

BEBERAPA SIFAT DASAR POLINOMIAL PERMUTASI LOKAL



VIVIE LUTHVIANA

H011201023



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

**BEBERAPA SIFAT DASAR
POLINOMIAL PERMUTASI LOKAL**

VIVIE LUTHVIANA

H011201023



**PROGRAM STUDI MATEMATIKA DEPARTEMEN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS HASANUDDIN**

MAKASSAR

2024

**BEBERAPA SIFAT DASAR
POLINOMIAL PERMUTASI LOKAL**

VIVIE LUTHVIANA

H011201023

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 DASAR POLINOMIAL PERMUTASI LOKAL

VIVIE LUTHVIANA
H011201023


Skripsi,

telah dipertahankan di depan Panitia Ujian Sarjana Sains pada tanggal 8 Agustus 2024
dan dinyatakan telah memenuhi syarat kelulusan
pada

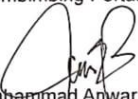
Program Studi Matematika
Departemen Matematika
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Hasanuddin
Makassar

Mengesahkan:

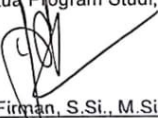
Pembimbing Utama,


Prof. Dr. Amir Kamal Amir, M.Sc.
NIP. 196808031992021001

Pembimbing Pertama,


Dr. Andi Muhammad Anwar, S.Si., M.Si.
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 Dasar Polinomial Permutasi Lokal" 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, 8 Agustus 2024



Vivie Luthviana
H011201023

UCAPAN TERIMA KASIH

Puji syukur atas kehadiran Allah *Subhanahu Wa ta'ala* yang telah melimpahkan rahmat dan hidayah-Nya. Shalawat serta salam senantiasa tercurahkan kepada junjungan Nabi Muhammad *Sallallahu 'Alaihi Wasallam*.

Penulis menyadari bahwa skripsi yang berjudul “Beberapa Sifat Dasar Polinomial Permutasi Lokal” ini dapat diselesaikan, karena adanya bantuan, dukungan, bimbingan, serta motivasi dari berbagai pihak. Oleh karena itu, pada kesempatan ini penulis menyampaikan rasa terima kasih yang sebesar-besarnya kepada orang tua penulis, **Fatma dan Burhan**, tante penulis **Suriani**, Nenek penulis **Pati**, serta seluruh keluarga yang telah memberikan doa dan dukungan dalam penyelesaian skripsi ini. Pada kesempatan ini pula, dengan segala kerendahan hati penulis ingin menyampaikan terima kasih kepada:

1. Bapak **Prof. Dr. Ir. Jamaluddin Jompa, M.Sc.**, selaku Rektor Universitas Hasanuddin beserta seluruh jajarannya, serta Bapak **Dr. Eng. Amiruddin** selaku Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam beserta jajarannya.
2. Bapak **Dr. Firman, S.Si., M.Si.**, selaku Ketua Departemen Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Hasanuddin sekaligus Tim Penguji.
3. Bapak **Prof. Dr. Amir Kamal Amir, M.Sc.**, dan Bapak **Dr. Andi Muhammad Anwar, S.Si., M.Si.** selaku Dosen Pembimbing yang dengan sabar, tulus, dan ikhlas banyak memberikan ilmu yang bermanfaat dan meluangkan waktu untuk membimbing dan memberi masukan serta motivasi dalam penulisan skripsi ini.
4. Bapak **Prof. Dr. Budi Nurwahyu, MS.**, selaku Tim Penguji sekaligus Dosen Penasehat Akademik penulis selama menempuh pendidikan sarjana.
5. Bapak dan Ibu Dosen Departemen Matematika yang telah memberikan banyak ilmu dan pengetahuan kepada penulis selama menjadi mahasiswa di Program Studi Matematika, serta Bapak dan Ibu Staff Departemen Matematika yang telah membantu dan memudahkan penulis dalam berbagai hal administrasi.
6. Teman-teman seperjuangan penulis, **Putri Jafar, Nurul Hidayah, Ariqah Mumtazah, Sitti Nurhalisa, Egidia, Nur Aulia Rahmadani Pratiwi, Nur Hasmah Sage, Naila Resqiyah, Ummu Kalsum**, serta seluruh pihak yang tidak dapat penulis sebut satu persatu yang senantiasa memberikan bantuan dan dukungan moril kepada penulis, serta memberikan momen berharga bagi penulis selama masa studi sarjana.
7. **Muh. Asman** yang senantiasa membersamai, memotivasi, teman berbagi pikiran, dan memberikan dukungan kepada penulis selama masa studi sarjana.

Akhir kata, penulis berharap semoga segala bentuk kebaikan yang telah diberikan bernilai ibadah dan mendapatkan balasan dari Allah *Subhanahu Wa Ta'ala*. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu pengetahuan.

Penulis

Vivie Luthviana

ABSTRAK

Vivie Luthviana. Beberapa Sifat Dasar Polinomial Permutasi Lokal. (Dibimbing oleh "Prof. Dr. Amir Kamal Amir, M.Sc." dan "Dr. Andi Muhammad Anwar, S.Si., M.Si.").

Polinomial permutasi lokal merupakan suatu kelas khusus dari polinomial yang memiliki sifat-sifat unik yang dapat digunakan dalam berbagai konteks matematika dan ilmu komputer serta memberikan kontribusi signifikan terhadap teori aljabar umum. Oleh karena itu, akan dikaji sifat dasar dan keluarga dari polinomial permutasi lokal dikaitkan dengan matriks sirkulan serta dibatasi oleh dua variable atas lapangan hingga. Untuk mengetahui hal tersebut yaitu dengan melakukan analisa data yang dimulai dengan menelaah seluruh konstruksi teoritis dari analisis mengenai polinomial permutasi lokal yang telah ada. Dengan melakukan pemetaan terhadap hasil-hasil terdahulu, mengetahui dan memahami teknik/metode pembuktian yang digunakan oleh peneliti terdahulu maka diperoleh definisi dari polinomial permutasi lokal. Polinomial $f: F_s \times F_s \rightarrow F_s$ yang menghasilkan persegi latin disebut polinomial permutasi lokal (atau LPP). Sebuah persegi latin berorde s adalah sebuah matriks L berukuran $s \times s$ dengan entri-entri dari suatu himpunan S dengan ukuran s sedemikian rupa sehingga setiap elemen dari S muncul tepat satu kali dalam setiap baris dan setiap kolom dari L . Misalkan L adalah sebuah persegi latin dengan orde t , dan misalkan $m \in \{1, \dots, t - 1\}$. L adalah m -sirkulan jika setiap baris diperoleh dengan menggeser secara siklis setiap entri di baris sebelumnya m tempat di sebelah kanan.

