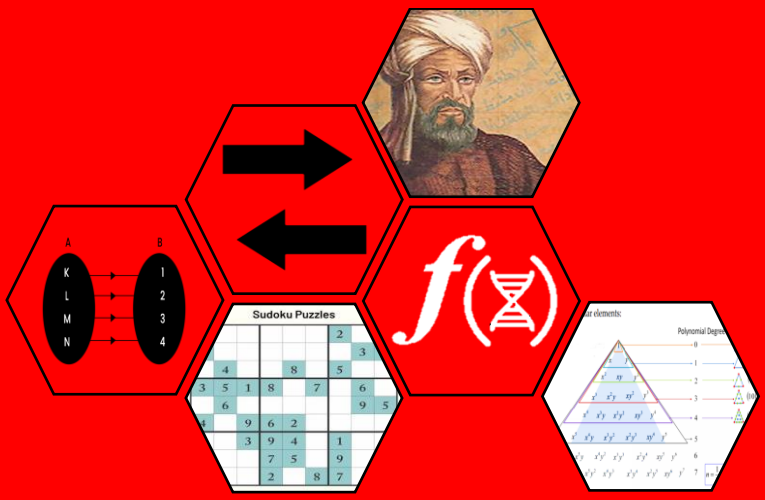
BEBERAPA SIFAT PASANGAN POLINOMIAL PERMUTASI



EGIDIA

H011201012

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

BEBERAPA SIFAT PASANGAN POLINOMIAL PERMUTASI

EGIDIA

H011201012

PROGRAM STUDI MATEMATIKA DEPARTEMEN MATEMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS HASANUDDIN

MAKASSAR

2024

BEBERAPA SIFAT PASANGAN POLINOMIAL PERMUTASI

EGIDIA

H011201012

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 PASANGAN POLINOMIAL PERMUTASI

EGIDIA

H011201012

Skripsi,

telah dipertahankan di depan Panitia Ujian Sarjana pada tanggal 09 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

KEMENTERIAN PENDIDIKAN DAN KEBUDAYAAN UNIVERSITAS HASANUDDIN DEPARTEMEN MATEMATIKA FAKULTAS MIPA

PERNYATAAN KEASLIAN SKRIPSI
DAN PELIMPAHAN HAK CIPTA

Dengan ini saya menyatakan bahwa, skripsi berjudul "Beberapa Sifat Pasangan 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, 09 Agustus 2024

Egidia

H011201012

UCAPAN TERIMA KASIH

Penulis mengucapkan syukur kepada Allah SWT atas rahmat dan hidayah-Nya. Shalawat dan salam kepada Nabi Muhammad SAW. Pada kesempatan ini pula, dengan segala kerendahan hati penulis ingin menyampaikan terima kasih kepada:

1. Kedua orang tua, ayah **Kamiluddin** dan ibu **Narti**, yang telah memberikan dukungan, doa, dan kasih sayang yang tak terhingga. Serta adik **Esti Aprilia Putri** dan **Estrid Amey Putri** yang telah menjadi sahabat dan motivasi bagi penulis.
2. 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.
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 dan memberikan arahan kepada penulis, serta meluangkan banyak waktu sehingga penulis dapat menyelesaikan skripsi ini.
4. Bapak **Prof. Dr. Eng. Mawardi, S.Si., M.Si.,** dan Ibu **Jusmawati Massalesse, S.Si., M.Si.** selaku penguji yang telah meluangkan waktunya untuk memberikan ilmu, saran, dan arahan kepada penulis dalam menyelesaikan skripsi ini.
5. Seluruh **Dosen** Departemen Matematika yang telah memberikan banyak ilmu dan pengetahuan kepada penulis selama menjadi mahasiswi di Program Studi Matematika, serta para **Staff** Departemen Matematika yang telah membantu dan memudahkan penulis dalam berbagai hal administrasi.
6. Kakak **Muhammad Yunus** yang senantiasa memberikan doa, bantuan dan dukungan baik moril maupun materil agar peneliti lebih semangat dalam menyelesaikan skripsi.
7. Kakak **Nurelisa** dan teman-teman seperjuangan penulis, **Sitti Nurhalisa, Vivie Luthviana** dan **Ariqah Mumtazah** yang telah mewarnai dunia perkuliahan penulis, senantiasa membersamai, menginspirasi, teman berbagi pikiran, dan memberikan dukungan kepada penulis selama masa studi sarjana.
8. Seluruh pihak yang tidak dapat penulis sebut satu persatu, terima kasih untuk segala dukungan, doa, motivasi, inspirasi, dan partisipasi yang diberikan kepada penulis.

