (a^2 + a^2 + a^2)^{-1}(a^2 + a^2 + a^2) + (a^2 + a^2 + a^2)^{-1}(a^2 + a^2 + a^2)]$$

$$3b^2 = b^2(a^2 + a^2 + a^2)^{-1}[(a^2 + a^2 + a^2) + (a^2 + a^2 + a^2) + (a^2 + a^2 + a^2)]$$

$$3b^2 = b^2(a^2 + a^2 + a^2)^{-1}(9a^2)$$

$$3b^2(9a^2)^{-1} = b^2(a^2 + a^2 + a^2)^{-1}(9a^2)(9a^2)^{-1}$$

$$3b^2(9a^2)^{-1} = b^2(3a^2)^{-1}\mathbf{1}$$

$$3b^2(9a^2)^{-1} = b^2(3a^2)^{-1}$$

Terbukti $3b^2(9a^2)^{-1} = b^2(3a^2)^{-1}$.

Dari (3.5)

$$W = 3b^2(9a^2)^{-1} - 2b^2(3a^2)^{-1} + a^{-1}c$$

Karena $3b^2(9a^2)^{-1} = b^2(3a^2)^{-1}$ maka

$$W = b^2(3a^2)^{-1} - 2b^2(3a^2)^{-1} + a^{-1}c$$

$$W = -b^2(3a^2)^{-1} + a^{-1}c \qquad (3.6)$$

Pandang bentuk $a^{-1}c$. Akan dibuktikan $a^{-1}c = (3a^2)^{-1}(3ac)$.

$$3ac = 3ac$$

$$3ac = ac + ac + ac$$

$$3ac = \mathbf{1}ac + \mathbf{1}ac + \mathbf{1}ac$$

$$3ac = a^{-1}aac + a^{-1}aac + a^{-1}aac$$

$$3ac = a^{-1}a^2c + a^{-1}a^2c + a^{-1}a^2c$$

$$3ac = a^2a^{-1}c + a^2a^{-1}c + a^2a^{-1}c$$

$$3ac = (a^2 + a^2 + a^2)a^{-1}c$$

$$3ac = (3a^2)a^{-1}c$$

$$(3a^2)^{-1}(3ac) = (3a^2)^{-1}(3a^2)a^{-1}c$$

$$(3a^2)^{-1}(3ac) = \mathbf{1}a^{-1}c$$

$$(3a^2)^{-1}(3ac) = a^{-1}c$$

Terbukti $a^{-1}c = (3a^2)^{-1}(3ac)$.

Dari (3.6) dan $a^{-1}c = (3a^2)^{-1}(3ac)$.

$$W = -b^2(3a^2)^{-1} + a^{-1}c$$

$$W = (3a^2)^{-1}(3ac - b^2)$$

Substitusi $W = (3a^2)^{-1}(3ac - b^2)$ pada (3.4) dan dengan pemisalan bahwa W merupakan koefisien dari y.

$$L = y^3 + y^2\{-2b(3a)^{-1} + a^{-1}b - b(3a)^{-1}\} + y\{(3a^2)^{-1}(3ac - b^2)\} + d' \quad (3.7)$$

Pandang koefisien dari y^2. Sebut $-2b(3a)^{-1} + a^{-1}b - b(3a)^{-1} = Z$. Maka

$$Z = -2b(3a)^{-1} + a^{-1}b - b(3a)^{-1}$$

$$Z = -3b(3a)^{-1} + a^{-1}b \quad (3.8)$$

Pandang bentuk $3b(3a)^{-1}$. Akan dibuktikan $3b(3a)^{-1} = ba^{-1}$.

$$3b = 3b$$

$$3b = b + b + b$$

$$3b = b\mathbf{1} + b\mathbf{1} + b\mathbf{1}$$

$$3b = ba^{-1}a + ba^{-1}a + ba^{-1}a$$

$$3b = ba^{-1}(a + a + a)$$

$$3b = ba^{-1}(3a)$$

$$3b(3a)^{-1} = ba^{-1}(3a)(3a)^{-1}$$

$$3b(3a)^{-1} = ba^{-1}\mathbf{1}$$

$$3b(3a)^{-1} = ba^{-1}$$

Terbukti $3b(3a)^{-1} = ba^{-1}$.