Kata kunci: Permutasi, Polinomial, Polinomial Permutasi Lokal, Matriks, Persegi Latin.

ABSTRACT

Vivie Luthviana. Some Basic Properties of Local Permutation Polynomials. (Guided by "Prof. Dr. Amir Kamal Amir, M.Sc." and "Dr. Andi Muhammad Anwar, S.Si., M.Si.").

Local permutation polynomials are a special class of polynomials that have unique properties that can be used in various mathematical and computer science contexts and make significant contributions to general algebraic theory. Therefore, we will study the basic properties and families of local permutation polynomials associated with a circular matrix and limited by two variables over a finite field. To find out this, you need to carry out data analysis which begins by examining all theoretical constructions from the analysis of existing local permutation polynomials. By mapping previous results, knowing and understanding the techniques/methods of proof used by previous researchers, we can obtain a definition of local permutation polynomials. A polynomial $f: F_s \times F_s \rightarrow F_s$ that gives rise to a Latin square is called a local permutation polynomial (or LPP). A Latin square of order s is an $s \times s$ matrix L with entries from a set S of size s such that each element of S occurs exactly once in every row and every column of L . Let L be a Latin square of order t , and let $m \in \{1, \dots, t - 1\}$. L is m -circulant if each row is obtained by cyclically shifting every entry in the previous row m places to the right.

Keywords: *Permutation, Polynomial, Local Permutation Polynomial, Matrix, Latin Square.*

DAFTAR ISI

| | Halaman |
|---|---------|
| HALAMAN JUDUL | i |
| PERNYATAAN PENGAJUAN..... | ii |
| HALAMAN PENGESAHAN..... | ii |
| PERNYATAAN KEASLIAN SKRIPSI..... | iii |
| UCAPAN TERIMA KASIH | v |
| ABSTRAK | vi |
| ABSTRACT | viii |
| DAFTAR ISI | viii |
| DAFTAR NOTASI..... | x |
| BAB I. PENDAHULUAN..... | 1 |
| 1.1 Latar Belakang..... | 1 |
| 1.2 Rumusan Masalah..... | 2 |
| 1.3 Batasan Penelitian..... | 2 |
| 1.4 Tujuan Penelitian | 2 |
| 1.5 Manfaat Penelitian | 2 |
| 1.6 Landasan Teori | 3 |
| 1.6.1 Grup | 3 |
| 1.6.2 Gelanggang..... | 4 |
| 1.6.3 Lapangan | 6 |
| 1.6.4 Permutasi | 7 |
| 1.6.5 Polinomial..... | 8 |
| 1.6.6 Lapangan Hingga..... | 11 |
| 1.6.7 Polinomial Permutasi..... | 13 |
| 1.6.8 Polinomial Permutasi Lokal | 14 |
| BAB II. METODOLOGI PENELITIAN..... | 15 |

| | | |
|-------------------------------------|----------------------------------|----|
| 2.1 | Metode Penelitian | 15 |
| 2.2 | Lokasi dan Waktu Penelitian..... | 15 |
| 2.3 | Prosedur Penelitian | 15 |
| BAB III. HASIL DAN PEMBAHASAN | | 17 |
| BAB IV. KESIMPULAN..... | | 33 |
| DAFTAR PUSTAKA | | 35 |

DAFTAR NOTASI

| Lambang | Arti dan penjelasan |
|----------------|----------------------------|
| \mathbb{Z} | Bilangan bulat |
| \mathbb{R} | Bilangan real |
| α | Alpha |
| σ | Sigma |
| β | Beta |
| τ | Tau |
| \mathbb{F} | Lapangan |
| \mathbb{F}_q | Lapangan Hingga |
| G | Grup |
| R | Gelanggang |

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 linear merupakan salah satu cabang ilmu matematika, yang mempelajari struktur aljabar termasuk sifat-sifat dari objek matematika seperti grup, gelanggang, lapangan, dan polinomial permutasi. Penelitian dalam bidang struktur aljabar merupakan salah satu aspek penting dalam pengembangan matematika modern. Melalui studi mendalam mengenai struktur aljabar, maka dapat dipahami dan dikembangkan konsep-konsep dasar salah satunya yaitu polinomial permutasi lokal. Polinomial permutasi memiliki peran penting dalam bidang keamanan informasi, seperti dalam desain algoritma enkripsi dan dalam kode koreksi kesalahan, serta mempelajari polinomial permutasi yang dapat membalikkan dirinya sendiri dalam konteks gelanggang komutatif lokal berhingga. Analisis lebih lanjut terhadap sifat-sifat polinomial dapat membantu memahami cara optimal dalam merestorasi data, serta memberikan wawasan baru dan meningkatkan efisiensi dalam pengembangan kode.

Polinomial permutasi lokal merupakan suatu kelas khusus dari polinomial yang memiliki sifat-sifat unik yang dapat digunakan dalam berbagai konteks matematika dan ilmu komputer serta memberikan kontribusi signifikan terhadap teori aljabar umum. Selain itu, sifat-sifat unik dari polinomial ini memungkinkannya digunakan dalam berbagai bidang praktis. Penting untuk dipahami bahwa permutasi adalah suatu pengaturan atau urutan elemen-elemen dalam suatu himpunan. Sementara itu, polinomial permutasi lokal dapat dianggap sebagai alat matematis yang memodelkan sifat permutasi dalam suatu domain tertentu. Menurut penelitian yang telah dilakukan, polinomial permutasi lokal memainkan peran penting dalam berbagai aspek teori aljabar dan aplikasinya. Misalnya, berkontribusi pada pengembangan konsep grup dan gelanggang, yang merupakan dasar dari banyak teori dan aplikasi matematika (Johnson, 2019).