Semoga skripsi ini membawa manfaat bagi pengembangan ilmu pengetahuan dan menjadi salah satu bentuk syukur kepada Allah SWT.

Penulis,

Egidia

ABSTRAK

EGIDIA. **Beberapa Sifat Pasangan Polinomial Permutasi**. (Dibimbing oleh “Prof. Dr. Amir Kamal Amir, M.Sc.” dan “Dr. Andi Muhammad Anwar, S.Si., M.Si.”).

Polinomial permutasi merupakan salah satu cabang dari matematika yang mempelajari bentuk dan sifat-sifat permutasi polinomial. Penelitian ini bertujuan untuk menunjukkan keterkaitan antara polinomial permutasi dengan pasangan permutasi dan sifat pasangan polinomial permutasi. Dalam penelitian ini, kita membahas tentang tupel polinomial permutasi dalam dua variabel atas lapangan hingga. Hasil penelitian menunjukkan bahwa polinomial permutasi lokal dapat diwakili sebagai q-tupel permutasi yang memenuhi syarat tertentu. Selain itu, kita juga menemukan bahwa terdapat pemetaan bijektif antara himpunan polinomial permutasi lokal dan himpunan q-tupel permutasi yang memenuhi syarat tersebut. Penelitian ini juga membahas tentang konsep keserupaan antara tupel polinomial permutasi dan polinomial permutasi lokal. Hasil penelitian ini diharapkan dapat memberikan kontribusi pada pemahaman yang lebih baik tentang keterkaitan antara polinomial permutasi dengan pasangan permutasi dan sifat pasangan polinomial permutasi.

Kata kunci: Polinomial Permutasi, Pasangan Permutasi, Tupel Polinomial Permutasi, Lapangan Hingga.

ABSTRACT

EGIDIA. ***Some Properties of Permutation Polynomial Pairs****. (Guided by "Prof. Dr. Amir Kamal Amir, M.Sc." and "Dr. Andi Muhammad Anwar, S.Si., M.Si.").*

Permutation polynomials are a branch of mathematics that studies the forms and properties of permutation polynomials. This research aims to show the relationship between permutation polynomials and permutation pairs, as well as the properties of permutation polynomial pairs. In this study, we discuss the tuple permutation polynomials in two variables over finite fields. The results show that local permutation polynomials can be represented as q-tuples of permutations that satisfy certain conditions. Additionally, we find that there is a bijective mapping between the set of local permutation polynomials and the set of q-tuples of permutations that satisfy these conditions. This research also discusses the concept of similarity between tuple permutation polynomials and local permutation polynomials. The results of this research are expected to contribute to a better understanding of the relationship between permutation polynomials and permutation pairs, as well as the properties of permutation polynomial pairs.

Keywords: *Permutation Polynomials, Permutation Pairs, Tuple Permutation Polynomials, Finite Fields.*

DAFTAR ISI

Halaman

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR NOTASI

Alpha		α
Beta		β
Gamma	Γ	
Delta		δ
Sigma	Σ	σ
Omega	Ω	
Phi	φ	
Bilangan bulat	$\mathbb{Z}$	
Bilangan real	$\mathbb{R}$	
Bilangan rasional	$\mathbb{Q}$	
Lapangan	$\mathbb{F}$	
Lapangan hingga	$\mathbb{F}_q$	
Elemen	$\in$	
Tau	τ	
Ruang vektor	$\boldsymbol{V}$	
Grup	$\boldsymbol{G}$	
Gelanggang	$\boldsymbol{R}$	

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 adalah cabang dari matematika yang mempelajari konsep-konsep operasi antara objek matematis linear seperti bilangan, vektor, dan matriks. Kata "linear" dalam aljabar linear berarti bahwa operasi yang digunakan, seperti penjumlahan dan perkalian, menghasilkan objek linear baru yang merupakan kombinasi linear dari objek aslinya. Aljabar linear memiliki latar belakang yang panjang dan kompleks, yang memicu perkembangan yang signifikan dalam berbagai bidang matematika, ilmu komputer, dan teknologi. Hingga saat ini, aljabar linear masih menjadi dasar untuk berbagai bidang ilmu pengetahuan dan teknologi, seperti ilmu komputer, teori kontrol, teori informasi, dan pemrograman komputer. Aljabar linear digunakan dalam pengembangan algoritma machine learning, neural network, computer vision, dan lain-lain. Selain itu, aljabar linear juga digunakan dalam analisis data, statistika, dan ekonomi.