Dari (3.8)

$$Z = -3b(3a)^{-1} + a^{-1}b$$

Substitusi $3b(3a)^{-1} = ba^{-1}$. Maka

$$Z = -ba^{-1} + a^{-1}b$$

$$Z = \mathbf{0}$$

Dari (3.7) dan $Z = \mathbf{0}$.

$$L = y^3 + y\{(3a^2)^{-1}(3ac - b^2)\} + d'$$

Sebut $(3a^2)^{-1}(3ac - b^2) = c'$.

Didapat

$$L = y^3 + y\,c' + d'$$

Karena $L = g(x) = x(x^2 + a^{-1}bx + a^{-1}c)$, didapat $x(x^2 + a^{-1}bx + a^{-1}c) = y^3 + y\,c' + d'$, dimana $c' = (3a^2)^{-1}(3ac - b^2)$.

Pada pembuktian Teorema 3.4 telah dibuktikan $ax^k + bx^j + c$ adalah polinomial permutasi jika dan hanya jika $x^k + a^{-1}bx^j$ adalah polinomial permutasi. Misalkan $a = \mathbf{1}$, $k = 3$, $j = 1$, $b = c'$, dan $c = d'$ maka $y^3 + y\,c' + d'$ adalah polinomial permutasi jika dan hanya jika $y^3 + c'y$ adalah polinomial permutasi. Misalkan $c' = (3a^2)^{-1}(3ac - b^2) = -\alpha$. Sehingga $\alpha = (3a^2)^{-1}(b^2 - 3ac)$. Jadi untuk membuktikan $x(x^2 + a^{-1}bx + a^{-1}c)$ merupakan polinomial permutasi cukup dengan membuktikan bahwa $y^3 - \alpha y$ merupakan polinomial permutasi, dimana $\alpha = (3a^2)^{-1}(b^2 - 3ac)$.

Sebut:

$h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$.

Akan dibuktikan $h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$, adalah polinomial permutasi pada $GF(q)$ jika dan hanya jika $b^2 = 3ac$ dan $q \equiv 2 \ (mod\ 3)$.

Pembuktian dilakukan dengan menggunakan bantuan logika proposisi.

Misalkan proposisi:

p_1: $h(x)$ polinomial permutasi pada $GF(q)$.

p_2: $b^2 = 3ac$ dan $q \equiv 2 \ (mod\ 3)$.

Maka akan dibuktikan $p_1 \leftrightarrow p_2$.

($\rightarrow$)

Jika diketahui $h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$, adalah polinomial permutasi pada $GF(q)$akan dibuktikan $b^2 = 3ac$ dan $q \equiv 2 \ (mod\ 3)$.

Pada Teorema 3.10 telah dibuktikan jika $ax^k + bx^{k-2} + c$ (dimana $a \neq \mathbf{0}$ dan $k \geq 2$) merupakan polinomial permutasi pada $GF(q)$ maka $q \not\equiv \pm 1 \ (mod\ k)$ atau $b = \mathbf{0}$.

Pandang $h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$. Jika disesuaikan dengan Teorema 3.10, maka $a = \mathbf{1}$, $k = 3$, $b = -\alpha$, dan $c = \mathbf{0}$.

Didapat berdasarkan Teorema 3.10:

jika $h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$, polinomial permutasi maka $q \not\equiv \pm 1 \ (mod\ 3)$ atau $-\alpha = \mathbf{0}$ (3.9)

Karena karakteristik dari $GF(q)$ bukan 3 dan karakteristiknya pasti bilangan prima (berdasarkan Teorema 2.14), maka q pasti bukan kelipatan 3.