Salah satu aplikasi utama dari polinomial permutasi lokal adalah dalam teori kode, khususnya dalam proses pengkodean dan dekoding informasi. Penelitian menunjukkan bahwa analisis lebih lanjut terhadap sifat-sifat polinomial dapat memberikan wawasan baru dan meningkatkan efisiensi dalam pengembangan kode dan protokol komunikasi (Wang, 2018). Dengan pemahaman yang mendalam, dapat menciptakan sistem komunikasi yang lebih andal dan efisien. Sifat dasar polinomial permutasi lokal juga dapat dihubungkan dengan masalah-masalah optimasi dan kombinatorika. Pemodelan dalam ilmu komputer polinomial permutasi lokal dapat digunakan untuk memodelkan struktur data dalam ilmu komputer, seperti representasi data dalam bentuk polinomial. Pemodelan menggunakan polinomial ini juga dapat membantu dalam memecahkan masalah optimasi yang kompleks, memberikan solusi yang lebih efektif dan efisien (Brown, 2017). Hal ini menunjukkan bahwa studi

mendalam mengenai polinomial permutasi lokal tidak hanya bermanfaat bagi teori aljabar, tetapi juga memiliki implikasi praktis yang signifikan dalam berbagai bidang lain.

Dalam ilmu komputer, polinomial permutasi lokal digunakan untuk memodelkan struktur data dan algoritma. Representasi data dalam bentuk polinomial dapat mempermudah manipulasi dan pengolahan data, serta meningkatkan efisiensi algoritma yang digunakan (Erkamin, 2024). Oleh karena itu pemahaman yang lebih baik mengenai sifat-sifat polinomial permutasi lokal dapat membantu dalam pengembangan algoritma dan struktur data yang lebih efisien, yang pada gilirannya dapat meningkatkan performa sistem komputasi.

Berdasarkan hal ini penulis tertarik untuk mengkaji lebih jauh sifat dasar polinomial permutasi lokal. Kajian ini diharapkan dapat memberikan kontribusi signifikan tidak hanya pada teori aljabar, tetapi juga pada aplikasi praktis dalam teori kode, optimasi, kombinatorika, dan ilmu komputer. Oleh karena itu, penelitian ini dituangkan dalam bentuk tulisan skripsi dengan judul:

“Beberapa Sifat Dasar Polinomial Permutasi Lokal”.

1.2 Rumusan Masalah

Polinomial $f: F_s \times F_s$ yang menghasilkan persegi latin yaitu suatu matriks L berukuran $s \times s$ dengan elemen-elemen a_{ij} adalah persegi latin jika dan hanya jika terdapat sebuah fungsi $f: S \times S \rightarrow S$ sedemikian hingga $f(i, j) = a_{ij} \forall i, j \in S$. Selain itu, $x, y, z \in S$ dan $y \neq z \Rightarrow f(x, y) \neq f(x, z)$, serta $x, y, z \in S$ dan $x \neq z \Rightarrow f(x, y) \neq f(z, y)$ disebut polinomial permutasi lokal (atau LPP). Dalam penelitian ini, rumusan masalah yang akan dikaji adalah bagaimana sifat dasar dan keluarga dari polinomial permutasi lokal dikaitkan dengan matriks sirkulan.

1.3 Batasan Penelitian

Berdasarkan rumusan masalah, diberikan batasan masalah yaitu polinomial permutasi lokal dibatasi oleh dua variable atas lapangan hingga.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah, maka penelitian ini bertujuan untuk menemukan sifat dasar dan keluarga dari polinomial permutasi lokal.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah

1. Memperluas pengetahuan dan pengembangan keilmuan dalam bidang ilmu matematika, secara khusus dalam aljabar.
2. Sebagai sarana penulis dalam mengembangkan ilmu pengetahuan yang selama ini menjadi bidang ilmu yang dipelajari.
3. Sebagai rujukan bagi pembaca untuk penelitian selanjutnya dan dapat mengembangkan ilmu matematika di bidang aljabar khususnya tentang polinomial permutasi lokal.

1.6 Landasan Teori

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

1.6.1 Grup

Pada himpunan semua bilangan bulat dikenal dua operasi penjumlahan dan perkalian yang dapat menggeneralisasi konsep operasi ke himpunan sembarang. Misalkan, S adalah himpunan dan misalkan $S \times S$ melambangkan himpunan semua pasangan terurut (s, t) dengan $s \in S, t \in S$. Maka pemetaan dari $S \times S$ ke S akan disebut operasi (biner) pada S . Berdasarkan definisi, pemetaan dari $(s, t) \in S \times S$ harus di S ; ini adalah sifat tertutup suatu operasi. Yang dimaksud dengan struktur aljabar adalah himpunan S dengan satu atau lebih operasi pada S .

Dalam aritmatika dasar diberikan dua operasi, penjumlahan dan perkalian, yang memiliki sifat asosiatif sebagai salah satu sifat terpentingnya. Dari berbagai struktur aljabar yang memiliki sifat asosiatif, grup merupakan struktur aljabar yang paling banyak dipelajari dan dikembangkan. Teori grup adalah salah satu bagian tertua dari aljabar abstrak dan juga kaya akan penerapan.