Dalam kaitannya dengan pemrograman komputer, aljabar linear menjadi dasar untuk memecahkan masalah linear dan non-linear menggunakan komputer. Aljabar linear memungkinkan untuk menggambarkan masalah sebagai sistem persamaan linier, yang kemudian dapat diselesaikan menggunakan metode-metode aljabar linear. Hal ini membuat aljabar linear menjadi sangat penting dalam pengembangan perangkat lunak dan sistem komputer. Penelitian tentang struktur aljabar adalah bagian penting dari pengembangan matematika kontemporer. Melakukan penelitian mendalam tentang struktur aljabar memungkinkan untuk memahami dan mengembangkan konsep-konsep penting seperti permutasi polinomial.

Polinomial permutasi memiliki sejarah yang kaya sejak abad ke-19, dengan kontribusi signifikan dari Hermite dan Dickson (Varsha, Prasanna, & G. R. Vadiraja, 2022). Polinomial ini, dibangun dengan memodifikasi polinomial linier dan afin menggunakan berbagai alat matematika seperti karakter aditif dan fungsi Trace, memainkan peran penting dalam memahami perilaku struktural dan fungsional objek atau konsep (Mritunjay & Rajesh, 2022). Penelitian terbaru telah berfokus pada penentuan permutasi dalam berbagai kelas polinomial di atas bidang terbatas, dengan kemajuan dalam memahami sifat dan aplikasinya di berbagai bidang seperti kriptografi, teori pengkodean, dan geometri terbatas (Zhiguo & Michael E, 2023). Selain itu, pendekatan aljabar linier telah diusulkan untuk mempelajari polinomial permutasi yang timbul dari peta linier di atas bidang terbatas, menyediakan kondisi yang diperlukan dan memadai untuk sifat permutasi dan algoritma mereka untuk mengevaluasi invers komposisi mereka (Megha & Harish K, 2022).

Polinomial permutasi sangat penting karena aplikasinya yang luas di berbagai bidang seperti kriptografi, teori pengkodean, kombinatorik, dan rekayasa (Varsha, Prasanna, & G. R. Vadiraja, 2022; Mritunjay & Rajesh, 2022). Relevansi mereka berasal dari kemampuan mereka untuk mewakili fungsi yang merupakan permutasi bidang

terbatas, menjadikannya berharga dalam kriptologi dan teori pengkodean (Xiaogang, 2021). Studi tentang polinomial permutasi telah melihat kemajuan besar dalam beberapa dekade terakhir, dengan para peneliti mengusulkan masalah baru yang terkait dengan bilangan prima dan bidang terbatas, menyoroti pentingnya dan relevansi yang berkelanjutan dari bidang penelitian ini (G. R. Vadiraja, Shankar, Vishnu, & Prasanna, 2020)

Polinomial permutasi adalah salah satu cabang dari matematika yang mempelajari bentuk dan sifat-sifat permutasi polinomial. Polinomial permutasi memiliki peran penting dalam berbagai bidang ilmu dan digunakan dalam berbagai situasi. Salah satu yang dipelajari pada polinomial permutasi adalah tupel polinomial permutasi.

Tupel polinomial permutasi adalah konsep signifikan yang didefinisikan oleh subkelompok permutasi Sq, di mana Sq adalah kelompok permutasi dengan elemen q (Gutierrez & Urroz, 2022). Pentingnya tupel polinomial permutasi terletak pada peningkatan kemampuan permutasi di bidang terbatas. Dengan mengeksplorasi lebih lanjut dan memahami sifat-sifat polinomial permutasi tupel, peneliti dapat menemukan aplikasi yang lebih luas dan lebih dalam di berbagai bidang, membuka potensi untuk penemuan matematika lebih lanjut. Mempertimbangkan polinomial permutasi tupel memungkinkan mencapai permutasi dan pemetaan yang lebih kompleks di dalam lapangan. Tupel polinomial permutasi ini terletak pada mendefinisikan polinomial permutasi lokal bivariat, yang sangat penting untuk membangun Persegi latin. Hubungan antara polinomial permutasi tupel dan Persegi latin memungkinkan terciptanya Persegi latin Mutual Ortogonal (MOLS), sebuah konsep penting dalam kombinatorik (Gutierrez & Urroz, 2022). Memahami dan memanfaatkan polinomial permutasi tupel sangat penting dalam berbagai bidang seperti Teori Pengkodean, Kriptografi, dan Kombinatorik. Selain itu, juga dapat diaplikasikan untuk memecahkan masalah matematika dan mengembangkan algoritma kriptografi berdasarkan bidang terbatas.