Misalkan proposisi:

$j: q \not\equiv \pm 1 (mod\ 3)$.

Karena q bukan kelipatan 3 maka kemungkinan yang tersisa adalah:

1. $q \equiv 1 (mod\ 3)$
2. $q \equiv 2 (mod\ 3)$ yang artinya sama dengan $q \equiv -1 (mod\ 3)$

Maka kasus manapun yang terjadi, proposisi j tidak berlaku. Sehingga berdasarkan (3.9), jika $\alpha \neq \mathbf{0}$ maka $h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$, bukan polinomial permutasi. Maka hanya ada satu kemungkinan α agar $h(x)$ menjadi polinomial permutasi yaitu $\alpha = \mathbf{0}$. Jika $\alpha = \mathbf{0}$ maka berdasarkan Teorema 3.2, $h(x) = x^3$ adalah polinomial permutasi jika dan hanya jika $gcd(3, q-1) = 1$. Maka $q - 1 \not\equiv (mod\ 3)$, sehingga kemungkinan yang tersisa adalah $q \equiv 2 (mod\ 3)$. Jadi jika $h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$, merupakan polinomial permutasi maka $\alpha = \mathbf{0}$ dan $q \equiv 2 (mod\ 3)$.

Namun $\alpha = \mathbf{0}$ berarti $(3a^2)^{-1}(b^2 - 3ac) = \mathbf{0}$. Karena pada premis $a \neq \mathbf{0}$ maka $(3a^2)^{-1} \neq \mathbf{0}$. Sehingga agar $(3a^2)^{-1}(b^2 - 3ac) = \mathbf{0}$ haruslah $(b^2 - 3ac) = \mathbf{0}$. Hal ini terjadi karena $GF(q)$ merupakan *field* sehingga berdasarkan Teorema 2.12 $GF(q)$ juga merupakan *integral domain*. Didapat $(b^2 - 3ac) = \mathbf{0}$ yakni $b^2 = 3ac$.

Terbukti jika $h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$, merupakan polinomial permutasi maka $b^2 = 3ac$ dan $q \equiv 2 (mod\ 3)$.

Terbukti $p_1 \rightarrow p_2$.

($\leftarrow$)

Akan dibuktikan $p_2 \rightarrow p_1$

Jika diketahui $b^2 = 3ac$ dan $q \equiv 2\ (mod\ 3)$ akan dibuktikan $h(x)$ polinomial permutasi pada $GF(q)$.

Karena $b^2 = 3ac$ maka $b^2 - 3ac = \mathbf{0}$. Karena $b^2 - 3ac = \mathbf{0}$ maka $\alpha = (3a^2)^{-1}(b^2 - 3ac) = \mathbf{0}$. Didapat $h(x) = x^3$. Berdasarkan Teorema 3.2, $h(x)$ adalah polinomial permutasi pada $GF(q)$ jika dan hanya $gcd(3, q - 1) = 1$. Akan tetapi diketahui $q \equiv 2\ (mod\ 3)$, maka didapat $gcd(3, q - 1) = 1$. Sehingga terbukti bahwa $h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$, adalah polinomial permutasi pada $GF(q)$.

Terbukti $p_2 \rightarrow p_1$.

Telah dibuktikan $p_1 \rightarrow p_2$ dan $p_2 \rightarrow p_1$, maka terbukti $p_1 \leftrightarrow p_2$. Yaitu $h(x) = x^3 - \alpha x$, dengan $\alpha = (3a^2)^{-1}(b^2 - 3ac)$, adalah polinomial permutasi pada $GF(q)$ jika dan hanya jika $b^2 = 3ac$ dan $q \equiv 2\ (mod\ 3)$. Sehingga terbukti pula bahwa $g(x) = x(x^2 + a^{-1}bx + a^{-1}c)$ polinomial permutasi pada $GF(q)$ jika dan hanya jika $b^2 = 3ac$ dan $q \equiv 2\ (mod\ 3)$. Karena telah dibuktikan $f(x)$ merupakan polinomial permutasi jika dan hanya jika $g(x)$ merupakan polinomial permutasi (yaitu $p \leftrightarrow r$), maka terbukti $f(x)$ merupakan polinomial permutasi jika dan hanya jika $b^2 = 3ac$ dan $q \equiv 2\ (mod\ 3)$.