Definisi 1.6.1.1 *Grup adalah himpunan G dengan operasi biner $*$ pada G sehingga tiga sifat berikut berlaku:*

1. *Bersifat asosiatif; yaitu, untuk setiap $a, b, c \in G$,*

$$a * (b * c) = (a * b) * c.$$
2. *Terdapat elemen identitas (atau kesatuan) elemen e di G sehingga untuk setiap $a \in G$,*

$$a * e = e * a = a.$$

3. *Untuk setiap $a \in G$, terdapat elemen invers, $a^{-1} \in G$ sehingga*

$$a * a^{-1} = a^{-1} * a = e.$$

(Lidl dan Niederreiter, 1983)

Definisi 1.6.1.2 *Grup dinamakan grup abel (atau grup komutatif) jika memenuhi: Untuk setiap $a, b \in G$,*

$$a * b = b * a.$$

(Lidl dan Niederreiter, 1983)

Dapat ditunjukkan bahwa elemen identitas e dan elemen a^{-1} dari suatu elemen tertentu $a \in G$ bersifat tunggal. Selanjutnya, $(a * b)^{-1} = b^{-1} * a^{-1}$ untuk setiap $a, b \in G$.

Contoh 1.6.1.1 Pasangan $(\mathbb{Z}, +)$ dengan \mathbb{Z} adalah himpunan bilangan bulat dan $+$ adalah operasi penjumlahan biasa merupakan grup dengan elemen identitas 0. Operasi $+$ bersifat asosiatif di himpunan \mathbb{Z} dan setiap elemen $x \in \mathbb{Z}$ mempunyai invers penjumlahan $-x$. Grup ini juga merupakan grup abel karena bersifat komutatif.

Contoh 1.6.1.2 Pasangan $(V,*)$ dengan $V = \{e, a, b, c\}$ dan $*$ adalah operasi yang ditunjukkan oleh tabel berikut (hasil operasi $x * y$ disepakati ada di baris x dan kolom y untuk setiap x, y di V) merupakan grup dengan elemen identitas e . Tabel yang menunjukkan operasi dari tiap elemen pada sembarang himpunan yang dilengkapi oleh operasi seperti pada tabel berikut yang disebut dengan tabel Cayley.

| | | | | |
|-----|-----|-----|-----|-----|
| * | e | a | b | c |
| e | e | a | b | c |
| a | a | e | c | b |
| b | b | c | e | a |
| c | c | b | a | e |

Berdasarkan tabel di atas, dapat diperoleh semua hasil operasi dari elemen-elemen di grup V misalnya $a * b = c$. Grup ini juga adalah grup abel sebab operasinya bersifat komutatif yang dapat diamati dengan jelas dari kesimetrisan tabel Cayley terdapat sumbu diagonal.

Definisi 1.6.1.3 Subhimpunan H dari grup G adalah subgrup dari G jika H sendiri merupakan grup terhadap operasi G . Subgrup dari G selain subgrup trivial $\{e\}$ dan G itu sendiri disebut subgrup nontrivial dari G .

(Lidl dan Niederreiter, 1983)

1.6.2 Gelanggang

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 $(b + c) \cdot a = b \cdot a + c \cdot a$.

Elemen identitas pada gelanggang R untuk operasi $+$ menggunakan notasi 0 (disebut elemen nol), dan invers penjumlahan dari a dilambangkan dengan $-a$; juga, $a + (-b)$ disingkat dengan $a - b$. Hasil operasi $a \cdot b$ akan ditulis ab . Berdasarkan definisi, diperoleh sifat $a0 = 0a = 0$ untuk setiap $a \in R$. Selain itu, diperoleh juga sifat $(-a)b = a(-b) = -ab$ untuk setiap $a, b \in R$.

Definisi 1.6.2.1

1. Suatu gelanggang disebut gelanggang beridentitas jika gelanggang tersebut 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 1.6.2.1

1. Misalkan R adalah sembarang grup abel dengan operasi grup $+$. Didefinisikan $ab = 0$ untuk semua $a, b \in R$; maka R adalah sebuah gelanggang.

2. Himpunan $\mathbb{Z}_n = \{0, 1, 2, 3, \dots, n-1\}$ dengan operasi penjumlahan (+) modulo n merupakan gelanggang dengan unsur identitas penjumlahannya adalah 0.
3. Bilangan bulat genap membentuk gelanggang komutatif tanpa elemen identitas.
4. Himpunan semua matriks 2×2 dengan bilangan real sebagai entrinya membentuk gelanggang nonkomutatif terhadap operasi penjumlahan dan perkalian matriks.

(Lidl dan Niederreiter, 1983)

Definisi 1.6.2.2 Subhimpunan S dari gelanggang R disebut subgelanggang dari R asalkan S tertutup atas operasi $+$ dan \cdot dan memenuhi sifat gelanggang.

(Lidl dan Niederreiter, 1983)

Definisi 1.6.2.3 Subhimpunan J dari gelanggang R disebut ideal asalkan J adalah 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 1.6.2.2

1. Misalkan R adalah lapangan \mathbb{Q} dari bilangan rasional. Maka himpunan \mathbb{Z} bilangan bulat merupakan subring dari \mathbb{Q} , tetapi bukan ideal karena, misalkan $1 \in \mathbb{Z}, \frac{1}{2} \in \mathbb{Q}$, 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 1.6.2.4 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 aditif suatu gelanggang, maka J ideal dari gelanggang R mendefinisikan partisi R menjadi koset yang saling lepas, yang disebut kelas residu modulo J . Kelas residu elemen a dari R modulo J akan dilambangkan dengan $[a] = a + J$, karena terdiri dari semua elemen R yang berbentuk $a + c$ untuk beberapa $c \in J$. Elemen $a, b \in R$ disebut modulo kongruen J , ditulis $a \equiv b \pmod{J}$, jika berada di kelas residu yang sama modulo J , atau setara, jika $a - b \in J$. Verifikasi bahwa $a \equiv n \pmod{J}$ menyiratkan $a + r \equiv b + r \pmod{J}$, $ar \equiv br \pmod{J}$, dan $ra \equiv rb \pmod{J}$ untuk setiap $r \in R$ dan $na \equiv nb \pmod{J}$ untuk setiap $n \in \mathbb{Z}$. Jika, sebagai tambahan, $r \equiv s \pmod{J}$, maka $a + r \equiv b + s \pmod{J}$ dan $ar \equiv bs \pmod{J}$.