Menjelajahi tupel polinomial permutasi membuka jalan bagi penelitian dan inovasi baru di bidang matematika, berkontribusi pada kemajuan pengetahuan dan aplikasi di bidang terkait. Sehingga pada penelitian ini akan dikembangkan dan dituangkan dalam bentuk penelitian yang berjudul, **“Beberapa Sifat Pasangan Polinomial Permutasi”**.

1.2 Rumusan Masalah

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

1. Bagaimana keterkaitan antara polinomial permutasi lokal dengan pasangan permutasi?
2. Bagaimana sifat pasangan polinomial permutasi?

1.3 Batasan Penelitian

Pada penelitian ini, penulis membatasi pada polinomial dua variabel atas lapangan hingga.

1.4 Tujuan Penelitian

Tujuan penelitian ini adalah menunjukkan keterkaitan antara polinomial permutasi lokal dengan pasangan permutasi dan sifat pasangan polinomial permutasi.

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 bahan referensi dalam kajian keilmuan matematika.
3. Bagi Universitas Hasanuddin:
   Sebagai pelengkap literatur mengenai matematika khususnya aljabar yang dapat dimanfaatkan 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 pasangan polinomial permutasi. Materinya berupa grup, gelanggang, lapangan, permutasi, polinomial, lapangan hingga, polinomial permutasi, tupel polinomial permutasi, polinomial permutasi lokal dan interpolasi Lagrange.

1.6.1 Grup

Pada himpunan semua bilangan bulat dikenal dua operasi penjumlahan dan perkalian. 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, peta dari $(s,t) \in S \times S$ harus di S; ini adalah sifat tertutup suatu operasi. Yang dimaksud dengan struktur aljabar atau sistem aljabar adalah himpunan S dengan satu atau lebih operasi pada S.

Dalam aritmatika dasar kita diberikan dua operasi, penjumlahan dan perkalian, yang memiliki sifat asosiatif sebagai salah satu sifat terpentingnya. Dari berbagai sistem aljabar yang memiliki sifat asosiatif, grup merupakan sistem 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 semua $e \in G$,
$$a * e = e * a = a$$
3. Untuk setiap $a \in G$, terdapat elemen invers, $a^{-1} \in G$ sehingga
$$a * a^{-1} = a^{-1} * a = e$$

Jika grup tersebut juga memenuhi,

4. Untuk semua $a, b \in G$
$$a * b = b * a,$$

maka grup tersebut dinamakan grup abel (atau grup komutatif)

(Lidl & Niederreiter, 1983)

Dalam grup G, elemen identitas e dan elemen a^{-1} bersifat tunggal, dan $(a * b)^{-1} = b^{-1} * a^{-1}$ untuk semua $a, b \in G$.

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. Jelas bahwa 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 sifatnya 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 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

Tabel 1 Operasi Biner

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

Contoh 1.6.1.3 Himpunan $\mathbb{Z}_n = \{0,1,2,3, \dots, n-1\}$ dengan operasi penjumlahan $(+)$ modulo n merupakan gelanggang dengan unsur identitas penjumlahannya adalah 0.

Definisi 1.6.1.2 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 & 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
$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ dan } (b + c) \cdot a = b \cdot a + c \cdot a$$

Definisi 1.6.2.1

1. Suatu gelanggang disebut gelanggang beridentitas jika gelanggang tersebut mempunyai identitas perkalian, yaitu jika terdapat unsur e sehingga $ae = ea = a$ untuk semua $a \in R$.
2. Suatu gelanggang disebut komutatif jika operasi $\cdot$ bersifat komutatif.

(Lidl & Niederreiter, 1983)

Contoh 1.6.2.1

1. Misalkan R adalah sembarang grup abelian dengan operasi grup $+$. Didefinisikan $\mathrm{ab} = 0$ untuk semua $\mathrm{a}, \mathrm{b} \in \mathrm{R}$; maka R adalah sebuah gelanggang.
2. Bilangan bulat genap 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 & 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 & 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 & 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, 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 $(a) = \{ra + na : r \in R, n \in \mathbb{Z}\}$. Jika R mengandung suatu identitas, maka $(a) = \{ra : r \in R\}$.