Teorema 3.12 membahas ciri-ciri dari binomial agar menjadi polinomial permutasi. Namun binomial tersebut dibatasi pada binomial yang derajatnya merupakan pangkat dari karakteristik *finite field*.

Teorema 3.12

Misalkan karakteristik $GF(q)$ adalah p dan $f(x) = x^{p^s} - \alpha x$ dengan $\alpha \neq \mathbf{0}$ anggota $GF(q)$ dan $s > 0$. Maka:

a) $f(x)$ polinomial permutasi atas $GF(q)$ jika dan hanya jika α bukan pangkat ke $p^s - 1$ dari anggota $GF(q)$.
b) Jika $f(x)$ polinomial permutasi atas $GF(q)$ maka $gcd(q-1, p^s - 1) > 1$.
c) Jika α merupakan elemen *primitive* pada $GF(q)$ maka $gcd(q - 1, p^s - 1) > 1$ jika dan hanya jika $f(x)$ polinomial permutasi atas $GF(q)$.

Bukti

Untuk a):

Akan dibuktikan: $f(x)$ polinomial permutasi atas $GF(q)$ jika dan hanya jika α bukan pangkat ke $p^s - 1$ dari anggota $GF(q)$.

(→)

Jika diketahui $f(x)$ polinomial permutasi pada $GF(q)$ maka akan dibuktikan dengan kontradiksi bahwa α bukan pangkat ke $p^s - 1$ dari anggota $GF(q)$.

Andaikan terdapat $\beta \neq \mathbf{0}$ anggota $GF(q)$ dimana $\beta^{p^s-1} = \alpha$. Maka f bukan fungsi satu-satu karena $\mathbf{0}$ dan β merupakan anggota $GF(q)$ yang berbeda namun sama-sama dipetakan oleh f ke $\mathbf{0}$. Karena f bukan fungsi satu-satu maka $f(x)$ bukan polinomial permutasi. Hal ini kontradiksi dengan yang diketahui di premis bahwa $f(x)$ polinomial permutasi. Sehingga pengandaian bahwa terdapat $\beta \neq \mathbf{0}$ anggota $GF(q)$ dimana $\beta^{p^s-1} = \alpha$ salah. Jadi tidak terdapat anggota $GF(q)$ sedemikian sehingga pangkat ke-$p^s - 1$nya sama dengan α.

(←)

Jika diketahui α bukan pangkat ke $p^s - 1$ dari anggota $GF(q)$ maka akan dibuktikan dengan kontradiksi bahwa $f(x)$ polinomial permutasi pada $GF(q)$.

Andaikan $f(x)$ bukan polinomial permutasi pada $GF(q)$ maka f bukan fungsi satu-satu. Sehingga terdapat w, y anggota $GF(q)$, $w \neq y$, sedemikian sehingga $f(w) = f(y)$. Didapat

$$w^{p^s} - \alpha w = y^{p^s} - \alpha y$$

$$w^{p^s} - y^{p^s} = \alpha w - \alpha y \tag{3.10}$$

Pandang bentuk berikut:

$$(w-y)^{p^s} = ((w-y)^p)^{p^{s-1}} \tag{3.11}$$

Berdasarkan Teorema 2.14, p merupakan bilangan prima. Dan w, y anggota $GF(q)$ sehingga berdasarkan Teorema 2.15, $(w-y)^p = w^p - y^p$.