Hal ini ditunjukkan bahwa himpunan kelas residu dari sebuah gelanggang R modulo ideal J membentuk sebuah gelanggang sehubungan dengan operasinya.

$$(a + J) + (b + J) = (a + b) + J, \quad (a + J)(b + J) = ab + J.$$

Definisi 1.6.2.5 Gelanggang kelas residu dari gelanggang R modulo J disebut gelanggang kelas residu (atau gelanggang faktor) dari R modulo J dan dilambangkan dengan R/J .

(Lidl dan Niederreiter, 1983)

Contoh 1.6.2.3 (Gelanggang kelas residu $\mathbb{Z}/\langle n \rangle$). Seperti dalam kasus grup, yang menyatakan koset atau kelas residu dari bilangan bulat a modulo bilangan bulat positif n dengan $[a]$, serta dengan $a + \langle n \rangle$, dimana $\langle n \rangle$ adalah ideal utama yang dihasilkan oleh n . Elemen $\mathbb{Z}/\langle n \rangle$ adalah

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

(Lidl dan Niederreiter, 1983)

Pemetaan $\varphi: R \rightarrow S$ dari gelanggang R ke gelanggang S adalah homomorfisma jika untuk $a, b \in R$ memenuhi

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{dan} \quad \varphi(ab) = \varphi(a)\varphi(b)$$

Jadi homomorfisma $\varphi: R \rightarrow S$ mempertahankan operasi $+$ dan \cdot dalam R . Himpunan

$$\ker \varphi = \{a \in R : \varphi(a) = 0 \in S\}$$

disebut inti dari φ .

Teorema 1.6.2.1 (Teorema Homomorfisma untuk Gelanggang). Jika φ adalah suatu homomorfisma gelanggang R ke gelanggang S , maka $\ker \varphi$ adalah ideal dari R dan S .

(Lidl dan Niederreiter, 1983)

1.6.3 Lapangan

Definisi 1.6.3.1 Misalkan R struktur aljabar dengan dua buah operasi tambah dan kali. 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 $R \setminus \{0\}$ membentuk grup abel terhadap operasi perkalian. Oleh karena itu, diperoleh definisi alternatif bagi lapangan: Struktur aljabar $(R, +, \cdot)$ adalah lapangan jika berlaku:

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

Dapat disimpulkan bahwa sistem bilangan real dan sistem bilangan rasional membentuk lapangan. Sedangkan sistem bilangan bulat tidak membentuk lapangan. Hal ini karena di \mathbb{Z} terdapat unsur tak nol yang bukan unit. Contohnya $2 \in \mathbb{Z}$ tidak mempunyai balikan di \mathbb{Z} .

Contoh 1.6.3.1 Gelanggang factor $F = \mathbb{Z}_2[X]/[x^2 + x + 1]$ membentuk lapangan dengan operasi penjumlahan dan perkaliannya dapat dilihat pada tabel berikut: ($p(x) + [x^2 + x + 1]$ cukup ditulis $p(x)$ dengan $p(x)$ adalah polinomial di $\mathbb{Z}_2[x]$).

| | | | | |
|---------|---------|---------|---------|---------|
| + | 0 | 1 | x | $x + 1$ |
| 0 | 0 | 1 | x | $x + 1$ |
| 1 | 1 | 0 | $x + x$ | x |
| x | x | $x + 1$ | 0 | 1 |
| $x + 1$ | $x + 1$ | x | 1 | 0 |
| · | 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 |

1.6.4 Permutasi

Definisi 1.6.4.1 Misalkan S himpunan tak kosong. Maka permutasi pada S adalah pemetaan di S^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 $|S| = n$, gunakan 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 1.6.4.1 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 $a_0 + a_1x + \dots + a_nx^n$. dengan a_i disebut koefisien ; x dipandang sebagai variabel: yaitu, dengan mensubstitusi bilangan sembarang a dengan x , diperoleh bilangan yang terdefinisi dengan baik $a_0 + a_1a + \dots + a_na^n$. Aritmatika polinomial diatur oleh aturan yang sudah dikenal. Konsep polinomial yang terkait operasi dapat digeneralisasikan ke pengaturan aljabar formal dengan cara yang langsung.

Definisi 1.6.5.1 Misalkan R adalah gelanggang sembarang. Polinomial di atas R adalah ekspresi dari bentuk

$$f(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1x + \dots + a_nx^n$$

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

Polinomial

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

pada R dikatakan sama jika dan hanya jika $a_i = b_i$ untuk $0 \leq i \leq n$.

Selanjutnya, mendefinisikan operasi penjumlahan,

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

Misalkan,

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

Sehingga didefinisikan operasi perkalian,

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

Dapat dilihat bahwa dengan operasi ini himpunan polinomial di 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 1.6.5.2 Misalkan $f(x) = \sum_{i=0}^n a_i x^i$ adalah polinomial pada R yang bukan polinomial nol, sehingga dapat dianggap $a_n \neq 0$. 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)

Teorema 1.6.5.1 Misalkan R adalah gelanggang, maka:

1. $R[x]$ bersifat komutatif jika dan hanya jika R bersifat komutatif.
2. $R[x]$ adalah gelanggang beridentitas jika dan hanya jika R mempunyai identitas.

(Lidl dan Niederreiter, 1983)

Misalkan F menunjukkan suatu lapangan (tidak harus berhingga). Konsep keterbagian, bila dikhususkan pada gelanggang $F[x]$, mengarah pada hal berikut. Polinomial $g \in F[x]$ membagi polinomial $f \in F[x]$ jika terdapat polinomial $h \in F[x]$ sehingga $f = gh$. Dapat dikatakan bahwa g adalah pembagi dari f , atau f adalah kelipatan g , atau f habis dibagi g . Satuan $F[x]$ 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 atas lapangan.