(Lidl & 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 $J = (a)$. Dalam hal ini, J disebut juga ideal utama yang dibangun oleh a.

(Lidl & 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 $a \equiv b \bmod J$, jika berada di kelas residu yang sama modulo J, atau setara, jika $a - b \in J$. Dapat diverifikasi bahwa $a \equiv n \bmod J$ menyiratkan $a + r \equiv b + r \bmod J$, $ar \equiv br \bmod J$, dan $ra \equiv rb \bmod J$ untuk setiap $r \in R$ dan $na \equiv nb \bmod J$ untuk setiap $n \in \mathbb{Z}$. Jika, sebagai tambahan, $r \equiv s \bmod J$, maka $a + r \equiv b + s \bmod J$ dan $ar \equiv bs \bmod J$.

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

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

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

Definisi 1.6.2.5 Gelanggang kelas residu dari gelanggang R modulo tersebut ideal J berdasarkan operasi di atas disebut gelanggang kelas residu (atau gelanggang faktor) dari R modulo J dan dilambangkan dengan R/J.

(Lidl & Niederreiter, 1983)

Contoh 1.6.2.3 (Gelanggang kelas residu $\mathbb{Z}/(n)$). Seperti dalam kasus grup, yang menyatakan koset atau kelas residu dari bilangan bulat a modulo bilangan bulat positif n

dengan $[a]$, serta dengan $a + (n)$, dimana (n) adalah cita-cita utama yang dihasilkan oleh n. Elemen $\mathbb{Z}/(n)$ adalah

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

(Lidl & Niederreiter, 1983)

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

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

Jadi homomorfisma $\varphi: R \to S$ 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 & Niederreiter, 1983)

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 1.6.3.1 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 & Astuti, 2007)

Dengan memperhatikan definisi gelanggang komutatif, dapat diperoleh kenyataan bahwa jika R lapangan, maka $R\backslash\{0\}$ membentuk grup abel terhadap operasi perkalian. Oleh karena itu, dapat 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. (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 $\mathbb{Z}$.

Teorema 1.6.3.1 Gelanggang $\mathbb{Z}/(p)$ dengan p bilangan prima p adalah sebuah lapangan.

(Muchlis & Astuti, 2007)

Contoh 1.6.3.1 Misalkan $\mathbb{F} = \mathbb{C}$ maka $\mathbb{F}$ adalah lapangan terhadap operasi penjumlahan dan operasi perkalian.

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 & 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 $|S| = n$, dapat 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 1.6.4.1 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 permutasi τ, dapat ditulis τ^{-1}, yang memenuhi $\tau \cdot \tau^{-1} = \tau^{-1} \cdot \tau = e$, dengan e adalah permutasi identitas. Sebagai contoh berikut:

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

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

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 terdefinisi dengan baik $a_0 + a_1a + \cdots + a_na^n$. 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

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

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 $0 \leq i \leq n$.

Diketahui polinomial di atas sehingga dapat didefinisikan operasi penjumlahan sebagai berikut,

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

Selanjutnya mendefinisikan operasi perkalian,

Misalkan,

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

maka diperoleh operasi perkalian 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 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 & 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 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 $n = deg\big(f(x)\big) = deg(f)$. Berdasarkan konvensi, dapat ditetapkan $deg(0) = -\infty$. 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 & Niederreiter, 1983)

Teorema 1.6.5.1 Misalkan R adalah sebuah 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 & Niederreiter, 1983)

Misalkan $\mathbb{F}$ menunjukkan suatu lapangan (tidak harus berhingga) Gelanggang $\mathbb{F}[x]$ memiliki sifat keterbagian. Misalkan polinomial $g \in \mathbb{F}[x]$ membagi polinomial $f \in \mathbb{F}[x]$ 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 $\mathbb{F}[x]$ 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 1.6.5.2 (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

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

(Lidl & Niederreiter, 1983)

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

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

$$\frac{-x^3 \quad -2x}{3x^2+2x+3}$$

$$\frac{-3x^2 \quad -1}{2x+2}$$

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

(Lidl & Niederreiter, 1983)

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

Definisi 1.6.5.3 Suatu polinomial $p \in \mathbb{F}[x]$ 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 & 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 $x^2 - 2 = \left(x + \sqrt{2}\right)(x - \sqrt{2})$ dapat direduksi pada lapangan bilangan real.

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

(Lidl & Niederreiter, 1983)

Hubungan penting antara akar dan pembagian diberikan oleh teorema berikut.