Dari (3.11)

$$(w-y)^{p^s} = ((w-y)^p)^{p^{s-1}}$$

$$(w-y)^{p^s} = (w^p - y^p)^{p^{s-1}}$$

$$(w-y)^{p^s} = ((w^p - y^p)^p)^{p^{s-2}} \tag{3.12}$$

Berdasarkan Teorema 2.15, $(w^p - y^p)^p = w^{p^2} - y^{p^2}$.

Dari (3.12)

$$(w-y)^{p^s} = ((w^p - y^p)^p)^{p^{s-2}}$$

$$(w-y)^{p^s} = (w^{p^2} - y^{p^2})^{p^{s-2}}$$

$$\vdots$$

$(w-y)^{p^s} = (w^{p^s} - y^{p^s})^{p^{s-s}}$

$(w-y)^{p^s} = (w^{p^s} - y^{p^s})^{p^0}$

$(w-y)^{p^s} = (w^{p^s} - y^{p^s})^{1}$

$(w-y)^{p^s} = \left(w^{p^s} - y^{p^s}\right)$ (3.13)

Dari (3.10)

$w^{p^s} - y^{p^s} = \alpha w - \alpha y$

Berdasarkan (3.13)

$(w-y)^{p^s} = \alpha w - \alpha y$

Berdasarkan sifat distributif pada *field*:

$(w-y)^{p^s} = \alpha(w-y)$ (3.14)

Kalikan kedua ruas pada persamaan (3.14) dengan $(w-y)^{-1}$. ($(w-y)^{-1}$ ada dan anggota $GF(q)$ karena $GF(q)$ adalah *field* dan $w - y \neq \mathbf{0}$).

Didapat:

$(w-y)^{p^s-1} = \alpha$

Sehingga didapat sebuah anggota $GF(q)$ yaitu $(w-y)$ dimana $(w-y)^{p^s-1} = \alpha$. Hal ini kontradiksi dengan yang diketahui bahwa α bukan pangkat ke $p^s - 1$ dari anggota $GF(q)$. Sehingga pengandaian bahwa $f(x)$ bukan polinomial permutasi pada $GF(q)$ salah. Jadi haruslah $f(x)$ polinomial permutasi pada $GF(q)$.

Untuk b):

Jika diketahui $f(x)$ polinomial permutasi pada $GF(q)$ maka akan dibuktikan dengan kontradiksi bahwa $gcd(q-1, p^s-1) > 1$.

Andaikan $gcd(q-1, p^s-1) = 1$. Maka berdasarkan Teorema 2.31 terdapat bilangan bulat m, n sedemikian sehingga $m(q-1) + n(p^s-1) = 1$.

$$\alpha^1 = \alpha$$

$$\alpha^{m(q-1)+n(p^s-1)} = \alpha$$

Karena $\alpha \in GF(q) - \{\mathbf{0}\}$ dan berdasarkan Teorema 2.3 serta Teorema 2.16, maka $\alpha^{(q-1)} = \mathbf{1}$.

$$\alpha^{n(p^s-1)} = \alpha$$

$$(\alpha^n)^{(p^s-1)} = \alpha$$

Sebut $\alpha^n = \gamma$ suatu anggota $GF(q)$. Maka α merupakan pangkat ke $p^s - 1$ dari anggota $GF(q)$. Sehingga berdasarkan bagian a) dari Teorema ini, $f(x)$ bukan polinomial permutasi. Hal ini kontradiksi dengan yang diketahui bahwa $f(x)$ merupakan polinomial permutasi pada $GF(q)$. Sehingga pengandaian bahwa $gcd(q-1, p^s-1) = 1$ salah. Jadi haruslah $gcd(q-1, p^s-1) > 1$.

Untuk c):

Jika diketahui α merupakan elemen *primitive* pada $GF(q)$ akan dibuktikan $gcd(q-1, p^s-1) > 1$ jika dan hanya jika $f(x)$ polinomial permutasi pada $GF(q)$.