Teorema 1.6.5.2 (Algoritma Pembagian). Misalkan $g \neq 0$ menjadi polinomial di $F[x]$. Maka untuk sembarang $f \in F[x]$ terdapat polinomial $q, r \in F[x]$ sehingga

$$f = qg + r, \quad \text{dengan } \deg(r) < \deg(g).$$

(Lidl dan Niederreiter, 1983)

Contoh 1.6.5.1 Misalkan $f(x) = 2x^5 + x^4 + 4x + 3 \in \mathbb{Z}_5[x]$, $g(x) = 3x^2 + 1 \in \mathbb{Z}_5[x]$. Menghitung polinomial $q, r \in \mathbb{Z}_5[x]$ dengan $f = qg + r$ menggunakan pembagian panjang:

$$\begin{array}{r} 4x^3 + 2x^2 + 2x + 1 \\ 3x^2 + 1 \sqrt{2x^5 + x^4 + 4x + 3} \\ \underline{-2x^5 - 4x^3} \\ x^4 + x^3 \\ \underline{-x^4 - 2x^3} \\ x^3 + 3x^2 + 4x \\ \underline{-x^3 - 2x} \\ 3x^2 + 2x + 3 \\ \underline{-3x^3 - 1} \\ + 2x + 2 \end{array}$$

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

(Lidl dan Niederreiter, 1983)

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

Definisi 1.6.5.3 Suatu polinomial $p \in F[x]$ dikatakan tidak tereduksi pada F (atau tidak dapat direduksi pada $F[x]$, atau prima pada $F[x]$) jika p berderajat positif dan $p = bc$ dengan $b, c \in F[x]$ 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 $x^2 - 2 = (x + \sqrt{2})(x - \sqrt{2})$ dapat direduksi pada lapangan bilangan real.

Definisi 1.6.5.4 Suatu elemen $b \in F$ disebut akar dari polinomial $f \in F[x]$ jika $f(b) = 0$.

(Lidl dan Niederreiter, 1983)

Hubungan penting antara akar dan pembagian diberikan oleh teorema berikut.

Teorema 1.6.5.3 Suatu elemen $b \in F$ adalah akar polinomial $f \in F[x]$ jika dan hanya jika $x - b$ membagi $f(x)$.

(Lidl dan Niederreiter, 1983)

Definisi 1.6.5.5 Misalkan $b \in F$ adalah akar dari polinomial $f \in F[x]$. 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 1.6.5.4 Misalkan $f \in F[x]$ dengan $\deg f = n \geq 0$. Jika $b_1, \dots, b_m \in F$ 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, $k_1 + \dots + k_m \leq n$, dan f bisa memiliki paling banyak n akar berbeda di F .

(Lidl dan Niederreiter, 1983)

Teorema 1.6.5.5 Polinomial $f \in F[x]$ berderajat 2 atau 3 tidak dapat direduksi dalam $F[x]$ jika dan hanya jika f tidak berakar pada F .

(Lidl dan Niederreiter, 1983)

Contoh 1.6.5.2 Polinomial tak tereduksi di $F_2[x]$ berderajat 2 atau 3 dapat diperoleh dengan menghilangkan polinomial dengan berakar pada F_2 dari himpunan semua polinomial di $F_2[x]$ berderajat 2 atau 3. Satu-satunya polinomial tak tereduksi di $F_2[x]$ berderajat 2 adalah $f(x) = x^2 + x + 1$, dan polinomial tak tereduksi di $F_2[x]$ berderajat 3 adalah $f_1(x) = x^3 + x + 1$ dan $f_2(x) = x^3 + x^2 + 1$.

(Lidl dan Niederreiter, 1983)

Dalam analisis dasar terdapat metode terkenal untuk membangun polinomial dengan koefisien riil yang mengasumsikan nilai tertentu yang ditetapkan untuk nilai tak tentu tertentu. Metode yang sama dapat diterapkan pada bidang apapun.

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_1, \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 di 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, sehingga, ekspresi $x_1x_2x_3x_4$ dan $x_4x_1x_3x_2$ diidentifikasi sama.

1.6.6 Lapangan Hingga

Teorema 1.6.6.1 Misalkan \mathbb{F} adalah lapangan hingga. Banyaknya elemen dari lapangan \mathbb{F} adalah p^n dengan p bilangan prima dan $n \in \mathbb{N}$. Selanjutnya, jika terdapat lapangan \mathbb{G} yang banyak elemennya juga adalah p^n maka $\mathbb{F} \cong \mathbb{G}$. Karena semua lapangan hingga berorde (yang mempunyai banyak elemen) p^n dinotasikan dengan $GF(p^n)$ atau \mathbb{F}_{p^n} .

(Jacobson, 1985)

Contoh 1.6.6.1 Gelanggang \mathbb{Z}_p dengan p adalah bilangan prima membentuk lapangan hingga.

Definisi 1.6.6.1 (Polinomial Tak Tereduksi) Misalkan F adalah lapangan dan $F[X]$ adalah gelanggang polinomial dengan koefisien-koefisiennya di F . Suatu polinomial $p(x) \in F[X]$ dikatakan tak tereduksi jika dan hanya jika $p(x)$ adalah polinomial tak konstan (berderajat $r \geq 1$) dan tidak dapat dinyatakan sebagai perkalian dua polinomial tak konstan di $F[X]$. Dengan kata lain, $p(x)$ tidak bisa dinyatakan sebagai $f(x)g(x)$ dengan derajat $f(x)$ dan $g(x)$ lebih dari 0.

(Gallian, 2021)

Contoh 1.6.6.2 $x^6 + x^5 + x^3 + x^2 + 1$ adalah salah satu polinomial di $\mathbb{Z}_2[X]$ yang tak tereduksi.

(Ruskey, 1970)

Teorema 1.6.6.2 Misalkan F adalah lapangan dan $p(x)$ adalah suatu polinomial di $F[X]$. Gelanggang faktor $F[X]/[p(x)]$ membentuk lapangan jika dan hanya jika $p(x)$ adalah polinomial tak tereduksi di $F[X]$.