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

(Lidl & Niederreiter, 1983)

Definisi 1.6.5.5 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 & Niederreiter, 1983)

Teorema 1.6.5.4 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 & Niederreiter, 1983)

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

(Lidl & Niederreiter, 1983)

Contoh 1.6.5.2 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 adalalh $f_1(x) = x^3 + x + 1$ dan $f_2(x) = x^3 + x^2 + 1$.

(Lidl & 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 $(i, \dots, i_n)$ 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, misalnya, ekspresi $x_1 x_2 x_3 x_4$ dan $x_4 x_1 x_3 x_2$ diidentifikasi sama.

1.6.6 Lapangan Hingga

Definisi 1.6.6.1 (Polinomial Tak Tereduksi) Misalkan $\mathbb{F}$ adalah lapangan dan $F[X]$ adalah gelanggang polinomial dengan koefisien-koefisiennya di $\mathbb{F}$. Suatu polinomial $p(x) \in \mathbb{F}[X]$ 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 $\mathbb{F}[X]$. 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 1.6.6.1 $x^6 + x^5 + x^3 + x^2 + 1$ adalah salah satu polinomial di $\mathbb{Z}_2[X]$ yang tak tereduksi.

Teorema 1.6.6.1 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 1.6.6.2 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

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

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

$x^8=x^6+x^5+x^3+x^2+x=x+1,$

$x^9=x^2+x,$

$x^{10}=x^3+x^2,$

$\vdots$

$x^{61}=x^6+x^5+x^4+x^2+x=x^4+x^3+x+1,$

$x^{62}=x^5+x^4+x^2+x,$

$x^{63}=x^6+x^5+x^3+x^2,$

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 $\left(\left(\mathbb{Z}_2[X]/[x^6+x^5+x^3+x^2+1]\right)^{\times},\cdot\right)$ adalah grup siklik berorde 63 dengan x sebagai generator siklik sehingga $\left(\mathbb{Z}_2[X]/[x^6+x^5+x^3+x^2+1]\right)^{\times} \cong \mathbb{Z}_{63}$. Jadi, setiap elemen taknol 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 1.6.6.3 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.

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

$x^3=x^2+1,$

$x^4=x^3+x=x^2+x+1,$

$x^5 = x^3 + x^2 + 1 = x + 1$,

$x^6 = x^2 + x$, dan

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

Contoh 1.6.6.4 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.

Lapangan hingga adalah lapangan yang terdiri dari sejumlah elemen terbatas. Lapangan hingga juga dinotasikan dengan $\mathbb{F}_q$ dengan q adalah jumlah elemen dari $\mathbb{F}$.

1.6.7 Polinomial Permutasi

Definisi 1.6.7.1 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)

Dengan keterbatasan $\mathbb{F}_q$, dapat dinyatakan definisi ini dalam beberapa cara yang setara.

Lemma 1.6.7.1 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-satu;
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 1.6.7.1 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 $\mathbb{F}_{11}$, dan dapat diamati bahwa $f(x)$ mewakili 3 siklus $(0,1,2)$.

(Shallue, 2012)

Contoh 1.6.7.2 Pertimbangkan polinomialnya

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

Seperti pada contoh sebelumnya dapat diperiksa apakah g merupakan PP dari $\mathbb{F}_{11}$ dengan menghitung nilainya pada $\mathbb{F}_{11}$. Didapatkan

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

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

(Shallue, 2012)

Contoh 1.6.7.3 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

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

1.6.8 Tupel Polinomial Permutasi

Definisi 1.6.8.1 Misalkan $f \in R[x_1, \dots, x_n]$ diberikan oleh

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

(Lidl & Niederreiter, 1997)

Jika $a_{i_1 \dots i_n} \neq 0$, maka $a_{i_1 \dots i_n} x_1^{i_1} \dots x_n^{i_n}$ disebut suku dari f dan $i_1 + \dots + i_n$ adalah derajat dari suku tersebut. Untuk $f \neq 0$, dapat didefinisikan derajat dari f, dilambangkan dengan deg(f), sebagai maksimum dari derajat suku-suku f. Untuk $f = 0$, dapat

ditetapkan deg(f) = - ∞. Jika $f = 0$ atau jika semua suku-suku dari f memiliki derajat yang sama, maka f disebut homogen.