(←)

Jika diketahui $f(x)$ polinomial permutasi pada $GF(q)$ akan dibuktikan $gcd(q-1, p^s-1) > 1$. Hal ini sudah dibuktikan pada bagian b) dari Teorema ini.

(→)

Jika diketahui $gcd(q-1, p^s-1) > 1$ akan dibuktikan dengan kontradiksi $f(x)$ polinomial permutasi pada $GF(q)$.

Andaikan $f(x)$ bukan polinomial permutasi pada $GF(q)$. Berdasarkan bagian a) dari Teorema ini, maka terdapat y anggota $GF(q)$ dimana $y^{p^s-1} = \alpha$. Selanjutnya jika diketahui α merupakan elemen *primitive* dari $GF(q)$ akan dibuktikan y juga merupakan elemen *primitive* dari $GF(q)$. Bukti:

> Ambil $t \neq \mathbf{0}$ anggota $GF(q)$. Karena α merupakan elemen *primitive* dari $GF(q)$ maka terdapat bilangan bulat l dimana $\alpha^l = t$. Namun $\alpha = y^{p^s-1}$. Maka $y^{l(p^s-1)} = t$ untuk suatu bilangan bulat $l(p^s-1)$. Karena untuk sembarang anggota $GF(q) - \{\mathbf{0}\}$ dapat dinyatakan sebagai pangkat dalam y, maka y juga merupakan elemen *primitive* dari $GF(q)$.

Didapat y merupakan elemen *primitive* dari $GF(q)$. Maka berdasarkan Teorema 2.19 bagian c), $y^{p^s-1} = \alpha$ juga merupakan elemen *primitive* dari $GF(q)$ jika dan hanya jika $gcd(p^s-1, q-1) = 1$. Diketahui α merupakan elemen *primitive* dari $GF(q)$ namun $gcd(p^s-1, q-1) > 1$. Hal ini merupakan kontradiksi. Sehingga pengandaian kita bahwa $f(x)$ bukan polinomial permutasi pada $GF(q)$ salah. Haruslah $f(x)$ polinomial permutasi pada $GF(q)$.

Teorema 3.13 membahas ciri-ciri dari *cyclotomic polynomial* agar menjadi polinomial permutasi.

Teorema 3.13

mth cyclotomic polynomial $Q_m(x)$ atas $GF(q)$ yang karakteristiknya bukan 2 merupakan polinomial permutasi jika dan hanya jika $m = 2$.

Bukti

Pembuktian akan dilakukan dengan bantuan logika proposisi.

Misalkan proposisi:

p: $Q_m(x)$ merupakan polinomial permutasi atas $GF(q)$.

r: $m = 2$.

(←)

Akan dibuktikan jika $m = 2$ maka $Q_m(x)$ merupakan polinomial permutasi atas $GF(q)$.

$x^2 - \mathbf{1} = \mathbf{0}$

$(x + \mathbf{1})(x - \mathbf{1}) = \mathbf{0}$

Didapat dua buah 2*nd root of unity* yaitu $\mathbf{1}$ dan $-\mathbf{1}$. Namun yang merupakan *primitive 2nd root of unity* hanyalah $-\mathbf{1}$. Sehingga $Q_2(x) = x + \mathbf{1}$, yang merupakan polinomial permutasi atas $GF(q)$.

(→)

Akan dibuktikan jika $Q_m(x)$ merupakan polinomial permutasi atas $GF(q)$ maka $m = 2$. Dengan kontrapositifnya. Jika diketahui $m \neq 2$ akan dibuktikan $Q_m(x)$ bukan polinomial permutasi atas $GF(q)$.

Kasus 1:

Jika m pangkat dari bilangan prima selain 2. Misalkan $m = p^l,\ l \in \mathbb{N}, p$ bilangan prima selain 2. Berdasarkan Teorema 2.30 bagian b),

$Q_{p^l} = \frac{x^{p^l}-\mathbf{1}}{x^{p^{l-1}}-\mathbf{1}}$.