(Gallian, 2021)

Contoh 1.6.6.3 Polinomial $x^6 + x^5 + x^3 + x^2 + 1$ dari contoh di atas dapat digunakan untuk mengonstruksi lapangan Galois $\mathbb{Z}_2[X]/[x^6 + x^5 + x^3 + x^2 + 1]$ karena polinomial $x^6 + x^5 + x^3 + x^2 + 1$ adalah polinomial tak tereduksi. Lebih lanjut, di lapangan $\mathbb{Z}_2[X]/[x^6 + x^5 + x^3 + x^2 + 1]$ (dengan menggunakan kesepakatan $p(x) + [x^6 + x^5 + x^3 + x^2 + 1]$ cukup ditulis $p(x)$) diperoleh

$$x^6 = x^5 + x^3 + x^2 + 1, x^7 = x^6 + x^4 + x^3 + x = x^5 + x^4 + x^2 + x + 1,$$

$$x^8 = x^6 + x^5 + x^3 + x^2 + x = x + 1, x^9 = x^2 + x, x^{10} = x^3 + x^2,$$

$$x^{11} = x^4 + x^3, x^{12} = x^5 + x^4, x^{13} = x^6 + x^5 = x^3 + x^2 + 1,$$

$$x^{14} = x^4 + x^3 + x, x^{15} = x^5 + x^4 + x^2, x^{16} = x^6 + x^5 + x^3 = x^2 + 1,$$

$$x^{17} = x^3 + x, x^{18} = x^4 + x^2, x^{19} = x^5 + x^3,$$

$$x^{20} = x^6 + x^4 = x^5 + x^4 + x^3 + x^2 + 1,$$

$$x^{21} = x^6 + x^5 + x^4 + x^3 + x = x^4 + x^2 + x + 1,$$

$$x^{22} = x^5 + x^3 + x^2 + x, x^{23} = x^6 + x^4 + x^3 + x^2 = x^5 + x^4 + 1,$$

$$x^{24} = x^6 + x^5 + x = x^3 + x^2 + x + 1, x^{25} = x^4 + x^3 + x^2 + x,$$

$$\begin{aligned}
x^{26} &= x^5 + x^4 + x^3 + x^2, x^{27} = x^6 + x^5 + x^4 + x^3 = x^4 + x^2 + 1, \\
x^{28} &= x^5 + x^3 + x, x^{29} = x^6 + x^4 + x^2 = x^5 + x^4 + x^3 + 1, \\
x^{30} &= x^6 + x^5 + x^4 + x = x^4 + x^3 + x^2 + x + 1, \\
x^{31} &= x^5 + x^4 + x^3 + x^2 + x, x^{32} = x^6 + x^5 + x^4 + x^3 + x^2 = x^4 + 1, \\
x^{33} &= x^5 + x, x^{34} = x^6 + x^2 = x^5 + x^3 + 1, \\
x^{35} &= x^6 + x^4 + x = x^5 + x^4 + x^3 + x^2 + x + 1, \\
x^{36} &= x^6 + x^5 + x^4 + x^3 + x^2 + x = x^4 + x + 1, x^{37} = x^5 + x^2 + x, \\
x^{38} &= x^6 + x^3 + x^2 = x^5 + 1, x^{39} = x^6 + x = x^5 + x^3 + x^2 + x + 1, \\
x^{40} &= x^6 + x^4 + x^3 + x^2 + x = x^5 + x^4 + x + 1, \\
x^{41} &= x^6 + x^5 + x^2 + x = x^3 + x + 1, x^{42} = x^4 + x^2 + x, \\
x^{43} &= x^5 + x^3 + x^2, x^{44} = x^6 + x^4 + x^3 = x^5 + x^4 + x^2 + 1, \\
x^{45} &= x^6 + x^5 + x^3 + x = x^2 + x + 1, x^{46} = x^3 + x^2 + x, \\
x^{47} &= x^4 + x^3 + x^2, x^{48} = x^5 + x^4 + x^3, \\
x^{49} &= x^6 + x^5 + x^4 = x^4 + x^3 + x^2 + 1, x^{50} = x^5 + x^4 + x^3 + x, \\
x^{51} &= x^6 + x^5 + x^4 + x^2 = x^4 + x^3 + 1, x^{52} = x^5 + x^4 + x, \\
x^{53} &= x^6 + x^5 + x^2 = x^3 + 1, x^{54} = x^4 + x, x^{55} = x^5 + x^2, \\
x^{56} &= x^6 + x^3 = x^5 + x^2 + 1, x^{57} = x^6 + x^3 + x = x^5 + x^2 + x + 1, \\
x^{58} &= x^6 + x^3 + x^2 + x = x^5 + x + 1, \\
x^{59} &= x^6 + x^2 + x = x^5 + x^3 + x + 1, \\
x^{60} &= x^6 + x^4 + x^2 + x = x^5 + x^4 + x^3 + x + 1, \\
x^{61} &= x^6 + x^5 + x^4 + x^2 + x = x^4 + x^3 + x + 1, \\
x^{62} &= x^5 + x^4 + x^2 + x, x^{63} = x^6 + x^5 + x^3 + x^2,
\end{aligned}$$

Serta x, x^2, x^3, x^4, x^5 , dan 0 merupakan semua koset yang mungkin dari $[x^6 + x^5 + x^3 + x^2 + 1]$ yang masing-masing berkorespondensi dengan polinomial berderajat 5 ke bawah. Selain itu, grup kali $\left(\mathbb{Z}_2[X]/[x^6 + x^5 + x^3 + x^2 + 1]^\times, \cdot\right)$ adalah grup siklik berorde 63 dengan x sebagai generator siklik sehingga $\mathbb{Z}_2[X]/[x^6 + x^5 + x^3 + x^2 + 1]^\times \cong \mathbb{Z}_{63}$. Jadi, setiap elemen tak nol di $\mathbb{Z}_2[X]/[x^6 + x^5 + x^3 + x^2 + 1]$ yang dinyatakan dalam bentuk polinomial dapat ditulis sebagai perpangkatan dari x .