Definisi 1.6.8.2 Sebuah polinomial $f \in \mathbb{F}_q[x_1, \dots, x_n]$ disebut polinomial permutasi dalam n tak tentu pada $\mathbb{F}_q$ jika persamaan $f(x_1, \dots, x_n) = a$ memiliki q^{n-1} solusi pada $\mathbb{F}_q^n$ untuk setiap $a \in \mathbb{F}_q$.

(Lidl & Niederreiter, 1997)

Contoh 1.6.8.1 Diberikan polinomial dua variabel,

$$f(x_1, x_2) = x_1 + x_2 \in \mathbb{Z}_3[x_1, x_2]$$

akan diperiksa apakah f merupakan permutasi

x_2 \ x_1	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabel 2 Hasil Operasi $f(x_1, x_2) = x_1 + x_2 \in \mathbb{Z}_3[x_1, x_2]$

Berdasarkan tabel di atas dapat dilihat bahwa f adalah permutasi karena bersifat satu-satu pada.

Contoh 1.6.8.2 Diberikan polinomial dua variabel,

$$f(x_1, x_2) = x_1 \cdot x_2 \in \mathbb{Z}_3[x_1, x_2]$$

akan diperiksa apakah f merupakan permutasi

x_2 \ x_1	0	1	2
0	0	0	0
1	0	1	2

2	0	2	1

Tabel 3 Hasil Operasi $f(x_1, x_2) = x_1 \cdot x_2 \in \mathbb{Z}_3[x_1, x_2]$

Berdasarkan tabel di atas dapat dilihat bahwa f bukan merupakan permutasi.

Pada skripsi ini hanya akan membahas $\mathbb{F}_q[x_1,\ x_2]$.

1.6.9 Polinomal Permutasi Lokal

Definisi 1.6.9.1 Suatu persegi latin berordo 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, Hartke, & Kenney, 2004)

Definisi 1.6.9.2 Polinomial $f: F_s \times F_s \to F_s$ yang menghasilkan kuadrat Latin (suatu matriks L berukuran $s \times s$ dengan elemen-elemen a_{ij} adalah persegi latin jika dan hanya jika terdapat sebuah fungsi $f: S \times S \to S$ 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 $x, y, x \in S$ dan $x \neq z \Rightarrow f(z,y)$) disebut polinomial permutasi lokal (atau LPP).

(Diestelkamp, Hartke, & Kenney, 2004)

Contoh 1.6.9.1 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:

y \ x	0	1	2
0	1	2	0
1	2	0	1
2	0	1	2

Tabel 4 Hasil Operasi $f(x,y) = x + y + 1$

1.6.10 Interpolasi Lagrange

Misalkan himpunan titik-titik (x_i, y_j) dengan nilai-nilai $f(x_i, y_j)$ pada setiap titik. Polinomial interpolasi Lagrange dua peubah dapat dinyatakan sebagai:

$$P(x,y) = \sum_{i=1}^{n} \sum_{j=1}^{m} f(x_i, y_j) L_{ij}\,(x,y)$$

di mana $L_i(x)$ dan $L_j(y)$ adalah polinomial interpolasi Lagrange satu peubah yang didefinisikan sebagai:

$$L_i(x) = \prod_{\substack{1<k<n \\ k \neq i}}^{n} \frac{x - x_k}{x_i - x_k}$$

$$L_j(y) = \prod_{\substack{1<l<m \\ l \neq j}}^{m} \frac{y - y_l}{y_j - y_l}$$

Dengan demikian, polinomial $P(x,y)$ akan melalui semua titik (x_i, y_j) dengan nilai fungsi $f(x_i, y_j)$ yang sesuai.

(Yazici, Altas, & Ergenc, 2005)

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

Jenis 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 yang terkait sifat pasangan polinomial permutasi dengan tujuan menunjang dan memastikan penelitian yang dilakukan belum diteliti sebelumnya oleh orang lain.

2.2 Lokasi dan Waktu Penelitian

Penelitian ini dilakukan di Universitas Hasanuddin tepatnya di Laboratorium Analisis Departemen Matematika FMIPA Universitas Hasanuddin. Waktu penelitian berlangsung sejak September 2023.

2.3 Prosedur Penelitian

Penelitian ini dilaksanakan dengan langkah-langkah sebagai berikut:

1. Pengumpulan Jurnal dan Literatur Terkait Penelitian

   Studi literatur untuk mengetahui bahwa penelitian yang dilakukan belum pernah diteliti oleh orang/individu, kelompok, atau lembaga lainnya. 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 sifat pasangan polinomial permutasi 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

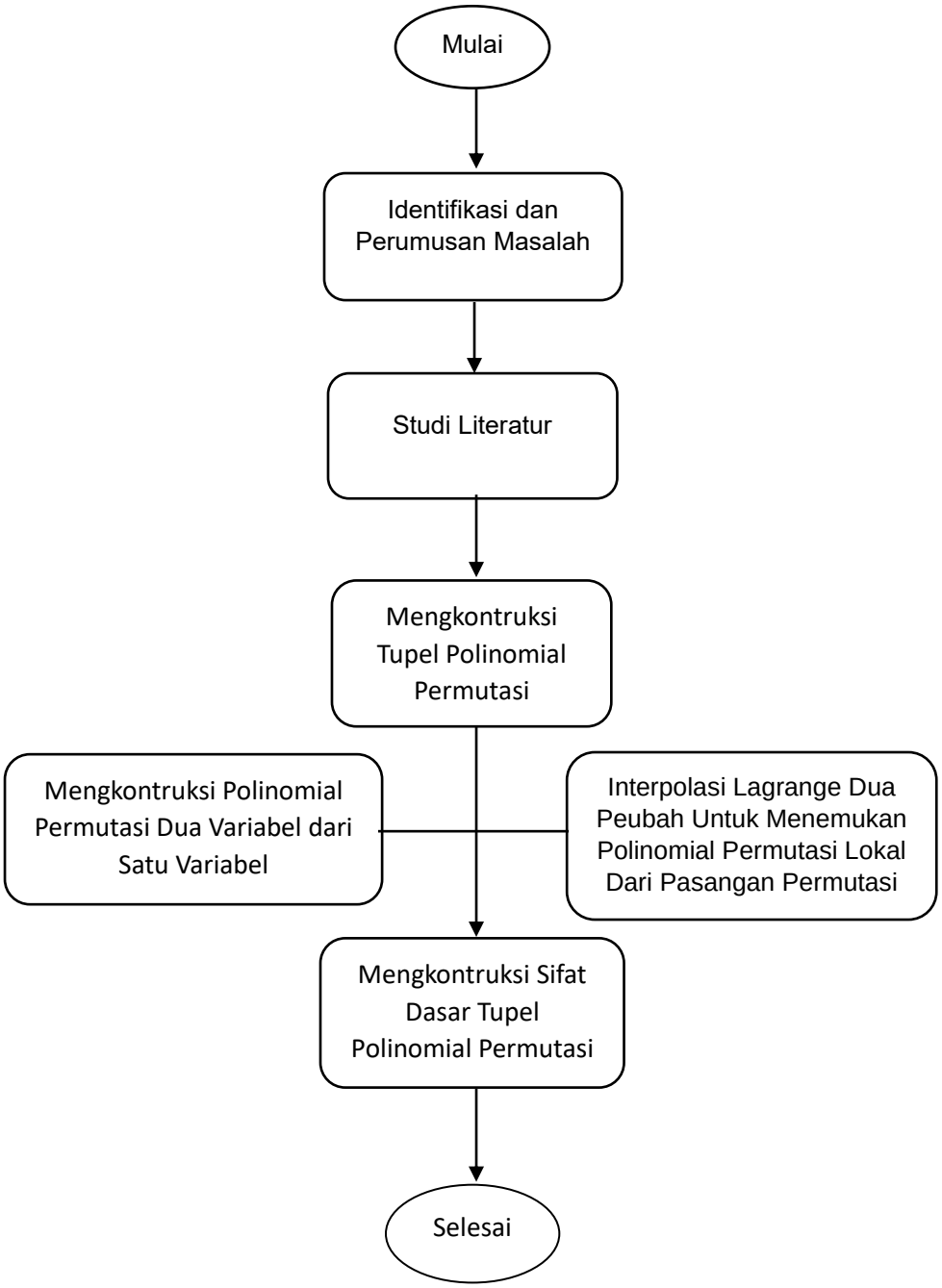
   Tahap akhir dilakukan verifikasi semua hasil yang telah dicapai dengan

menyajikan semua hasil pada tahap-tahap sebelumnya kedalam bentuk teorema dan lemma yang dilengkapi bukti-bukti secara matematis. Indikator keberhasilan dari penelitian ini adalah dapat menunjukkan beberapa sifat pasangan polinomial permutasi, yaitu keterkaitan antara polinomial permutasi lokal dengan pasangan permutasi dan sifat pasangan polinomial permutasi.

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:



Gambar 1 Diagram Alur