$Q_{p^l}(-\mathbf{1}) = \mathbf{1} = Q_{p^l}(\mathbf{0})$

Sehingga Q_m bukan polinomial permutasi karena bukan fungsi satu-satu.

Kasus 2:

Jika $m \neq 2$ merupakan pangkat dari 2. Misalkan $m = 2^l,\ l > 1 \in \mathbb{N}$. Berdasarkan Teorema 2.30 bagian a),

$Q_{2^l} = \mathbf{1} + x^{2^{l-1}}$

Sehingga

$Q_{2^l}(\mathbf{1}) = \mathbf{1} + \mathbf{1} = Q_{2^l}(-\mathbf{1})$

Sehingga Q_m bukan polinomial permutasi karena bukan fungsi satu-satu.

Kasus 3:

Untuk m selain pada kasus-kasus sebelumnya.

Berdasarkan Teorema 2.33, untuk m bilangan bulat positif lebih dari 1, terdapat tepat satu cara untuk menyatakan m dalam bentuk $m = {p_1}^{a_1}{p_2}^{a_2} \ldots {p_k}^{a_k}$, dengan $p_1 < p_2 < p_3 \ldots < p_k$ bilangan-bilangan prima, dan $a_1, a_2, \ldots, a_k$ bilangan bulat positif. Sebut ${p_1}^{a_1}{p_2}^{a_2} \ldots {p_{k-1}}^{a_{k-1}} = A$. Maka $m = A{p_k}^{a_k}$, dimana p_k tidak membagi A.

$Q_m = Q_{A{p_k}^{a_k}}$

Berdasarkan Teorema 2.29 bagian a),

$$Q_m = Q_{Ap_k{}^{a_k}} = Q_{Ap_k} \circ \left(x^{p_k^{a_k-1}}\right)$$

Berdasarkan Teorema 2.29 bagian b),

$$Q_{Ap_k} = \frac{Q_A \circ x^{p_k}}{Q_A}$$

Sehingga

$$Q_m(x) = \frac{Q_A(x^{p_k^{a_k}})}{Q_A(x^{p_k^{a_k-1}})}$$

$$Q_m(x)Q_A(x^{p_k^{a_k-1}}) = Q_A(x^{p_k^{a_k}})$$

Substitusi $x = \mathbf{0}$ dan $x = \mathbf{1}$, didapat

$$(Q_m(\mathbf{0}) - \mathbf{1})Q_A(\mathbf{0}) = \mathbf{0} \quad (3.15)$$

$$(Q_m(\mathbf{1}) - \mathbf{1})Q_A(\mathbf{1}) = \mathbf{0} \quad (3.16)$$

Karena $\mathbf{0}$ dan $\mathbf{1}$ bukan *primitive Ath root of unity* maka $Q_A(\mathbf{0}) \neq \mathbf{0}$ dan $Q_A(\mathbf{1}) \neq \mathbf{0}$. Berdasarkan (3.15) dan fakta bahwa $GF(q)$ *integral domain* maka $(Q_m(\mathbf{0}) - \mathbf{1}) = \mathbf{0}$ atau $Q_m(\mathbf{0}) = \mathbf{1}$. Berdasarkan (3.16) dan fakta bahwa $GF(q)$ *integral domain* maka $(Q_m(\mathbf{1}) - \mathbf{1}) = \mathbf{0}$ atau $Q_m(\mathbf{1}) = \mathbf{1}$. Didapat

$$Q_m(\mathbf{0}) = \mathbf{1} = Q_m(\mathbf{1})$$

Sehingga Q_m bukan polinomial permutasi karena bukan fungsi satu-satu.

Jika $m \neq 2$, terbukti $Q_m(x)$ bukan polinomial permutasi atas $GF(q)$. Sehingga, jika $Q_m(x)$ polinomial permutasi atas $GF(q)$ maka $m = 2$.