Contoh 1.6.6.4 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 disubstitusi $x = 0$ dan $x = 1$, diperoleh $0^3 + 0^2 + 1 = 1 \neq 0$ 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.

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

$$\begin{aligned}
x^3 &= x^2 + 1, \\
x^4 &= x^3 + x = x^2 + x + 1, \\
x^5 &= x^3 + x^2 + 1 = x + 1,
\end{aligned}$$

$$x^6 = x^2 + x, \text{ dan}$$

$$x^7 = x^3 + x^2 = 1.$$

Contoh 1.6.6.5 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

Definisi 1.6.7.1 Suatu polinomial $f \in F_q[x]$ disebut Polinomial Permutasi (PP) dari F_q jika fungsi polinomial terkait $f: c \rightarrow f(c)$ merupakan permutasi dari F_q .

(Shallue, 2012)

Dengan keterbatasan F_q , dapat menyatakan definisi ini dalam beberapa cara yang setara.

Lemma 1.6.7.1 Polinomial $f \in F_q[x]$ adalah polinomial permutasi dari F_q jika dan hanya jika salah satu kondisi berikut terpenuhi:

1. Fungsi $f: c \rightarrow f(c)$ adalah fungsi satu-satunya;
2. Fungsi $f: c \rightarrow f(c)$ adalah fungsi pada;
3. $f(x) = a$ mempunyai solusi dalam F_q untuk setiap $a \in F_q$;
4. $f(x) = a$ mempunyai solusi unik di F_q untuk setiap $a \in F_q$.

(Shallue, 2012)

Contoh 1.6.7.1 Pertimbangkan polinomialnya

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

$$= 3(x + 9)(x^4 + 5x + 8)(x^4 + 8x^3 + 10x^2 + 7x + 8) \in F_{11}[x]$$

Dengan menghitung nilainya pada himpunan $\{0,1, \dots, 10\} = F_{11}$ 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 F_{11} , dan dengan mengamati bahwa $f(x)$ mewakili 3 siklus (0,1,2).

(Shallue, 2012)

Contoh 1.6.7.2 Pertimbangkan polinomialnya

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

Seperti pada contoh sebelumnya periksa apakah g merupakan PP dari F_{11} dengan menghitung nilainya pada 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 |

Lihat bahwa g adalah PP dari F_{11} dengan struktur siklus $(0,1,2,9,4,10)(3,6,8,7)$.

(Shallue, 2012)

Contoh 1.6.7.3 Terakhir, pertimbangkan 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 |

Lihat bahwa $h(x)$ bukan PP dari F_{11} .

1.6.8 Polinomial Permutasi Lokal

Definisi 1.6.8.1 Suatu persegi latin berorde s adalah sebuah matriks L berukuran $s \times s$ dengan entri-entri dari himpunan S yang ukuran s sedemikian sehingga setiap elemen dari S muncul tepat satu kali dalam setiap baris dan setiap kolom dari L .

(Diestelkamp, dkk., 2004)

Definisi 1.6.8.2 (Mullen) Polinomial $f: F_s \times F_s \rightarrow F_s$ yang menghasilkan persegi latin disebut polinomial permutasi lokal (atau LPP).

(Diestelkamp, dkk., 2004)

Contoh 1.6.8.1 Misalkan $S = \{0,1,2\}$. Berikut ini adalah persegi latin dengan orde 3 pada S : (Perhatikan bahwa S adalah sebuah himpunan 3 – elemen sembarang). Dengan fungsi polinomial $f(x, y) = x + y + 1$, yaitu:

| | | | |
|-----|---|---|---|
| f | 0 | 1 | 2 |
| 0 | 1 | 2 | 0 |
| 1 | 2 | 0 | 1 |
| 2 | 0 | 1 | 2 |

BAB II

METODOLOGI PENELITIAN

Pada bab ini dibahas mengenai metodologi penelitian yang mencakup metode penelitian, lokasi dan waktu penelitian, serta prosedur penelitian.

2.1 Metode Penelitian

Penelitian yang dilakukan dalam penyusunan tugas akhir ini adalah penelitian Pustaka (*library research*) dan analisis deskriptif, yakni melakukan penelitian terhadap beberapa literatur-literatur yang ada seperti dari buku, jurnal ilmiah, dan artikel di internet atau literatur lainnya yang terkait dengan polinomial permutasi lokal.

2.2 Lokasi dan Waktu Penelitian

Penelitian ini dilakukan di Universitas Hasanuddin tepatnya di Laboratorium Aljabar dan Kombinatorika Departemen Matematika FMIPA Universitas Hasanuddin. Waktu penelitian berlangsung sejak Februari 2024.

2.3 Prosedur Penelitian

Penelitian ini dilaksanakan dengan langkah-langkah sebagai berikut:

1. Pengumpulan Jurnal dan Literatur Terkait Penelitian.
Studi literatur dengan referensi berasal dari buku, jurnal ilmiah, artikel, dan sumber lain yang berhubungan dengan pokok bahasan yang diteliti.
2. Analisis Literatur.
Analisa data dimulai dengan menelaah seluruh konstruksi teoritis dari analisis mengenai polinomial permutasi lokal yang telah ada. Target pada tahap ini adalah dapat melakukan pemetaan terhadap hasil-hasil terdahulu, mengetahui dan memahami Teknik/metode pembuktian yang digunakan oleh peneliti terdahulu.
3. Konstruksi Teori.
Pada proses konstruksi teori baru ini semua prinsip-prinsip penalaran baik secara induktif dan deduktif akan digunakan secara penuh, mulai dari reduksi data, paparan data, dan penarikan kesimpulan.
4. Verifikasi Hasil.
Tahap akhir dilakukan verifikasi semua hasil yang telah dicapai dengan menyajikan semua hasil pada tahap-tahap sebelumnya.
5. Penyempurnaan.
Pada tahap ini, hasil penelitian yang telah diperoleh akan ditulis dalam bentuk Skripsi menggunakan Microsoft Word.

Langkah-langkah dalam penelitian ini dapat digambarkan melalui diagram alur penelitian sebagai berikut:

