BEBERAPA SIFAT GRUP POLINOMIAL PERMUTASI

SITTI NURHALISA

H011201006

PROGRAM STUDI MATEMATIKA DEPARTEMEN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS HASANUDDIN
MAKASSAR
2024

BEBERAPA SIFAT GRUP POLINOMIAL PERMUTASI

SITTI NURHALISA

H011201006

PROGRAM STUDI MATEMATIKA DEPARTEMEN MATEMATIKA

AS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS HASANUDDIN

MAKASSAR

2024

BEBERAPA SIFAT GRUP POLINOMIAL PERMUTASI

SITTI NURHALISA

H011201006

Skripsi

sebagai salah satu syarat untuk mencapai gelar sarjana

Program Studi Matematika

pada

PROGRAM STUDI MATEMATIKA

DEPARTEMEN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS HASANUDDIN

MAKASSAR

2024

SKRIPSI

BEBERAPA SIFAT GRUP POLINOMIAL PERMUTASI

SITTI NURHALISA
H011201006

Skripsi,

telah dipertahankan di depan Panitia Ujian Sarjana pada tanggal 27 Agustus 2024

dan dinyatakan telah memenuhi syarat kelulusan

pada

Program Studi Matematika

Departemen Matematika

Fakultas Matematika dan Ilmu Pengetahuan Alam

Universitas Hasanuddin

Makassar

Mengesahkan:

Pembimbing Utama,	Pembimbing Pertama,
Prof. Dr. Amir Kamal Amir, M.Sc.	Dr. Andi Muhammad Anwar, S.Si., M.Si.
NIP. 196808031992021001	NIP. 199012282018031001

Mengetahui:
Ketua Program Studi,

Dr. Firman, S.Si., M.Si.
NIP. 196804292002121001

PERNYATAAN KEASLIAN SKRIPSI DAN PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa, skripsi berjudul "Beberapa Sifat Grup Polinomial Permutasi" adalah benar karya saya dengan arahan dari bapak Prof. Dr. Amir Kamal Amir, M.Sc. sebagai Pembimbing Utama dan bapak Dr. Andi Muhammad Anwar, S.Si., M.Si. sebagai Pembimbing Pertama. Karya ilmiah ini belum diajukan dan tidak sedang diajukan dalam bentuk apa pun kepada perguruan tinggi mana pun. Sumber informasi yang berasal atau dikutip dari karya yang diterbitkan maupun tidak diterbitkan dari penulis lain telah disebutkan dalam teks dan dicantumkan dalam Daftar Pustaka skripsi ini. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini adalah karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut berdasarkan aturan yang berlaku.

Dengan ini saya melimpahkan hak cipta (hak ekonomis) dari karya tulis saya berupa skripsi ini kepada Universitas Hasanuddin.

Makassar, 27 Agustus 2024

Sitti Nurhalisa
H011201006

UCAPAN TERIMA KASIH

Puji dan syukur atas kehadirat Allah SWT yang telah melimpahkan rahmat, dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi ini. Shalawat serta salam senantiasa tercurahkan kepada Nabi Muhammad SAW sebagai suri tauladan bagi seluruh umatnya, sehingga penyusunan skripsi yang berjudul "Beberapa Sifat Grup Polinomial Permutasi" dapat diselesaikan dengan baik. Skripsi ini tidak akan terwujud tanpa dukungan, bimbingan, dan bantuan dari berbagai pihak. Oleh karena itu, dengan segala kerendahan hati, penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak **Prof. Dr. Jamaluddin Jompa, M.Si.** selaku Rektor Universitas Hasanuddin, Bapak **Dr. Eng. Amiruddin** selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam, serta Bapak **Dr. Firman, S.Si., M.Si.** selaku Ketua Departemen Matematika.
2. Seluruh **Dosen** dan **Staf** Departemen Matematika yang telah memberikan ilmunya kepada penulis selama menjadi mahasiswa di Departemen Matematika.
3. Bapak **Prof. Dr. Amir Kamal Amir, M.Sc.** sebagai Pembimbing Utama dan bapak **Dr. Andi Muhammad Anwar, S.Si., M.Si**.sebagai Pembimbing Pertama atas kesediaan dan kesabarannya dalam membimbing penulis, serta meluangkan banyak waktu sehingga penulis dapat menyelesaikan skripsi ini.
4. Ibu **Prof. Dr. Aidawayati Rangkuti, M.S.** dan Ibu **Naimah Aris, S.Si., M.Math.** selaku penguji yang telah meluangkan waktunya untuk memberikan ilmu, saran, dan arahan kepada penulis dalam menyelesaikan skripsi ini.
5. Ayah kebanggan penulis **Abdullah** dan ibu kesayangan penulis **Hudriana** yang telah membesarkan dan mendidik penulis dengan penuh kesabaran. Kakak kesayangan penulis **Nurhidayah, Amd.Keb.** dan **Nur Malasari, S.Sos.**, serta seluruh keluarga yang telah mendoakan dan memberikan dukungan.
6. Teman-teman seperjuangan penulis, **Yusriani, Sri Rahayu Adi Ningsih, Muharram, Egidia, Vivie Luthviana** dan **Ariqah Mumtazah** yang telah mewarnai dunia perkuliahan penulis, senantiasa memberikan dukungan, menginspirasi, tidak kenal lelah peduli dan menasehati penulis selama masa studi sarjana.
7. Teman seperjuangan Kuliah Kerja Nyata (KKNT Pertanian Perkebunan Peternakan G.110 Posko Desa Kalepadang, Kec. Bontoharu, Kab. Kepulauan Sekayar) yang telah memberikan warna baru dalam masa perkuliahan penulis dan senantiasa mendukung penulis.
8. Seluruh pihak yang tidak dapat saya sebutkan satu per satu**,** yang telah membantu dan memberikan dukungan dalam bentuk apapun.

Akhir kata, penulis berharap semoga segala bentuk kebaikan yang telah diberikan bernilai ibadah dan semoga skripsi ini dapat bermanfaat bagi pembaca dan dapat si yang berarti dalam bidang ilmu pengetahuan.

Penulis,

Sitti Nurhalisa

ABSTRAK

SITTI NURHALISA. **Beberapa Sifat Grup Polinomial Permutasi.** (Dibimbing oleh “Prof. Dr. Amir Kamal Amir, M.sc.” dan “Dr. Andi Muhammad Anwar, S.Si., M.Si.”).

Polinomial permutasi adalah jenis polinomial yang memiliki sifat khusus yaitu, ketika diaplikasikan pada semua elemen dari sebuah lapangan hingga akan menghasilkan permutasi elemen-elemen yang merupakan pemetaan bijektif. Polinomial permutasi berkaitan erat dengan sifat-sifat grup polinomial permutasi dalam aljabar abstrak. Penelitian ini bertujuan menunjukkan sifat-sifat grup polinomial permutasi pada polinomial permutasi satu variabel atas lapangan hingga $\mathbb{F}_q$ dan karakteristik dari polinomial permutasi atas lapangan $\mathbb{F}_{q^2}$. Hasil penelitian ini menunjukkan bahwa ada beberapa sifat grup polinomial permutasi atas lapangan hingga $\mathbb{F}_q$ dalam konteks subgrup N yang merupakan subgrup dari grup perkalian $G = \mathbb{F}_q^*$. Selain itu, ditemukan juga karakteristik polinomial permutasi yang membentuk kelompok permutasi atas lapangan hingga $\mathbb{F}_{q^2}$ berdasarkan nilai $b \in \mathbb{F}_q^*$ dan $a, \delta, g \in \mathbb{F}_{q^2}$. Hasil penelitian ini diharapkan dapat memberikan pemahaman tentang sifat-sifat grup polinomial permutasi serta karakteristik polinomial permutasi yang membentuk kelompok permutasi.

Kata kunci: Grup Permutasi, Polinomial Permutasi, Grup Polinomial Permutasi, Sifat Polinomial Permutasi.

ABSTRACT

SITTI NURHALISA. ***Some Properties of Permutation Polynomials Group.*** *(Guided by "Prof. Dr. Amir Kamal Amir, M.Sc." and "Dr. Andi Muhammad Anwar, S.Si., M.Si.").*

Permutation polynomials are a type polynomial that has special properties, when applied to all elements of a field to produce permutations of element which is bipolar mapping. Permutation polynomials are closely related to the proporties of permutation polynomial groups in abstract algebra. This study aims to show the polynomials groups in permutation polynomials of one variable over the finte field $\mathbb{F}_q$ *and characteristics of permutation polynomials over the finite field* $\mathbb{F}_{q^2}$*. The results of study show that there are several properties of polynomials groups permutation over the finite field* $\mathbb{F}_q$ *in the context of subgroup* N *which is a subgroup of the multiplication group* $G = \mathbb{F}_q^*$*. In addition, it was also found that the polynomial charactetistucs of permutations formed over finite field* $\mathbb{F}_{q^2}$ *based on the values of* $b \in \mathbb{F}_q^*$ *dan* $a, \delta, g \in \mathbb{F}_{q^2}$*. The results of this study are expected to provide an understanding of the properties of permutation polynomial groups and characteristics of permutation polynomials that form permutation groups.*

Keywords: *Permutation Groups, Permutation Polynomials, Permutation Polynomial Groups, Proporties of Permutation Polynomial Groups.*

DAFTAR ISI

Halaman

DAFTAR NOTASI

Lambang	Arti dan penjelasan
$\mathbb{Z}$	Bilangan bulat
$\mathbb{R}$	Bilangan real
$\mathbb{Q}$	Bilangan rasional
$\boldsymbol{\tau}$	Tau
$\boldsymbol{\delta}$	Delta
$\boldsymbol{\alpha}$	Alpha
$\boldsymbol{\beta}$	Beta
$\boldsymbol{\varphi}$	Phi
$\boldsymbol{G}$	Grup
$\boldsymbol{N}$	Subgrup
$\boldsymbol{R}$	Gelanggang
$\mathbb{F}$	Lapangan
$\mathbb{F}_{\boldsymbol{q}}$	Lapangan hingga
$\in$	Elemen
$\sum$	Sigma
$\mathbf{deg}\,(\boldsymbol{f})$	Derajat f
$\boldsymbol{\phi}$	Phi variant
$\boldsymbol{\psi}$	Psi
$\mathbf{Tr}_{\boldsymbol{m}}^{\boldsymbol{n}}(\boldsymbol{x})$	Fungsi trace

BAB I
PENDAHULUAN

Pada bab ini dibahas mengenai latar belakang, rumusan masalah penelitian, batasan masalah, tujuan penelitian, manfaat penelitian, dan landasan teori.

1.1 Latar Belakang

Aljabar abstrak merupakan salah satu cabang matematika yang berfokus pada studi struktur aljabar seperti grup, gelanggang, dan lapangan. Dalam konteks aljabar abstrak, grup adalah himpunan yang dilengkapi dengan satu operasi biner yang memenuhi sifat assosiatif, memiliki elemen identitas dan setiap elemen memiliki invers. Teori grup sangat penting dalam banyak bidang matematika, termasuk dalam kajian tentang polinomial permutasi atas lapangan hingga (Fraleigh, 2003).

Lapangan hingga adalah sebuah struktur aljabar yang memiliki jumlah elemen yang terbatas, dimana operasi-operasi dasar seperti penambahan, pengurangan, perkalian, dan pembagian (kecuali nol) dapat dilakukan. Misalnya, lapangan hingga dengan q elemen, dengan $q = p^n$, dimana p adalah bilangan prima dan n adalah bilangan bulat positif, yang biasa ditulis dengan $\mathbb{F}_q$. Lapangan hingga menjadi dasar dari berbagai aplikasi dalam kriptografi dan teori koding karena sifat aljabarnya yang kuat dan terstruktur (Lidl & Niederreiter, 1997).

Polinomial permutasi adalah jenis polinomial yang memiliki sifat khusus yaitu, ketika diaplikasikan pada semua elemen dari sebuah lapangan hingga akan menghasilkan permutasi elemen-elemen tersebut. Ini berarti setiap elemen dalam lapangan hingga dipetakan ke elemen yang berbeda, dan tidak ada dua elemen yang dipetakan ke elemen yang sama, membuatnya menjadi pemetaan bijektif (Lidl & Muller, 1982).

Studi tentang polinomial permutasi atas lapangan hingga telah dimulai sejak abad ke-19 ketika Hermite dan kemudian Dickson memelopori bidang penelitian ini. Dalam beberapa tahun terakhir, minat terhadap polinomial permutasi meningkat secara signifikan karena potensi aplikasinya dalam sistem kriptografi kunci publik, seperti yang dijelaskan dalam paper Levine dan Chandler (1987), juga diterapkan dalam desain kombinatorial seperti deret de Bruijn (Blackburn dkk., 1996), dan banyak aplikasi lainnya.

Polinomial permutasi berkaitan erat dengan sifat-sifat grup polinomial permutasi dalam aljabar abstrak. Polinomial permutasi membentuk grup di bawah operasi komposisi, di mana komposisi dua polinomial permutasi menghasilkan polinomial permutasi lain, dan setiap polinomial permutasi memiliki invers yang juga merupakan polinomial permutasi. Sifat simetri yang dimiliki oleh banyak polinomial permutasi penting dalam aplikasi seperti desain kombinatorial dan kriptografi, mencerminkan pola simetri dalam grup. Polinomial ini juga sering terkait dengan fungsi kuasa dalam teori bilangan, m analisis elemen lapangan hingga dan pemecahan masalah yang engan demikian, keterkaitan ini menggarisbawahi pentingnya dalam memahami dan menerapkan konsep grup dalam berbagai an ilmu komputer (Ding dan Niederreiter, 1996).

polinomial permutasi menjadi subjek penelitian yang penting ikasi yang luas dalam berbagai bidang matematika dan aplikasi

praktis. Penelitian tentang sifat dan karakteristik dari grup polinomial permutasi memberikan pemahaman yang mendalam tentang struktur aljabar yang kompleks untuk pengembangan sistem kriptografi yang aman, desain kode yang efisien, dan analisis lapangan hingga. Dengan memahami dan menganalisis sifat-sifat dan karakteristik ini, dapat dikembangkan teori yang lebih kuat dan aplikasi yang lebih luas, memungkinkan inovasi dalam bidang-bidang seperti keamanan informasi, pengkodean data, dan matematika diskrit (Zieve, 2009).

Oleh karena itu, pemahaman yang mendalam tentang struktur, sifat dan karakteriktik dari grup polinomial permutasi ini sangat penting bagi pengembangan teknologi kriptografi modern. Sehingga, judul dari penelitian ini adalah **"Beberapa Sifat Grup Polinomial Permutasi"**.

1.2 Rumusan Masalah

Berdasarkan uraian pada latar belakang, maka rumusan masalah dalam penelitian ini adalah sebagai berikut.

1. Bagaimana sifat dari grup polinomial permutasi atas lapangan hingga $\mathbb{F}_q$?
2. Bagaimana karakteristik polinomial permutasi atas lapangan $\mathbb{F}_{q^2}$?

1.3 Batasan Penelitian

Berdasarkan rumusan masalah, diberikan batasan masalah pada polinomial satu variabel atas lapangan hingga $\mathbb{F}_q$.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, maka penelitian ini bertujuan menunjukkan sifat-sifat grup polinomial permutasi pada polinomial permutasi satu variabel atas lapangan hingga $\mathbb{F}_q$ dan karakteristik dari polinomial permutasi atas lapangan $\mathbb{F}_{q^2}$.

1.5 Manfaat Penelitian

Hasil dari penelitian ini diharapkan dapat memberikan manfaat kepada berbagai pihak sebagai berikut:

1. Bagi Penulis:
   a. Sebagai sarana untuk memperkaya pengetahuan dan wawasan mengenai ilmu matematika khususnya pada bidang aljabar.
   b. Sebagai sarana untuk menambah keterampilan dalam menerapkan teori-teori yang telah diperoleh dalam perkuliahan maupun yang diperoleh secara mandiri.
2. Bagi Pembaca:
   a. Sebagai sarana untuk menambah pemahaman tentang teori-teori dalam bidang aljabar.
   b. Sebagai sarana untuk menambah referensi dalam kajian keilmuan matematika.
3. Bagi Universitas Hasanuddin:
   a. Sebagai sarana untuk menambah literatur mengenai matematika khususnya aljabar yang dapat digunakan oleh setiap civitas akademik Universitas Hasanuddin.

1.6 Landasan Teori

Pada subbab ini diberikan beberapa materi yang akan digunakan sebagai landasan teori dalam mengkaji sifat-sifat dari grup polinomial permutasi. Materinya berupa grup, gelanggang, lapangan, permutasi, polinomial, lapangan hingga, polinomial permutasi, dan grup polinomial permutasi.

1.6.1 Grup

Pada bagian ini akan diperkenalkan sistem matematika yang disebut grup. Digunakan notasi $(G,*)$ untuk menyatakan sistem matematika yang dibentuk oleh himpunan G dan operasi biner $*$.

Definisi 1.1 Grup adalah himpunan tak kosong G, yang dilengkapi dengan sebuah operasi biner yang dinotasikan dengan $*$, yang memenuhi aksioma berikut:

1. (Asosiatif) Untuk setiap $a, b, c \in G$
$$(a * b) * c = a * (b * c)$$
2. (Identitas) Terdapat elemen $e \in G$ dimana
$$e * a = a * e = a$$
untuk setiap $a \in G$.
3. (Invers) Untuk setiap $a \in G$, terdapat elemen $a^{-1} \in G$ dimana
$$a * a^{-1} = a^{-1} * a = e$$

(Roman, 2007)

Contoh 1.1 Misalkan $G = \mathbb{Z}$ maka G adalah grup terhadap operasi penjumlahan karena memenuhi aksioma asosiatif, memiliki identitas yaitu 0, dan setiap $a \in \mathbb{Z}$ memiliki invers yaitu $-a \in \mathbb{Z}$.

Definisi 1.2 Grup G abel atau komutatif jika $a * b = b * a$, untuk setiap $a, b \in G$.

(Suryanti, 2017)

Contoh 1.2 Misalkan $G = \mathbb{Z}$ bersifat komutatif karena penjumlahan pada bilangan bulat bersifat komutatif.

Definisi 1.3 Subhimpunan H dari grup G adalah subgrup dari G jika H terhadap operasi di G membentuk sebuah grup. Dalam hal ini ditulis $H \leq G$, dan jika juga $H \neq G$, maka ditulis $H < G$.

(Muchlis dan Astuti, 2007)

Definisi 1.4 Misalkan G grup, maka G dan $\{e\}$ adalah subgrup tak sejati dari G, dan semua subgrup selain itu adalah subgrup sejati.

(Suryanti, 2017)

salkan $(G,*)$ dan $(H,\circ)$ adalah grup, fungsi dari G dan H dikatakan operasi/homomorfisma jika:

$$f(x * y) = f(x) \circ f(y), \forall x, y \in G$$

(Suryanti, 2017)

Definisi 1.6 Misalkan $f: G \to H$ adalah homomorfisma grup, maka

1. Jika f injektif maka f dinamakan monomorfisma
2. Jika f surjektif maka f dinamakan epimorfisma
3. Jika f bijektif maka f dinamakan isomorfisma

(Suryanti, 2017)

Contoh 1.3 Misalkan $f: \mathbb{Z} \to 2\mathbb{Z}$ dengan $f(x) = 2x$. Fungsi f merupakan isomorfisma karena memenuhi untuk setiap $a, b \in \mathbb{Z}$,

$$f(a+b) = 2(a+b) = 2a + 2b = f(a) + f(b)$$

dan f merupakan fungsi bijektif.

Definisi 1.7 Orde grup. Jumlah elemen dari grup G (terbatas atau tak terbatas) disebut orde dan dinotasikan dengan $|G|$.

(Gallian, 2006)

Definisi 1.8 Orde elemen. Orde dari suatu elemen g dalam suatu grup G adalah bilangan bulat positif n sedemikian sehingga $g^n = e$. (Untuk operasi penjumlahan biasanya dituliskan menjadi $ng = 0$). Jika tidak ada bilangan bulat seperti itu, maka g memiliki orde tak terbatas. Orde dari suatu elemen g dinotasikan dengan $|g|$.

(Gallian, 2006)

Definisi 1.9 Misal H adalah subgrup dari G, dam $a \in G$. Koset kiri dari H dalam G adalah

$$aH = \{ah | h \in H\}$$

Sedangkan koset kanan dari H dalam G adalah

$$Ha = \{ha | h \in H\}$$

(Suryanti, 2017)

1.6.2 Gelanggang

Konsep aljabar yang disebut gelanggang dapat dipandang sebagai generalisasi dari struktur aljabar yang sudah dikenal seperti sistem bilangan real, sistem bilangan rasional dan sistem bilangan bulat.

Definisi 1.10 Gelanggang $(R, +, \cdot)$ adalah himpunan R, dengan dua operasi biner yang dilambangkan dengan $+$ dan $\cdot$, sehingga:

1. R adalah grup abel terhadap $+$.
2. Operasi biner $\cdot$ bersifat asosiatif yaitu, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ untuk setiap $a, b, c \in R$.
3. Hukum distributif berlaku; yaitu, untuk setiap $a, b, c \in R$ memenuhi $a \cdot (b + c) = a \cdot b + a \cdot c$ dan $(b + c) \cdot a = b \cdot a + c \cdot a$.

dentitas pada gelanggang R untuk operasi $+$ menggunakan notasi
nen nol), dan invers penjumlahan dari a dilambangkan dengan $-a$;
disingkat dengan $a - b$. Hasil operasi $a \cdot b$ akan ditulis ab.
efinisi, diperoleh sifat $a0 = 0a = 0$ untuk setiap $a \in R$. Selain itu,
sifat $(-a)b = a(-b) = -ab$ untuk setiap $a, b \in R$.
u gelanggang disebut gelanggang beridentitas jika gelanggang
but mempunyai identitas perkalian, yaitu jika terdapat unsur 1

sehingga $a1 = 1a = a$ untuk semua $a \in R$.

2. Suatu gelanggang disebut komutatif jika operasi $\cdot$ bersifat komutatif.

(Lidl dan Niederreiter, 1983)

Contoh 1.4

1. Misalkan R adalah sembarang grup abelian dengan operasi grup $+$. Didefinisikan $ab = 0$ untuk semua $a, b \in R$; maka R adalah sebuah gelanggang.
2. Bilangan bulat genap $2\mathbb{Z}$ membentuk gelanggang komutatif tanpa elemen identitas.
3. Himpunan semua matriks 2×2 dengan bilangan real sebagai entrinya membentuk gelanggang nonkomutatif terhadap operasi penjumlahan dan perkalian matriks.

(Lidl dan Niederreiter, 1983)

Definisi 1.11 Subhimpunan S dari gelanggang R disebut subgelanggang dari R apabila S tertutup atas operasi $+$ dan $\cdot$ dan memenuhi sifat gelanggang.

(Lidl dan Niederreiter, 1983)

Definisi 1.12 Subhimpunan J dari gelanggang R disebut ideal apabila J subgrup atas operasi penjumlahan dari R dan untuk semua $a \in J$ dan $r \in R$ diperoleh $ar \in J$ dan $ra \in J$.

(Lidl dan Niederreiter, 1983)

Contoh 1.5

1. Misalkan R adalah lapangan $\mathbb{Q}$ dari bilangan rasional. Maka himpunan $\mathbb{Z}$ bilangan bulat merupakan subgelanggang dari $\mathbb{Q}$, tetapi bukan ideal karena, misalnya, $1 \in \mathbb{Z}, \frac{1}{2} \in \mathbb{Q}$, tetapi $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.
2. Misalkan R adalah gelanggang komutatif, $a \in R$, dan misalkan $J = \{ra : r \in R\}$, maka J adalah ideal.
3. Misalkan R adalah gelanggang komutatif. Maka ideal terkecil yang mengandung elemen tertentu $a \in R$ adalah ideal $\langle a \rangle = \{ra + na : r \in R, n \in \mathbb{Z}\}$. Jika R mengandung suatu identitas, maka $\langle a \rangle = \{ra : r \in R\}$.

(Lidl dan Niederreiter, 1983)

Definisi 1.13 Misalkan R adalah gelanggang komutatif. Ideal J dari R dikatakan ideal utama jika terdapat $a \in R$ sehingga $J = \langle a \rangle$. Dalam hal ini, J disebut juga ideal utama yang dibangun oleh a.

(Lidl dan Niederreiter, 1983)

Karena ideal adalah subgrup normal dari grup penjumlahan suatu
aka J ideal dari gelanggang R mendefinisikan partisi R menjadi
ng lepas, yang disebut kelas residu modulo J. Kelas residu elemen
ulo J akan dilambangkan dengan $[a] = a + J$, karena terdiri dari
R yang berbentuk $a + c$ untuk beberapa $c \in J$. Elemen $a, b \in R$
kongruen J, ditulis $a \equiv b \bmod J$, jika berada di kelas residu yang
J, atau setara, jika $a - b \in J$. Verifikasi bahwa $a \equiv n \bmod J$
$+ r \equiv b + r \bmod J$, $ar \equiv br \bmod J$, dan $ra \equiv rb \bmod J$ untuk setiap

$r \in R$ dan $na \equiv nb \bmod J$ untuk setiap $n \in \mathbb{Z}$. Jika $r \equiv s \bmod J$, maka $a + r \equiv b + s \bmod J$ dan $ar \equiv bs \bmod J$.

Definisi 1.14 Gelanggang kelas residu dari gelanggang R modulo ideal J berdasarkan operasi

$$(a + J) + (b + J) = (a + b) + J,$$
$$(a + J)(b + J) = ab + J,$$

disebut gelanggang kelas residu (atau gelanggang faktor) dari R modulo J dan dilambangkan dengan R/J.

(Lidl dan Niederreiter, 1983)

Contoh 1.6 Elemen $\mathbb{Z}/\langle n\rangle$ adalah

$$[0] = 0 + \langle n\rangle, [1] = 1 + (n), \dots, [n-1] = n - 1 + \langle n\rangle,$$

dengan $\mathbb{Z}/\langle n\rangle$ membentuk gelanggang kelas residu dengan operasi penjumlahan dan perkalian kelas residu.

(Lidl dan Niederreiter, 1983)

Pemetaan $\varphi: R \to S$ dari gelanggang R ke gelanggang S adalah homomorfisma jika untuk $a, b \in R$ memenuhi $\varphi(a + b) = \varphi(a) + \varphi(b)$ dan $\varphi(ab) = \varphi(a)\varphi(b)$. Jadi homomorfisma $\varphi: R \to S$ mempertahankan operasi $+$ dan $\cdot$ dalam R.

1.6.3 Lapangan

Lapangan dipandang sebagai generalisasi sistem bilangan real. Pada sistem bilangan real sudah diamati bahwa sistem ini membentuk gelanggang komutatif dan bahwa setiap unsur tak nolnya mempunyai balikan terhadap operasi kali.

Definisi 1.15 Misalkan R suatu sistem matematika dengan dua buah operasi tambah dan kali. Sistem R disebut lapangan jika R membentuk gelanggang komutatif dan setiap unsur tak nolnya merupakan unit, yaitu untuk setiap $a \in R$ dengan $a \neq 0$ terdapat $b \in R$ sehingga

$$ab = ba = 1,$$

(Muchlis dan Astuti, 2007)

Dengan memperhatikan definisi gelanggang komutatif, diperoleh kenyataan bahwa jika R lapangan, maka $R\backslash\{0\}$ membentuk grup abel terhadap operasi perkalian. Oleh karena itu, diperoleh definisi alternatif bagi lapangan: Sistem matematika $(R, +, \cdot)$ adalah lapangan jika berlaku:

1. $(R, +)$ adalah grup abel,
2. $(R, \cdot)$ adalah grup abel, dan
3. distributif) $a \cdot (b + c) = a \cdot b + a \cdot c$, untuk semua $a, b, c \in R$.

simpulkan bahwa sistem bilangan real dan sistem bilangan rasional pangan. Sedangkan sistem bilangan bulat tidak membentuk ini karena di $\mathbb{Z}$ terdapat unsur tak nol yang bukan unit. Contohnya mpunyai balikan di $\mathbb{Z}$.

Teorema 1.1 Gelanggang $\mathbb{Z}/\langle p\rangle$ *dengan* p *bilangan prima* p *adalah lapangan.*

(Muchlis dan Astuti, 2007)

1.6.4 Permutasi

Permutasi adalah pengaturan ulang elemen-elemen dari suatu himpunan dimana setiap elemen hanya muncul sekali dalam setiap urutan. Permutasi digunakan dalam berbagai cabang matematika termasuk teori grup.

Definisi 1.16 Misalkan S himpunan tak kosong. Maka permutasi pada S adalah pemetaan dari S ke S yang bersifat satu-satu pada.

(Muchlis dan Astuti, 2007)

Grup semua permutasi pada S dinamakan grup simetri pada S dan gunakan notasi $Sim(S)$ untuk menyatakannya. Setiap subgrup dari $Sim(S)$ disebut grup permutasi. Dalam hal $|S| = n$, digunakan notasi S_n, untuk $Sim(S)$.

Berikut ini akan dikaji grup S_n. Pertama-tama diberikan suatu cara mempresentasikan unsur S_n. Misalkan $\tau \in S_n$. Permutasi τ dapat dinyatakan sebagai suatu matriks dengan dua baris: pada baris pertama dituliskan $1,2,\dots,n$, dan pada baris kedua dituliskan $\tau(1),\tau(2),\dots,\tau(n)$.

Contoh 1.7

Pada S_4

$$\begin{bmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{bmatrix}$$

Menyatakan permutasi yang memetakan 1 ke 2, 2 ke 4, 3 ke 1, dan 4 ke 3. Juga permutasi identitas dinyatakan oleh

$$\begin{bmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 3 & 4\end{bmatrix}$$

Dengan notasi di atas, komposisi dua permutasi dibaca dari kanan ke kiri seperti membaca komposisi dua pemetaan biasa. Dengan demikian diperoleh contoh berikut:

$$\begin{bmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{bmatrix}\begin{bmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 2 & 4\end{bmatrix} = \begin{bmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{bmatrix}$$

Balikan dari suatu permutasi τ dapat dibaca sebaliknya: τ^{-1} terletak pada baris pertama di atas i. Jadi,

$$\begin{bmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{bmatrix}^{-1} = \begin{bmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 4 & 2\end{bmatrix}.$$

1.6.5 Polinomial

Dalam aljabar dasar, polinomial dianggap sebagai ekspresi dari bentuk $a_0 + a_1x + \cdots + a_nx^n$ dengan a_i disebut koefisien ; x dipandang sebagai variabel: yaitu, dengan mensubtitusi bilangan sembarang a dengan x, diperoleh bilangan yang gan baik $a_0 + a_1a + \cdots + a_na^n$. Aritmatika polinomial diatur oleh sudah dikenal. Konsep polinomial yang terkait operasi dapat an ke pengaturan aljabar formal dengan cara yang langsung.

isalkan R adalah gelanggang sembarang. Polinomial atas R adalah entuk

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_i x + \cdots + a_n x^n$$

n adalah bilangan bulat non-negatif, koefisien a_i, dimana $0 \leq i \leq n$, adalah elemen dari R, dan x adalah variabel bebas dengan domain R.
Polinomial

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad dan \quad g(x) = \sum_{i=0}^{n} b_i x^i$$

pada R dikatakan sama jika dan hanya jika $a_i = b_i$ untuk $0 \leq i \leq n$.
Dapat didefinisikan dengan operasi penjumlahan sebagai berikut,

$$f(x) + g(x) = \sum_{i=0}^{n} (a_i + b_i)\, x^i.$$

Selanjutnya, polinomial

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad dan \quad h(x) = \sum_{j=0}^{m} c_j x^j$$

Dapat didefinisikan dengan operasi perkalian sebagai berikut,

$$f(x)\, h(x) = \sum_{k=0}^{n+m} d_k x^k, \quad dimana \quad d_k = \sum_{\substack{i+j=k \\ 0 \leq i \leq n,\ 0 \leq j \leq m}} a_i c_j$$

Mudah dilihat bahwa dengan operasi ini himpunan polinomial atas R membentuk gelanggang. Gelanggang yang dibentuk oleh polinomial atas R dengan operasi di atas disebut gelanggang polinomial atas R dan dilambangkan dengan $R[x]$.

(Lidl dan Niederreiter, 1983)

Elemen nol dari $R[x]$ adalah polinomial yang semua koefisiennya adalah 0. Polinomial ini disebut polinomial nol dan dilambangkan dengan 0.

Definisi 1.18 Misalkan $f(x) = \sum_{i=0}^{n} a_i x^i$ adalah polinomial pada R yang bukan polinomial nol, sehingga dapat menganggap $a_n \neq 0$. Maka a_n disebut koefisien terdepan dari $f(x)$ dan a_0 merupakan suku konstanta, sedangkan n disebut derajat $f(x)$, dengan simbol $n = deg(f(x)) = deg(f)$. Berdasarkan konvensi, menetapkan $deg(0) = -\infty$. Polinomial yang berderajat 0 disebut polinomial konstan. Jika R mempunyai identitas 1 dan jika koefisien terdepan dari $f(x)$ adalah 1, maka $f(x)$ disebut polinomial monik.

(Lidl dan Niederreiter, 1983)

isalkan R adalah gelanggang, maka:
t komutatif jika dan hanya jika R bersifat komutatif.
n gelanggang beridentitas jika dan hanya jika R mempunyai

(Lidl dan Niederreiter, 1983)

Misalkan F menunjukkan suatu lapangan (tidak harus berhingga). Polinomial $g \in \mathbb{F}[x]$ membagi polinomial $f \in \mathbb{F}[x]$ jika terdapat polinomial $h \in \mathbb{F}[x]$ sehingga $f = gh$. Dapat dikatakan bahwa g adalah pembagi dari f, atau f adalah kelipatan g, atau f habis dibagi g. Satuan $\mathbb{F}[x]$ adalah pembagi dari polinomial konstanta 1, yang semuanya merupakan polinomial konstanta bukan nol.

Sedangkan untuk gelanggang bilangan bulat, terdapat pembagi dengan sisa pada gelanggang polinomial di atas lapangan.

Teorema 1.3 (Algoritma Pembagian). Misalkan $g \neq 0$ menjadi polinomial di $\mathbb{F}[x]$. Maka untuk sembarang $f \in \mathbb{F}[x]$ terdapat polinomial $q, r \in \mathbb{F}[x]$ sehingga $f = qg + r$, dengan $deg(r) < deg(g)$.

(Lidl dan Niederreiter, 1983)

Contoh 1.8 Misalkan $f(x) = 2x^5 + x^4 + 4x + 3 \in \mathbb{Z}_5[x]$, $g(x) = x^2 + 1 \in \mathbb{Z}_5[x]$. Menghitung polinomial $q, r \in \mathbb{Z}_5[x]$ dengan $f = qg + r$ menggunakan pembagian panjang:

$$
\begin{array}{r}
2x^3 + x^2 - 2x - 1 \\
x^2 + 1 \overline{)\, 2x^5 + x^4 + 4x + 3} \\
\underline{2x^5 + 2x^3} \quad - \\
x^4 - 2x^3 + 4x + 3 \\
\underline{x^4 + x^2} \quad - \\
-2x^3 - x^2 + 4x + 3 \\
\underline{-2x^3 - 2x} \quad - \\
-x^2 + 6x + 3 \\
\underline{-x^2 - 1} \quad - \\
6x + 4
\end{array}
$$

Jadi $q(x) = 2x^3 + x^2 - 2x - 1$, $r(x) = 6x + 4$, dan tentu saja $\deg(r) < \deg(g)$.

(Lidl dan Niederreiter, 1983)

Unsur prima pada gelanggang $\mathbb{F}[x]$ biasa disebut polinomial tak tereduksi. Untuk menekankan konsep ini, dapat dilihat pada definisi berikut.

Definisi 1.19 Suatu polinomial $p \in \mathbb{F}[x]$ dikatakan tidak tereduksi pada $\mathbb{F}$ (atau tidak dapat direduksi pada $\mathbb{F}[x]$, atau prima pada $\mathbb{F}[x]$) jika p berderajat positif dan $p = bc$ dengan $b, c \in \mathbb{F}[x]$ merupakan polinomial konstan.

(Lidl dan Niederreiter, 1983)

Dapat direduksi atau tidak dapat direduksi suatu polinomial tertentu sangat bergantung pada lapangan yang digunakan. Misalnya, polinomial $x^2 - 2 \in \mathbb{Q}[x]$ tidak dapat direduksi pada lapangan $\mathbb{Q}$ bilangan rasional, tetapi $x^2 - 2 =$ $\sqrt{2}$) dapat direduksi pada lapangan bilangan real.

uatu elemen $b \in \mathbb{F}$ disebut akar dari polinomial $f \in \mathbb{F}[x]$ jika $f(b) =$

(Lidl dan Niederreiter, 1983)

ting antara akar dan pembagian diberikan oleh teorema berikut.

Teorema 1.4 Suatu elemen $b \in \mathbb{F}$ adalah akar polinomial $f \in \mathbb{F}[x]$ jika dan hanya jika $x - b$ membagi $f(x)$.

(Lidl dan Niederreiter, 1983)

Definisi 1.21 Misalkan $b \in \mathbb{F}$ adalah akar dari polinomial $f \in \mathbb{F}[x]$. Jika k adalah bilangan bulat positif sehingga $f(x)$ habis dibagi $(x-b)^k$, tetapi tidak habis dibagi $(x-b)^{k+1}$, maka k disebut multiplisitas b. Jika $k = 1$, maka b disebut akar sederhana dari f.

(Lidl dan Niederreiter, 1983)

Teorema 1.5 Misalkan $f \in \mathbb{F}[x]$ dengan $deg\, f = n \geq 0$. Jika $b_1, \dots, b_m \in \mathbb{F}$ adalah akar-akar berbeda dari f dengan multiplisitas $k_1, \dots, k_m$, berturut-turut, maka $(x-b_1)^{k_1} \dots (x-b_m)^{k_m}$ membagi $f(x)$. Akibatnya, $k_1 + \cdots + k_m \leq n$, dan f bisa memiliki paling banyak n akar berbeda di $\mathbb{F}$.

(Lidl dan Niederreiter, 1983)

Teorema 1.6 Polinomial $f \in \mathbb{F}[x]$ berderajat *2* atau *3* tidak dapat direduksi dalam $\mathbb{F}[x]$ jika dan hanya jika f tidak memiliki akar pada $\mathbb{F}$.

(Lidl dan Niederreiter, 1983)

Contoh 1.9 Polinomial tak tereduksi di $\mathbb{F}_2[x]$ berderajat 2 atau 3 dapat diperoleh dengan menghilangkan polinomial dengan berakar pada $\mathbb{F}_2$ dari himpunan semua polinomial di $\mathbb{F}_2[x]$ berderajat 2 atau 3. Satu-satunya polinomial tak tereduksi di $\mathbb{F}_2[x]$ berderajat 2 adalah $f(x) = x^2 + x + 1$, dan polinomial tak tereduksi di $\mathbb{F}_2[x]$ berderajat 3 adalah $f_1(x) = x^3 + x + 1$ dan $f_2[x] = x^3 + x^2 + 1$.

(Lidl dan Niederreiter, 1983)

Selanjutnya akan diberikan definisi dari polinomial peubah banyak.

Definisi 1.22 Misalkan R melambangkan gelanggang komutatif dengan identitas dan misalkan $x_1, \dots, x_n$ adalah simbol yang berfungsi sebagai bilangan tak tentu. Elemen $R[x_1, \dots, x_n]$ di definisikan sebagai berikut,

$$f = f(x_1, \dots, x_n) = \sum a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$$

Dengan koefisien $a_{i_1 \dots i_n} \in R$, dimana penjumlahannya diperluas ke banyak n –tupel $(i, \dots, i_n)$ dari bilangan bulat non-negatif dan konvensi $x_j^0 = 1 (1 \leq j \leq n)$ diamati. Ekspresi seperti ini disebut polinomial dalam $x_1, \dots, x_n$ atas R. Dua polinomial $f, g \in R[x_1, \dots, x_n]$ adalah sama jika dan hanya jika semua koefisien yang sesuai adalah sama. Asumsikan bahwa $x_1, \dots, x_n$ dibolak-balik satu sama lain bermakna sama, seType equation here.hingga, misalnya, ekspresi $x_1 x_2 x_3 x_4$ dan $x_4 x_1 x_2 x_3$ diidentifikasi sama.

olinomial $f(x)$-stabil adalah $f(x) \neq 0 \; \forall \; x \in G|\{0\}$

(Park & Lee, 2001)

$(x) = x^2 + 1$ merupakan $f(x)$-stabil atas $\mathbb{Z}_{11}$ karena untuk setiap kibatkan $f(x) \neq 0$

$\Rightarrow f(1) = 1^2 + 1 = 2 \; mod \; 11 = 2$

Dengan cara yang sama diperoleh tabel berikut.

x	0	1	2	3	4	5	6	7	8	9	10
$f(x) = x^2 + 1$	1	2	5	10	6	4	4	6	10	5	2

1.6.6 Lapangan Hingga

Lapangan hingga merupakan struktur aljabar yang memiliki jumlah elemen yang berhingga.

Teorema 1.7 Misalkan $\mathbb{F}$ adalah lapangan dan $p(x)$ adalah suatu polinomial di $\mathbb{F}[X]$. Gelanggang faktor $\mathbb{F}[X]/[p(x)]$ membentuk lapangan jika dan hanya jika $p(x)$ adalah polinomial tak tereduksi di $\mathbb{F}[X]$.

(Gallian, 2021)

Contoh 1.11 Polinomial $x^2 + x + 1$ dapat digunakan untuk mengonstruksi lapangan hingga $\mathbb{Z}_2[X]/[x^2 + x + 1]$ karena polinomial $x^2 + x + 1$ adalah polinomial tak tereduksi. Lebih lanjut, di lapangan $\mathbb{Z}_2[X]/[x^2 + x + 1]$ (dengan menggunakan kesepakatan $p(x) + [x^2 + x + 1]$ cukup ditulis $p(x)$) diperoleh elemen-elemen lapangan hingga sebagai berikut yang ditunjukkan dalam bentuk tabel berikut.

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Contoh 1.12 Polinomial $x^3 + x^2 + 1$ adalah polinomial tak tereduksi di $\mathbb{Z}_2[X]$ sebab seandainya tereduksi maka polinomial berderajat 3 ini haruslah dapat dinyatakan sebagai perkalian polinomial berderajat 1 dan polinomial berderajat 2. Keberadaan faktor linier (polinomial berderajat 1) mengimplikasikan keberadaan akar. Sementara itu, $x^3 + x^2 + 1$ tidak mempunyai akar di $\mathbb{Z}_2$ karena apabila disubtitusi $x = 0$ dan $x = 1$, diperoleh $0^3 + 0^1 + 1 = 1 \neq 0$ dan juga diperoleh $1^3 + 1^2 + 1 = 1 \neq 0$. Ini adalah kontradiksi, sehingga haruslah $x^3 + x^2 + 1$ adalah polinomial tak tereduksi.

$x^3 + x^2 = 1$ adalah polinomial tak tereduksi di $\mathbb{Z}_2[X]$ maka $+ 1]$ membentuk lapangan. Di lapangan ini, diperoleh $x^3 = x^2 + 1$, $x^2 + x + 1$, $x^5 = x^3 + x^2 + 1 = x + 1$, $x^6 = x^2 + x$, dan $x^7 = x^3 +$

Contoh 1.13 Pemilihan polinomial tak tereduksi yang berbeda dapat memengaruhi hasil operasi perkalian pada lapangan yang dikonstruksi. Sebagai contoh, $x^3 + x + 1$ juga merupakan polinomial tak tereduksi di $\mathbb{Z}_2[X]$ sehingga dapat digunakan untuk mengonstruksi lapangan $\mathbb{Z}_2[X]/[x^3 + x + 1]$. Pada lapangan $\mathbb{Z}_2[X]/[x^3 + x + 1]$, diperoleh hasil kali $(x^2 + x)(x + 1) = x^3 + x^2 + x^2 + x = x^3 + x = x^2 + 1 + x$.

Dengan demikian, polinomial tak tereduksi yang digunakan dapat dijadikan sebagai kunci dalam proses enkripsi sebab pemilihan polinomial berbeda mengakibatkan hasil perhitungan aritmatika yang berbeda pula.

1.6.7 Polinomial Permutasi

Lebih spesifiknya, objek yang menjadi perhatian dalam skripsi ini adalah fungsi $f: \mathbb{F}_q \to \mathbb{F}_q$ yang mengubah elemen $\mathbb{F}_q$. Artinya, tertarik pada bijeksi $\mathbb{F}_q$. Diasumsikan bahwa fungsi tersebut adalah polinomial yang berderajat paling banyak $q - 1$.

Definisi 1.24 Suatu polinomial $f \in \mathbb{F}_q[x]$ disebut Polinomial Permutasi (PP) dari $\mathbb{F}_q$ jika fungsi polinomial terkait $f: c \to f(c)$ merupakan permutasi dari $\mathbb{F}_q$.

(Shallue, 2012)

Sifat berhingga dari $\mathbb{F}_q$ dapat digunakan untuk menyatakan definisi di atas dalam beberapa cara yang setara.

Lema 1.1 Polinomial $f \in \mathbb{F}_q[x]$ adalah polinomial permutasi dari $\mathbb{F}_q$ jika dan hanya jika salah satu kondisi berikut terpenuhi:

1. Fungsi $f: c \to f(c)$ adalah fungsi satu-satunya;
2. Fungsi $f: c \to f(c)$ adalah fungsi pada;
3. $f(x) = a$ mempunyai solusi dalam $\mathbb{F}_q$ untuk setiap $a \in \mathbb{F}_q$;
4. $f(x) = a$ mempunyai solusi unik di $\mathbb{F}_q$ untuk setiap $a \in \mathbb{F}_q$.

(Shallue, 2012)

Contoh 1.14 Perhatikan polinomial berikut,

$$f(x) = 3x^9 + 7x^8 + 4x^7 + 9x^6 + 8x^5 + 6x^4 + 2x^3 + 5x^2 + x + 1$$
$$= 3(x + 9)(x^4 + 5x + 8)(x^4 + 8x^3 + 10x^2 + 7x + 8) \in \mathbb{F}_{11}[x]$$

Dengan menghitung nilainya pada himpunan $\{0,1, \dots ,10\} = \mathbb{F}_{11}$ diperoleh

x	0	1	2	3	4	5	6	7	8	9	10
$f(x)$	1	2	0	3	4	5	6	7	8	9	10

Karena $f(x)$ adalah suatu bijeksi, maka $f(x)$ adalah polinomial permutasi dari $\mathbb{F}_{11}$, engamati bahwa $f(x)$ mewakili 3 siklus $(0,1,2)$.

(Shallue, 2012)

isalkan diberikan polinomial

$$g(x) = x^3 + 1 \in F_{11}[x]$$

ontoh sebelumnya periksa apakah g merupakan PP dari $\mathbb{F}_{11}$ itung nilainya pada $\mathbb{F}_{11}$. Diperoleh

x	0	1	2	3	4	5	6	7	8	9	10
$g(x)$	1	2	9	6	10	5	8	3	7	4	0

Perhatikan bahwa g adalah PP dari $\mathbb{F}_{11}$ dengan struktur siklus $(0,1,2,9,4,10)(3,6,8,7)$.
(Shallue, 2012)

Contoh 1.16 Misalkan diberikan polinomial

$$h(x) = x^2 + 3x + 5 \in F_{11}[x]$$

yang mengambil nilai-nilai tersebut

x	0	1	2	3	4	5	6	7	8	9	10
$h(x)$	5	9	4	1	0	1	4	9	5	3	3

Perhatikan bahwa $h(x)$ bukan PP dari $\mathbb{F}_{11}$.

1.6.8 Grup Polinomial Permutasi

Misalkan N adalah subgrup dari grup perkalian $G = \mathbb{F}_q{}^*$. Sebuah polinomial di $\mathbb{F}_q[x]$ disebut grup polinomial permutasi atas N atau hanya polinomial permutasi atas N jika polinomial tersebut menginduksi pemetaan satu-satu pada di N. Sebagai contoh, jika FPB$(r, |N|) = 1$ dan $\alpha \in N$, maka αx^r adalah sebuah grup polinomial permutasi atas N. Polinomial permutasi ini disebut monomials.