FORUM GURU BESAR
INSTITUT TEKNOLOGI BANDUNG

Orasi ilmiah Guru Besar Institut Teknologi Bandung

POSISI ALJABAR SEBAGAI PONDASI PENERAPAN ILMU PENGETAHUAN DAN TEKNOLOGI

Profesor Muchtadi Intan Detiena
Fakultas Matematika dan Ilmu Pengetahuan Alam
Institut Teknologi Bandung

Aula Barat ITB
16 September 2023

Orasi ilmiah Guru Besar
Institut Teknologi Bandung

POSISI ALJABAR SEBAGAI PONDASI PENERAPAN ILMU PENGETAHUAN DAN TEKNOLOGI

Orasi ilmiah Guru Besar
Institut Teknologi Bandung

POSISI ALJABAR SEBAGAI PONDASI PENERAPAN ILMU PENGETAHUAN DAN TEKNOLOGI

Prof. Muchtadi Intan Detiena

16 September 2023
Aula Barat ITB

FORUM GURU BESAR
INSTITUT TEKNOLOGI BANDUNG

ITB PRESS

Orasi ilmiah Guru Besar Institut Teknologi Bandung:
POSISI ALJABAR SEBAGAI PONDASI PENERAPAN ILMU PENGETAHUAN DAN TEKNOLOGI

Penulis : Prof. Muchtadi Intan Detiena
Reviewer : Prof. Edy Tri Baskoro
Editor Bahasa : Rina Lestari
Cetakan I : 2023
ISBN : 978-623-297-325-1

ITB PRESS
Gedung STP ITB, Lantai 1,
Jl. Ganesa No. 15F Bandung 40132
+62 22 20469057
www.itbpress.id
office@itbpress.id
Anggota Ikapi No. 043/JBA/92
APPTI No. 005.062.1.10.2018

PRAKATA

Segala puji syukur kami panjatkan ke hadirat Allah Swt., bahwasanya atas berkat rahmat dan karunia-Nya kami dapat menyelesaikan naskah orasi ilmiah dengan judul: **Posisi Aljabar sebagai Pondasi Penerapan Ilmu Pengetahuan dan Teknologi.**

Naskah orasi ilmiah ini berisi perjalanan kami dalam bersenang-senang dengan Representasi Aljabar, baik Aljabar untuk Matematika itu sendiri, maupun Aljabar sebagai dasar untuk bidang lain seperti Teknik Elektro, Informatika, Rekayasa Pertambangan, Hidrogeologi, dan bidang-bidang yang sedang populer saat ini seperti Kecerdasan Buatan (*Artificial Intelligence*) dan Sains Data.

Kami mengucapkan terima kasih sebesar-besarnya kepada pimpinan dan anggota Forum Guru Besar Institut Teknologi Bandung yang telah memberi kesempatan untuk menyampaikan orasi ilmiah dan menyebarluaskan hasil studi ini. Terima kasih sebesar-besarnya untuk Rektor Institut Teknologi Bandung beserta jajarannya, Dekanat Fakultas Matematika dan Ilmu Pengetahuan Institut Teknologi Bandung (FMIPA ITB), guru-guru kami sejak TK sampai Pasca-Doktor, para dosen di KK Aljabar serta di Komunitas Matematika ITB, para kolega peneliti di berbagai universitas di dalam dan luar negeri, mahasiswa S1, S2, dan S3 yang banyak membantu dan mendukung kami.

Terima kasih atas dukungan dan doa tulus orang tua, almarhum Ayahanda, dan juga Ibunda, dan juga kedua mertua, yang tidak putus-putusnya mendoakan kami. Terima kasih sebesar-besarnya bagi suami tercinta Dr. Andry Alamsyah, serta putri-putri kami Sandra Samara Alamsyah dan Marita Almira Sarah Alamsyah atas segala dukungan dan doa hingga pencapaian gelar tertinggi ini.

Semoga tulisan ini bermanfaat bagi peminat Aljabar, masyarakat penggunanya dan juga bagi pengembangan ilmu pengetahuan dan teknologi.

Bandung, 16 September 2023

Prof. Dr. Muchtadi Intan Detiena, S.Si., M.Si.

SINOPSIS

Tulisan ini menggambarkan perjalanan penulis dalam melakukan penelitian di bidang Aljabar selama 20 tahun terakhir. Tulisan ini didasari berbagai penelitian Aljabar yang dilakukan penulis bersama rekan-rekan dosen dan mahasiswa Kelompok Keahlian Aljabar FMIPA ITB, STEI ITB, FTTM ITB, FITB ITB, dan kolaborator dari universitas-universitas lain baik dalam negeri maupun luar negeri. Tulisan ini terbagi dalam empat bagian besar. Dimulai dengan Bab Pendahuluan yang membahas berbagai peranan Teori Representasi Aljabar dalam berbagai bidang. Kemudian dilanjutkan dengan bab kedua mengenai Teori Representasi Aljabar, yang membahas penelitian-penelitian Representasi Aljabar yang digunakan untuk mengklasifikasi aljabar; juga membahas visualisasi dari aljabar, modul dan struktur aljabar lainnya menggunakan kuiver dan graf. Selanjutnya bab ketiga membahas mengenai berbagai penggunaan representasi aljabar dalam bidang Kriptografi, Teori Koding, pemodelan menggunakan metode kuadrat terkecil 3D dan pemodelan dinamika robot, serta penggunaan wavelet. Pada bab keempat dibahas penggunaan representasi kuiver dalam ilmu-ilmu terkini seperti kecerdasan buatan (*artificial intelligence)* dan sains data (*data science*). Terakhir Bab Penutup menutup keseluruhan tulisan ini dengan menyimpulkan penggunaan representasi aljabar tidak hanya untuk bidang Aljabar sendiri, melainkan juga sebagai pondasi ilmu pengetahuan dan teknologi.

No discovery of mine has made, or is likely to make, directly or indirectly, for good or ill, the least difference to the amenity of the world. […] (but) I have added something to knowledge, and helped others to add more; and that these somethings have a value which differs in degree only, and not in kind, from that of the creations of the great mathematicians, or of any of the other artists, great or small, who have left some kind of memorial behind them.

from A Mathematician Apology by G. H. Hardy

DAFTAR ISI

PRAKATA ..... **v**

SINOPSIS ..... **vii**

DAFTAR ISI ..... **xi**

DAFTAR GAMBAR ..... **xiii**

DAFTAR TABEL ..... **xv**

1. PENDAHULUAN **1**

2. REPRESENTASI ALJABAR **3**

2.1 Teori Representasi Aljabar 3

2.2 Graf dari Struktur Aljabar 14

3. APLIKASI ALJABAR **19**

3.1 Kriptografi 19

3.2 Teori Koding 28

3.3 Aljabar Linier 32

3.4 Wavelet dan Transformasi Paket Gelombang (*Wave Packet Transform*) 37

4. APLIKASI REPRESENTASI KUIVER **38**

4.1 Kecerdasan Buatan (*Artificial Intelligence*) 38

4.2 Analisis Data Topologi *(Topological Data Analysis)* 40

5. PENUTUP **44**

6. UCAPAN TERIMA KASIH **45**

DAFTAR PUSTAKA **49**

CURRICULUM VITAE **59**

DAFTAR GAMBAR

Gambar 2.1 Bagan keterkaitan ekuivalensi Morita dan ekuivalensi bentukan. 4
Gambar 2.2 Lintasan non-trivial 5
Gambar 2.3 Diagram komutatif morfisma representasi. 6
Gambar 2.4 Kuiver Kronecker. 6
Gambar 2.5 Representasi M dan M' sebagai representasi dari kuiver Kronecker. 6
Gambar 2.6 Morfisma representasi M ke representasi M'. 6
Gambar 2.7 Kuiver siklus. 7
Gambar 2.8 Kuiver garis. 7
Gambar 2.9 Bagan grup ekuivalensi bentukan dan penggunaannya dalam teori representasi braid group. 10
Gambar 2.10 42-gon Π_{42} bersama tujuh m-diagonalnya. 11
Gambar 2.11 Kuiver garis tak hingga. 12
Gambar 2.12 Kuiver Auslander-Reiten untuk aljabar KQ dengan Q kuiver tipe An (Baur dkk., 2019) 13
Gambar 2.13 Resolusi projektif-U dari M = (i j) ditinjau di kuiver Auslander-Reiten (Baur dkk., 2019). 13
Gambar 2.14 Graf $\Gamma_{g,H,G}$, dengan G grup simetri S_3 , g = (1 2 3), dan H = {e, (1 2 3), (1 3, 2)} (Nasiri dkk., 2020). 15
Gambar 2.15 Graf Jacobson dari Z_6 , $\Im_{Z6}$ (Aditya dan Muchtadi-Alamsyah, 2021). 16
Gambar 2.16 Graf Jacobson dari Z_{25} , $\Im_{Z25}$ (Aditya dan Muchtadi-Alamsyah, 2021) 16
Gambar 2.17 Graf Jacobson matriks 2x2 dari Z_2 , $\Im_{Z2^{2x2}}$ (Humaira dkk., 2022). 17
Gambar 2.18 Graf Jacobson matriks $\Im_{M2(Z2)}$ (Humaira, 2023). 18
Gambar 3.1 Operasi penjumlahan titik-titik pada kurva eliptik. 19
Gambar 3.2 Gambaran perbandingan lapangan prima GF(299) dan lapangan komposit $GF(2^{13})^{23}$. 20
Gambar 3.3 Enkripsi dalam *Instant Messaging*. 26
Gambar 3.4 Kurva eliptik $y^2 = x^3 + 7$ yang digunakan dalam skema tanda tangan digital kurva eliptik (ECDSA), digambarkan untuk lapangan real. 27

Gambar 3.5 Diagram alir penelitian kode atas gelanggang. 31
Gambar 3.6 Model analisis perilaku berkelompok burung (Erfianto dan Muchtadi-Alamsyah, 2019). 33
Gambar 3.7 Hasil anisotropi elipsoida 3D dilihat dari (a) atas (b) depan, dan (c) samping (Muchtadi-Alamsyah dkk., 2022a). 36
Gambar 4.1 Contoh kuiver jaringan (Armenta dan Jodoin, 2021). 39
Gambar 4.2 Contoh representasi tipis dari suatu kuiver jaringan (Armenta dan Jodoin, 2021). 39
Gambar 4.3 (a) Kuiver jaringan *(network quiver)* Q (b) Jaringan syaraf (*neural network*) berbasis pada Q dengan bobot W dan fungsi aktivasi f (c) Jaringan syaraf yang sama tapi dengan perubahan basis pada setiap neuron (titik) (Armenta dkk., 2023). 40
Gambar 4.4 Contoh fitur penebalan dari X (Laha, 2019). 41
Gambar 4.5 Filtrasi sublevel dan konstruksi *persistent barcode* saat jari-jari bola meningkat (Chazal dan Michel, 2021). 42

DAFTAR TABEL

Tabel 3.1 Perbandingan antara Pollard Rho standar dengan Pollard Rho yang menggunakan Algoritma Brent *Cycle Detection* (Muchtadi-Alamsyah dan Utomo, 2017). 24

Tabel 3.2 Perbandingan antara Pollard Rho standar dengan Pollard Rho dengan Algoritma Brent *Cycle Detection* untuk kurva Koblitz tanpa pemetaan Frobenius (Muchtadi-Alamsyah dan Utomo, 2017)..... 24

Tabel 3.3 Perbandingan antara Pollard Rho standar dengan Pollard Rho dengan Algoritma Brent *Cycle Detection* untuk kurva Koblitz dengan pemetaan Frobenius (Muchtadi-Alamsyah dan Utomo, 2017) 24

Tabel 3.4 Perbandingan antara Pollard Rho dengan pemetaan Frobenius dan Pollard Rho tanpa pemetaan Frobenius untuk kurva Koblitz, keduanya menggunakan Algoritma Brent *Cycle Detention* (Muchtadi-Alamsyah dan Utomo, 2017). 25

Tabel 3.5 Perbandingan antara Pollard Rho dengan pemetaan Frobenius dan Pollard Rho tanpa pemetaan Frobenius untuk kurva Koblitz, keduanya tanpa Algoritma Brent *Cycle Detention* dan tanpa pemetaan negasi (Muchtadi-Alamsyah dan Utomo, 2017). 25

Tabel 3.6 Perbandingan antara Pollard Rho dengan pemetaan Frobenius dan Pollard Rho tanpa pemetaan Frobenius untuk kurva Koblitz, keduanya tanpa Algoritma Brent *Cycle Detention* tetapi menggunakan pemetaan negasi (Muchtadi-Alamsyah dan Utomo, 2017). 26

Tabel 3.7 Banyaknya kode θ- siklik *Euclidean self dual* atas F_8, dengan $\theta(y) = y^2$ (Irwansyah dkk., 2021)..... 30

Tabel 3.8 Kode-kode θ-siklik *self-dual* Euclid optimal atas gelanggang B_k dengan panjang n dan jarak d (Irwansyah, 2016). 30

1. PENDAHULUAN

Teori Representasi Aljabar adalah cabang matematika yang berfokus pada cara-cara menggambarkan struktur aljabar dan menyelidiki sifat-sifat yang terkait. Aljabar sendiri adalah bagian dari Matematika yang mempelajari struktur dan relasi antara objek matematika melalui simbol dan operasi. Representasi aljabar mencakup berbagai cara untuk menggambarkan objek matematika secara konkret maupun abstrak, dan menjadi pondasi bagi banyak aplikasi di dunia nyata.

Dalam ilmu pengetahuan dan teknologi, Teori Representasi Aljabar telah membawa dampak besar dalam beberapa bidang utama berikut.

1. Matematika dan Teori Komputasi: Teori Representasi Aljabar memiliki peran penting dalam pengembangan algoritma dan perangkat lunak; struktur aljabar seperti grup, gelanggang, dan lapangan, digunakan untuk memodelkan data dan operasi pada data tersebut. Representasi aljabar memungkinkan manipulasi simbol matematika secara otomatis, yang membantu penyelesaian masalah kompleks dalam matematika murni dan terapan.
2. Teori Graf: Dalam Teori Graf, representasi aljabar berperan dalam mewakili struktur data kompleks dalam bentuk matriks dan vektor. Representasi ini memungkinkan analisis lebih lanjut tentang sifat graf seperti hubungan antara titik dan sisi, lintasan terpendek, dan analisis jaringan kompleks.
3. Kriptografi: Dalam bidang Kriptografi, aljabar abstrak membantu mengembangkan algoritma kriptografi yang kuat dan aman, seperti algoritma enkripsi RSA dan kurva eliptik dalam kriptografi kurva eliptik. Penerapan teori representasi aljabar dalam kriptografi memungkinkan keamanan data dan pesan yang dikirimkan melalui jaringan.
4. Kimia: Teori Representasi Aljabar juga digunakan dalam Kimia untuk menggambarkan simetri molekul, mengidentifikasi sifat-sifat spektroskopi molekul dan meramalkan interaksi kimia.
5. Sains Data: Dalam sains data (*data science*), Teori Representasi Aljabar sangat penting untuk memodelkan data dalam bentuk matematika. Representasi aljabar memungkinkan analisis *big data* dan pemrosesan data yang efisien, termasuk penggunaan metode aljabar linier dan metode statistika.

6. Robotika dan Kecerdasan Buatan *(Artificial Intelligence)*: Dalam pengembangan robotika dan kecerdasan buatan, representasi aljabar membantu dalam memodelkan kinematika dan dinamika robot, serta perumusan dan analisis algoritma kecerdasan buatan seperti jaringan saraf tiruan (*neural network*).

Dengan terus berkembangnya teknologi, Teori Representasi Aljabar terus menjadi landasan penting dalam berbagai aspek ilmu pengetahuan dan teknologi. Penerapan representasi aljabar memungkinkan pengembangan solusi yang lebih canggih dan kompleks, serta membantu memahami dan menjelaskan fenomena alamiah secara lebih rinci dan akurat.

Sesuai dengan judul orasi ilmiah ini, akan dipaparkan posisi representasi aljabar yang digunakan untuk mengklasifikasi aljabar itu sendiri, yaitu dengan adanya klasifikasi berdasarkan kategori bentukan bersama invariansinya; dan juga menggunakan kuiver (graf berarah) sebagai visualisasi dari aljabar dan modul. Lalu dipaparkan beberapa graf dan sifat-sifatnya yang dibentuk dari struktur aljabar seperti grup dan gelanggang, yang dapat memperkaya Teori Graf. Kemudian dipaparkan mengenai penerapan aljabar dalam bidang Kriptografi, Teori Koding, pemodelan menggunakan metode kuadrat terkecil 3D dan pemodelan dinamika robot, serta penggunaan wavelet.

Seiring dengan berkembangnya ilmu pengetahuan dan teknologi di mana saat ini merupakan era kecerdasan buatan dan *big data*, dipaparkan juga penerapan representasi kuiver dalam jaringan syaraf tiruan (*artificial neural network*) dan analisis data topologi (*topological data analysis*) sebagai penelitian yang masih terus berlangsung.

2. REPRESENTASI ALJABAR

Untuk memahami berbagai struktur dalam Aljabar, struktur-struktur tersebut dikategorikan berdasarkan sifat-sifat yang serupa. Objek-objek dalam satu kategori memiliki sifat-sifat yang sama/ serupa. Dengan demikian tidak perlu semua objek dipelajari tetapi cukup representasinya saja.

Dalam Aljabar, objek yang dikaji adalah himpunan atau koleksi himpunan yang dilengkapi dengan suatu pemetaan yang mempertahankan struktur. Klasifikasi biasanya dilakukan berdasarkan isomorfisma. Jika terdapat isomorfisma antara dua objek, maka dua objek tersebut akan memiliki sifat-sifat yang sama. Dengan demikian pengkajian struktur-struktur aljabar tersebut dapat dilakukan melalui pengkajian kelas isomorfisma dari objek-objek. Pendekatan seperti ini sudah umum dilakukan dalam Teori Kategori.

2.1 Teori Representasi Aljabar

Teori Representasi adalah studi tentang realisasi konkret dari aljabar abstrak aksiomatik. Studi ini diawali dengan kajian mengenai grup permutasi dan aljabar matriks.

Teori Representasi Aljabar berdimensi hingga dimulai pada tahun 1970-an, ketika kuiver (graf berarah) menjadi populer dan metode-metode dari aljabar homologi memberikan konsep-konsep baru. Teori Representasi Aljabar berdasar kepada deskripsi Hamilton mengenai bilangan kompleks sebagai pasangan dua bilangan real. Pada tahun 1930-an, Emmy Noether memperkenalkan pendekatan modern pada teori ini dengan menginterpretasikan representasi sebagai modul (Van der Waerden, 1985). Hal ini memberikan suatu teknik dalam mempelajari aljabar semi sederhana, juga penggunaan Aljabar Homologi dan Teori Kategori dalam Teori Representasi. Dengan penggunaan tersebut, Teori Representasi menjadi teori yang berkembang pesat selama 40 tahun terakhir.

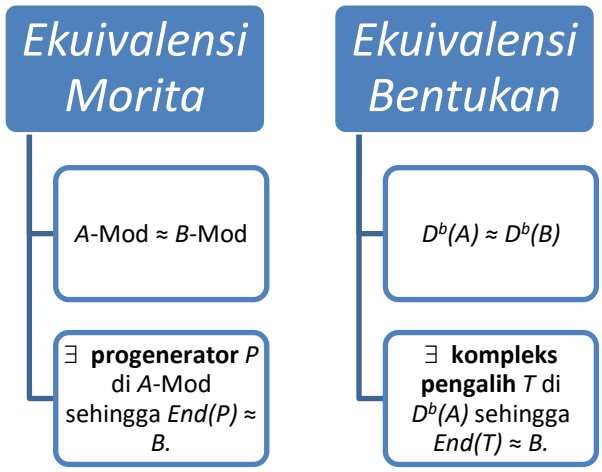
Dalam Teori Representasi, kategori modul dari suatu aljabar, dan klasifikasi aljabar diklasifikasi berdasarkan ekuivalensi kategori modul yang merupakan keserupaan yang lebih lemah daripada isomorfisma. Pada awal tahun 1960-an Grothendieck dan Verdier (Deligne, 1977; Verdier, 1996) memperkenalkan kategori bentukan (*derived category*) dan lebih umum

kategori tersegitigakan (*triangulated category*) sebagai suatu alat dalam Geometri Aljabar untuk memformulasikan dan membuktikan perluasan Teorema Dualitas Serre. Lebih dari dua puluh tahun kemudian, kategori bentukan digunakan dalam Teori Representasi. Awal penggunaannya adalah interpretasi Happel untuk Teori Pengalih (*Tilting Theory*) (Happel, 1988) yang merupakan generalisasi ekuivalensi Morita dalam bentuk ekuivalensi bentukan.

Sejak tahun 1990-an, keserupaan lain yang menggunakan kategori bentukan dianggap lebih cocok untuk klasifikasi aljabar, dan ekuivalensi Morita dipandang terlalu kuat. Pada tahun 1989, Rickard dan Keller (Rickard, 1991; Keller, 1993) memberikan syarat perlu dan cukup untuk keberadaan ekuivalensi bentukan antara dua gelanggang, sebagai perumuman dari ekuivalensi Morita.

Teorema 2.1 (Rickard, 1991; Keller, 1993) Diberikan dua gelanggang A dan B, kategori bentukan $D^b(A)$ dan $D^b(B)$ dari A dan B, ekuivalen sebagai kategori tersegitigakan jika dan hanya jika terdapat sebuah objek T di $D^b(A)$, dinamakan kompleks pengalih (*tilting complex*), yang memenuhi sifat similar dengan progenerator, sedemikian sehingga B isomorfik dengan gelanggang endomorfisma dari T di $D^b(A)$.

Bagan keterkaitan ekuivalensi Morita dan ekuivalensi bentukan dapat dilihat pada Gambar 2.1.



Gambar 2.1 Bagan keterkaitan ekuivalensi Morita dan ekuivalensi bentukan.

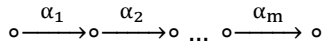
Dalam (Muchtadi-Alamsyah, 2005) telah dihasilkan metode untuk menentukan gelanggang endomorfisma dari kompleks pengalih atas suatu aljabar A, sehingga dapat ditentukan aljabar B yang ekuivalen bentukan dengan aljabar A tersebut. Metode penentuan gelanggang endomorfisma dari kompleks pengalih telah dimanfaatkan dalam (Abe, 2017) untuk menjawab pertanyaan apakah suatu pasangan modul *tilting* dan *cotilting* dapat menentukan kompleks pengalih.

2.1.1 Kuiver (Graf Berarah)

Ide untuk merepresentasikan objek matematika yang abstrak menjadi objek yang lebih sederhana sangatlah berguna, misalnya dalam pengklasifikasian. Suatu aljabar dapat direpresentasikan dalam bentuk kuiver (graf berarah) dan sebaliknya suatu aljabar lintasan (*path algebra*) dapat diperoleh dari graf berarah (Assem dkk., 2006).

Keuntungan pengkajian aljabar lintasan adalah kemudahan untuk memvisualisasi, yang sangat berguna untuk kajian representasi aljabar, karena sifat-sifat aljabar lintasan, seperti dimensi dan kesederhanaan, dapat ”dibaca” melalui sifat-sifat grafnya.

Suatu kuiver $Q= (Q_0, Q_1, s, t: Q_1 \rightarrow Q_0)$ diberikan oleh himpunan titik Q_0 , misalnya $\{1, 2, \ldots, n\}$, dan himpunan busur Q_1. Suatu busur α bermula di titik $s(\alpha)$ dan berujung di $t(\alpha)$. Suatu lintasan non-trivial di Q adalah barisan busur-busur $\alpha_1 \ldots \alpha_m$ $(m \geq 1)$ yang memenuhi $s(\alpha_i) = t(\alpha_{i+1})$ untuk $1 \leq i \leq m$ (lihat Gambar 2.2).



Gambar 2.2 Lintasan non-trivial

Lintasan ini berawal di $s(\alpha_1)$ dan berujung di $t(\alpha_m)$. Untuk setiap titik i, lintasan trivial yang bermula dan berujung di i dinotasikan dengan e_i .

2.1.2 Aljabar Lintasan

Misalkan K suatu lapangan yang tertutup secara aljabar (misalkan saja lapangan bilangan kompleks). Aljabar lintasan KQ adalah aljabar atas K, dengan basis lintasan-lintasan di Q, dan perkalian antara dua lintasan x dan

y, xy, diberikan oleh komposisi lintasan x dan y jika t(y) = s(x), dan 0 jika lainnya. Perkalian ini bersifat asosiatif.

Misalkan Q suatu kuiver. Suatu representasi M = (M_a,φ_α) dari Q diberikan oleh K-ruang vektor M_a untuk setiap titik a di Q_0 dan pemetaan linier φ_α: $M_a \rightarrow M_b$ untuk setiap busur α: a $\rightarrow$ b di Q_1.

Misalkan M dan M' dua representasi dari Q. Suatu morfisma f: M$\rightarrow$ M' adalah barisan f = (f_a) sedemikian sehingga diagram pada Gambar 2.3 komutatif:

$$\begin{array}{ccc} M_a & \stackrel{\varphi_\alpha}{\rightarrow} & M_b \\ \downarrow f_a & & \downarrow f_b \\ M'_a & \stackrel{\varphi'_\alpha}{\rightarrow} & M'_b \end{array}$$

Gambar 2.3 Diagram komutatif morfisma representasi.

Sebagai contoh, kuiver Kronecker pada Gambar 2.4 memiliki representasi M dan M' yang diberikan pada Gambar 2.5, dan morfisma representasinya diberikan pada Gambar 2.6.

$$1 \underset{\beta}{\overset{\alpha}{\leftarrow\!\leftarrow}} 2.$$

Gambar 2.4 Kuiver Kronecker.

$$M = \left(K^2 \underset{\leftarrow}{\overset{\begin{pmatrix}1\\0\end{pmatrix}}{\leftarrow}} K \right), \qquad M' = \left(K^2 \underset{\leftarrow}{\overset{\begin{pmatrix}1&0\\0&1\end{pmatrix}}{\leftarrow}} K^2 \right).$$

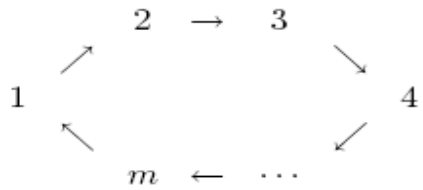
Gambar 2.5 Representasi M dan M' sebagai representasi dari kuiver Kronecker.

$$\begin{array}{ccc} K^2 & \overset{\begin{pmatrix}1\\0\end{pmatrix}}{\underset{\begin{pmatrix}0\\1\end{pmatrix}}{\leftarrow}} & K \\ \begin{pmatrix}1&0\\0&1\end{pmatrix} \downarrow & & \downarrow \begin{pmatrix}1\\0\end{pmatrix}. \\ K^2 & \overset{\begin{pmatrix}1&0\\0&1\end{pmatrix}}{\underset{\begin{pmatrix}0&0\\1&0\end{pmatrix}}{\leftarrow}} & K^2 \quad . \end{array}$$

Gambar 2.6 Morfisma representasi M ke representasi M'.

Kategori representasi kuiver $\mathrm{Rep}_K(Q)$ didefinisikan dengan objeknya adalah representasi kuiver, dan morfismanya adalah morfisma representasi kuiver. Kategori $\mathrm{Rep}_K(Q)$ ekuivalen dengan kategori modul atas KQ, sehingga $\mathrm{Rep}_K(Q)$ memberikan representasi (visual) dari kategori modul atas KQ.

Aljabar Nakayama *self-injective* N_{nm} adalah aljabar lintasan atas lapangan K dari kuiver siklus pada Gambar 2.7, modulo ideal yang dibangun oleh komposisi n+1 busur-busur berurutan. Sebagai contoh, aljabar N_{23} memiliki basis lintasan-lintasan (1), (2), (3), (12), (13), (23), (21), (31), (32), dengan (i j) melambangkan lintasan yang dimulai di i dan berakhir di titik j dan (i) melambangkan lintasan trivial.



Gambar 2.7 Kuiver siklus.

Aljabar Nakayama tipe A_n adalah aljabar lintasan dari kuiver garis pada Gambar 2.8.

$$1 \xrightarrow{\alpha_1} 2 \xrightarrow{\alpha_2} \circ \ \ldots \ \circ \xrightarrow{\alpha_{n-1}} n$$

Gambar 2.8 Kuiver garis.

Muchtadi-Alamsyah (2008) menggunakan dua aljabar eksplisit dan memberikan kompleks pengalih eksplisit yang memberikan ekuivalensi antara dua aljabar tersebut. Aljabar pertama adalah aljabar Nakayama simetri N_{nn} yang didefinisikan oleh kuiver, dan aljabar kedua adalah aljabar pohon Brauer (*Brauer tree algebra*) yang berkaitan dengan garis tanpa titik eksepsional.

Teorema 2.2 Misalkan B aljabar Nakayama N_{nn} atas K and A aljabar pohon Brauer yang berkaitan dengan garis tanpa titik eksepsional. Jika T adalah jumlah langsung rantai A-modul projektif

$$T_i: 0 \to P_n \to P_{n-1} \to \cdots \to P_{i+1} \to P_i \to 0, \ i = 1,2,\ldots,n, \qquad (2.1)$$

maka $End_{Db(A)}(T) \approx B$. Dengan demikian terdapat ekuivalensi bentukan antara aljabar Nakayama N_{nn} dan aljabar pohon Brauer yang berkaitan dengan garis tanpa titik eksepsional.

Bukti: Berdasarkan (Koenig dan Zimmermann, 1998), order Green yang berkaitan dengan aljabar A adalah R-order Λ berikut:

$$R\begin{pmatrix} R & R \\ \pi & R \end{pmatrix}\begin{pmatrix} R & R \\ \pi & R \end{pmatrix} \cdots \begin{pmatrix} R & R \\ \pi & R \end{pmatrix}\begin{pmatrix} R & R \\ \pi & R \end{pmatrix}\begin{pmatrix} R & R \\ \pi & R \end{pmatrix}R \tag{2.2}$$

dengan R adalah himpunan bilangan n+1-adic $\mathbf{Z}_{n+1}$, dan π = Rad(R) = < n+1 >. Lebih tepatnya,

$$\Lambda = \left\{ \begin{array}{l} \left(d_0, \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}, \cdots, \begin{pmatrix} a_{n-1} & b_{n-1} \\ c_{n-1} & d_{n-1} \end{pmatrix}, a_n \right), \\ a_i, b_i, c_i, d_i \in R, n+1 \mid (d_i - a_{i+1}), n+1 \mid c_i \end{array} \right\} \tag{2.3}$$

Definisikan kompleks T adalah sebagai jumlah langsung $T_1 \oplus T_2 \oplus \ldots \oplus T_n$ dengan $T_1, T_2, \ldots, T_n$ sebagai berikut:

$$\begin{array}{lllllllllllll} T_1 & : & 0 & \to & P_n & \to & P_{n-1} & \to & \cdots & \to & P_2 & \to & P_1 & \to & 0 \\ \oplus & & & & \oplus & & \oplus & & \oplus & & \oplus & & \oplus & & \\ T_2 & : & 0 & \to & P_n & \to & P_{n-1} & \to & \cdots & \to & P_2 & \to & 0 & & \\ \oplus & & & & \oplus & & & & & & & & & & \\ \vdots & & & & \vdots & & & & \iddots & & & & & & \\ \oplus & & & & \oplus & & & & & & & & & & \\ T_n & : & 0 & \to & P_n & \to & 0 & & & & & & & & \end{array} \tag{2.4}$$

Berdasarkan Lema 5.12 dalam (Koenig dan Zimmermann, 1998), T adalah kompleks pengalih. Homologi ke-n dari Ti adalah sama untuk setiap i, dan homologi di tengah adalah 0 untuk setiap $1 \le i \le n-2$.

Gelanggang endomorfisma dari T, $End_{Db(A)}(T)$ adalah

$$\begin{pmatrix} Hom(T_1,T_1) & Hom(T_1,T_2) & \cdots & Hom(T_1,T_n) \\ Hom(T_2,T_1) & Hom(T_2,T_2) & \cdots & Hom(T_2,T_n) \\ \vdots & & & \\ Hom(T_n,T_1) & Hom(T_n,T_2) & & Hom(T_n,T_n) \end{pmatrix} \tag{2.5}$$

dengan semua homomorfisma merupakan homomorfisma dalam kategori bentukan.

Berdasarkan Teorema 2.1 dalam (Muchtadi-Alamsyah, 2005),

$$\mathrm{Hom}(T_i,T_j)=\begin{cases}\mathrm{Hom}(H_nT_1,H_nT_1)\cong R & \text{jika } i<j\\ \mathrm{Hom}(P_n,H_nT_1)\cong \pi & \text{jika } i>j\\ \text{pullback dari } (H_nT_1,H_nT_1) \text{ dan } (H_iT_i,H_iT_i) & \text{jika } i=j\end{cases} \tag{2.6}$$

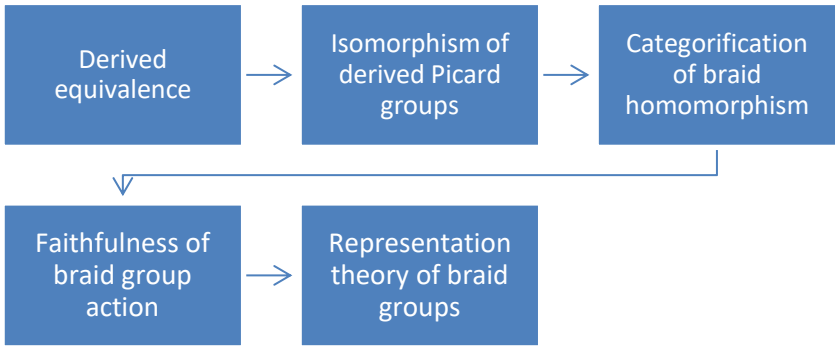
dengan R-R = $\{(a,b)\in R\times R: a-b\in\pi\}$. Sehingga $\mathrm{End}_{\mathrm{Db}(A)}(T)$ adalah

$$\begin{array}{cc} R & \\ R & \begin{pmatrix} R & R & \cdots & R \\ \pi & R & \cdots & R \\ \pi & \pi & \ddots & R \\ \pi & \pi & & R \end{pmatrix} \\ & R \end{array} \tag{2.7}$$

dan ini merupakan order Green yang berkaitan dengan aljabar Nakayama B. QED.

Dalam (Muchtadi-Alamsyah, 2008) telah dikaji grup ekuivalensi bentukan dari aljabar Nakayama *self-injective* N_{nn}, yaitu grup yang berisikan semua pemetaan yang menyebabkan ekuivalensi bentukan pada aljabar N_{nn}, dan diperoleh bahwa dalam grup tersebut terdapat subgrup yang menyerupai *braid group*. Grup ekuivalensi bentukan ini telah dikembangkan lebih lanjut dalam (Zvonareva, 2015; Zvonareva, 2015a; Volkov dan Zvonareva, 2017), dan ternyata berkaitan dengan konsep mutasi *silting complex* (Eisele, 2022).

Berdasarkan Akibat 4.10 dalam (Muchtadi-Alamsyah, 2008), terdapat representasi dari *braid group* Artin dan representasi dari *braid group* $B(K_n)$ dan juga kategorifikasi dari homomorfisma *braid group*. Lebih lanjut, dengan hasil ini diperoleh bahwa aksi *braid group* afin pada kategori bentukan dari aljabar bintang Brauer tanpa titik eksepsional dalam (Schaps dan Zakay-Illouz, 2002) merupakan aksi yang *faithful* (Teorema 5.2 dalam (Muchtadi-Alamsyah, 2008)) Pada Gambar 2.9 diberikan bagan grup ekuivalensi bentukan dan penggunaannya dalam representasi grup.



Gambar 2.9 Bagan grup ekuivalensi bentukan dan penggunaannya dalam teori representasi *braid group*.

Selanjutnya, dengan menggunakan kuiver sebagai alat untuk visualisasinya, Santika dan Muchtadi-Alamsyah (2012) menyelidiki sifat invariansi dari ekuivalensi bentukan untuk suatu subruang p-regular, dan dalam (Darmajid dan Muchtadi-Alamsyah, 2012; Darmajid dan Muchtadi-Alamsyah, 2013) telah diperoleh sifat-sifat geometri dari kategori bentukan.

Lebih lanjut dalam (Faisal dan Muchtadi-Alamsyah, 2013; Faisal dan Muchtadi-Alamsyah, 2016) telah diperoleh karakterisasi aljabar Nakayama *self-injective* dan tipe A_n berdasarkan kategori orbit dari kategori bentukan, sebagai berikut:

Misalkan $\Pi_{m(n+1)+2}$ adalah m(n+1)+2-gon regular, m,n di N, dengan titik ujungnya dinomori searah jarum jam dari 1 sampai m(n+1)+2. Suatu diagonal D di $\Pi_{m(n+1)+2}$, dilambangkan sebagai pasangan (i,j). Jelas bahwa diagonal (i,j) sama dengan diagonal (j,i). Diagonal D dari $\Pi_{m(n+1)+2}$ disebut m-diagonal jika D membagi $\Pi_{m(n+1)+2}$ menjadi dua bagian (mj+2)-gon dan (m(n-j)+2)-gon dengan $j = 1,2,\ldots\left\lfloor\frac{n}{2}\right\rfloor$.

Proposisi 2.3 (Faisal dan Muchtadi-Alamsyah, 2016) Misalkan C_{An}^{m} adalah kategori orbit $D^b(KA_n)/F_m$ dengan $F_m = \tau^{-1}[m]$ dengan τ adalah AR-translasi, dan $m \geq n-2$. Misalkan $D_1 = (1,m+2)$, $D_2 = (1, nm+2)$ dan untuk $i = 3,\ldots,n$,

$$D_i = ((n-(i-2))m-(i-4),(n-(i-3))m-(i-5)), \tag{2.8}$$

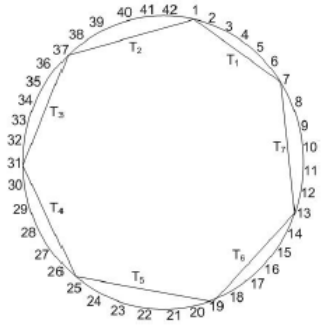
maka

1) $D_1, D_2, \ldots, D_n$ adalah m-diagonal di $\Pi_{m(n+1)+2}$
2) $D= D_1 \oplus D_2 \oplus \ldots \oplus D_n$ adalah objek pengalih m-*cluster*

3) *m-cluster tilted algebra* End(T) isomorfik aljabar Nakayama KQ/I dengan Q berbentuk
   a) kuiver siklik dengan n titik jika m = n-2
   b) kuiver garis jika m > n-2

dan I adalah ideal yang dibangun oleh lintasan dengan panjang dua.

Sebagai contoh: misalkan m = 5 dan n = 7 maka m(n+1)+2 = 5(7+1)+2 = 42. Pandang 42-gon Π_{42}, dan misalkan D_1 = (1, 7), D_2 = (1,37), D_3 = (31, 37), D_4 = (25, 31), D_5 = (25,19), D_6 = (13,19) dan D_7 = (7,13) then D= $D_1 \oplus D_2 \oplus \ldots \oplus D_5$ merupakan objek pengalih 5-*cluster* tilting object. Gambar Π_{42} bersama tujuh m-diagonalnya diberikan dalam Gambar 2.10.



Gambar 2.10 42-gon Π_{42} bersama tujuh m-diagonalnya

2.1.3 Aljabar Lintasan Leavitt

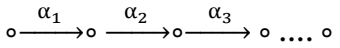
Penelitian 15 tahun terakhir dalam bidang teori representasi adalah kajian mengenai Aljabar Lintasan Leavitt yang merupakan ”versi Aljabar” dari Cuntz-Krieger graph C*-algebra, suatu kelas aljabar yang secara intensif dipelajari di bidang analisis selama lebih dari dua dekade. Untuk aljabar lintasan Leavitt, beberapa sifat telah dikaji melalui sifat grafnya seperti sifat sederhana (*Simplicity Theorem)* (Abrams dan Pino, 2005), sifat-sifat terkait modul untuk aljabar lintasan Leavitt (Ara dkk., 2007), ideal dari aljabar lintasan Leavitt (Abrams, 2015), ideal prima dan semiprima mendasar (Wardati dkk., 2014).

Di lain pihak kajian submodul prima telah dilakukan dalam (Wardhana dkk., 2016; Saleh dkk., 2016), sehingga memotivasi untuk kajian modul prima atas aljabar lintasan dan aljabar lintasan Leavitt. Dalam (Muchtadi dkk., 2018) telah dikaji karakterisasi dan visualisasi modul tak terdekomposisi atas aljabar

lintasan tipe A_n, D_n, E_6, E_7, E_8, yang selanjutnya digunakan untuk mengklasifikasi modul prima dan modul herediter atas aljabar lintasan dan aljabar lintasan Leavitt (Risnawita dkk., 2021; Kariman dkk., 2019). Beberapa hasilnya adalah sebagai berikut:

Teorema 2.4 (Risnawita dkk., 2021) Jika K lapangan dan A aljabar atas K berdimensi hingga, maka setiap A-modul prima berbentuk S^n untuk suatu bilangan asli n dan suatu A-modul sederhana S.

Teorema 2.5 (Risnawita dkk., 2021) Jika Q suatu kuiver yang bukan berupa titik saja atau loop saja, maka terdapat modul sederhana atas aljabar lintasan Leavitt yang *completely prime* jika dan hanya jika Q adalah kuiver garis tak hingga dalam Gambar 2.11.



Gambar 2.11 Kuiver garis tak hingga.

Teorema 2.6 (Kariman dkk., 2019) Semua modul projektif atas aljabar lintasan Leavitt dari kuiver garis tak hingga adalah herediter.

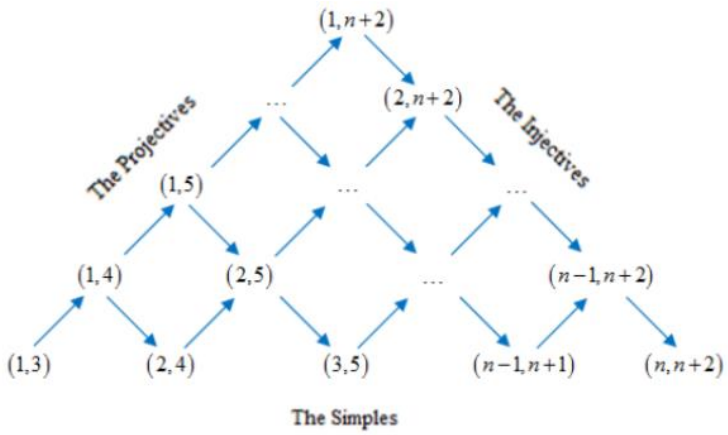
Dari hasil-hasil ini dapat disimpulkan bahwa pengklasifikasian modul dapat dilakukan dengan mengidentifikasi bentuk kuivernya.

2.1.4 Rantai Kompleks

Rantai kompleks merupakan objek dalam kategori kompleks, kategori homotopi dan kategori bentukan. Pada tahun 2002, Davvaz dan Shabani-Solt memperkenalkan pengertian kompleks-U dan homologi-U untuk memperumum konsep-konsep tertentu dalam aljabar homologi (Davvaz dan Shabani-Solt, 2022). Terinspirasi oleh hal ini, Mahatma dan Muchtadi-Alamsyah (2017) memperkenalkan gagasan resolusi projektif-U dan ekstensi-U. Ditemukan juga bahwa barisan eksak pendek modul atas aljabar herediter selalu dapat diperluas menjadi barisan eksak panjang homologi-U yang terdiri dari modul ekstensi-U.

Penelitian lebih lanjut adalah kajian resolusi projektif-U dari aljabar lintasan dari kuiver tipe A_n (Baur dkk., 2019) dan representasi geometrisnya

berdasarkan (Baur dan Torkildsen, 2020). Pada Gambar 2.12 diberikan kuiver Auslander-Reiten dari kuiver tipe A_n dengan modul-modulnya dituliskan sebagai pasangan (i,j).

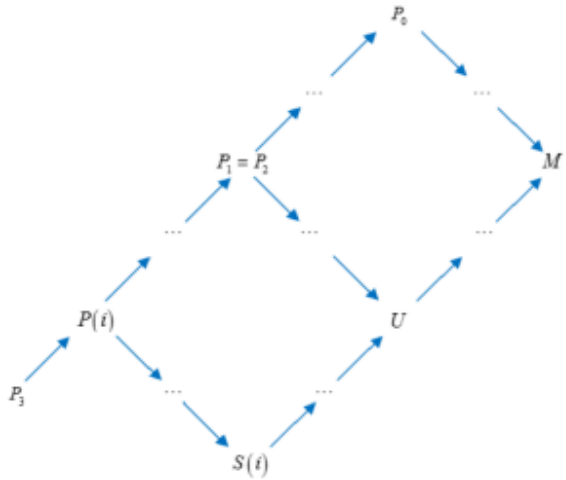


Gambar 2.12 Kuiver Auslander-Reiten untuk aljabar KQ dengan Q kuiver tipe An (Baur dkk., 2019)

Teorema 2.7 (Baur dkk., 2019) Resolusi projektif-(i,m) dari modul (i,j) diberikan oleh barisan berikut:

$$0 \to (1,i+1) \to (1,m) \to \begin{matrix}(1,m)\\ \uparrow \\ (1,i+1)\end{matrix} \to \begin{matrix}(1,j)\\ \uparrow \\ (1,m)\end{matrix} \to \begin{matrix}(i,j)\\ \uparrow \\ (i,m)\end{matrix} \to 0 \tag{2.8}$$

Ditinjau di kuiver Auslander-Reiten, resolusi projektif-U dari M=(i j) dapat dilihat pada Gambar 2.13.



Gambar 2.13 Resolusi projektif-U dari M = (i j) ditinjau di kuiver Auslander-Reiten (Baur dkk., 2019).

Teorema 2.7 digunakan dalam (Kariman dkk., 2021) untuk mengkonstruksi resolusi projektif-U dari modul sederhana atas aljabar lintasan Leavitt. Dengan memvisualisasikan sebagai kuiver, pengkajian modul dan resolusi projektif menjadi lebih mudah.

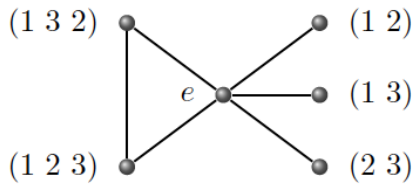
Terkait kategori kompleks-U, Elviyanti dkk. (2016) membuktikan sifat abelian dari kategori kompleks-U dan kemudian Elviyanti dkk. (2020) memperlemahnya menjadi kategori kompleks-U lemah, supaya dapat dilanjutkan untuk membentuk kategori bentukan. Kemudian Hafezi dan Muchtadi-Alamsyah (2021) menggunakan pendekatan lain dengan mengkaji struktur eksak untuk kategori monomorfisme.

Melanjutkan kajian mengenai kompleks pengalih, Muchtadi-Alamsyah dan Palu (2021) mengkaji mengenai keterkaitan antara modul τ_n-*tilting* dan *silting complex* dengan panjang n. Modul τ_n-*tilting* dan *silting complex* masing-masing merupakan perumuman dari modul pengalih dan kompleks pengalih.

2.2 Graf dari Struktur Aljabar

Penentuan sifat grup hingga melalui graf menjadi topik yang menarik dalam beberapa tahun terakhir ini. Terdapat banyak cara mengaitkan graf dengan grup hingga, seperti misalnya, graf Engel dan graf *noncommuting* (Abdollahi, 2007; Abdollahi dkk., 2006; Abdollahi dan Mohammadi Hassanabadi 2007). Paul Erdos adalah yang pertama kali mengkaji graf *noncommuting,* dan untuk keterkaitan antara graf dan grup, Abdollahi dkk. (2006) mengkaji bagaimana sifat teoritis graf Γ_G memengaruhi sifat teoritis grup G.

Perumuman dari graf *noncommuting* telah dipelajari dalam (Barati, 2014; Nasiri dkk., 2016; Nasiri dkk., 2017; Tolue dan Erfanian 2013; Tolue dkk., 2014). Dalam (Nasiri dkk., 2020) dikaji mengenai graf g-*noncommuting* relatif $\Gamma_{g,H,G}$ yang berkaitan dengan suatu elemen g di grup G dan suatu subgrup H dari G. Himpunan titik-titiknya adalah G, dan dua titik x dan y bertetangga jika komutator [x,y] tidak sama dengan g dan g^{-1}, dengan x atau y berada di H. Pada Gambar 2.14 diberikan contoh graf $\Gamma_{g,H,G}$, dengan G grup simetri S_3, dan H = {e,(1 2, 3), (1 3 2)}.



Gambar 2.14 Graf $\Gamma_{g,H,G}$, dengan G grup simetri S_3 , g = (1 2 3), dan H = {e, (1 2 3), (1 3, 2)} (Nasiri dkk., 2020).

Misalkan Γ adalah suatu graf. Derajat dari suatu titik v di Γ, deg(v) adalah banyaknya sisi dari Γ yang berinsiden dengan v. Jika S suatu himpunan hingga, notasikan |S| sebagai jumlah elemen dalam himpunan S. Lema berikut memberikan derajat dari titik-titik di graf $\Gamma_{g,H,G.}$

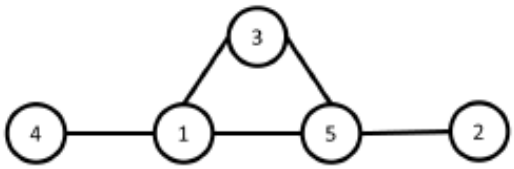
Lema 2.8 (Nasiri dkk., 2020) Misalkan G suatu grup dan H subgrup dari G.

1) Misalkan x di G-H, dan $C_H(x) = \{y \in H: xy = yx\}$. Pandang x sebagai titik di graf $\Gamma_{g,H,G}$.
   a) Jika g^2 bukan e, maka $deg(x) = |H| - s|C_H(x)|$ dengan s = 1 jika x konjugat ke xg atau xg^{-1} di H, tapi tidak keduanya, dan s = 2 jika x konjugat ke xg dan xg^{-1} di H.
   b) Jika $g^2 = e$, maka $deg(x) = |H| - |C_H(x)|$ jika xg konjugat ke x di H. Untuk g = e berlaku $deg(x) = |H| - |C_H(x)|$.
   c) Jika xg dan xg^{-1} tidak konjugat ke x di H, maka deg(x) = |H|.
2) Misalkan x di H.
   a) Jika g^2 bukan e, maka $deg(x) = |G| - s|C_G(x)|-1$ dengan s = 1 jika x konjugat ke xg atau xg^{-1}, tapi tidak keduanya, dan s = 2 jika x konjugat ke xg dan xg^{-1}.
   b) Jika $g^2 = e$, maka $deg(x) = |G| - |C_G(x)|-1$ jika xg konjugat ke x. Untuk g = e berlaku $deg(x) = |G| - |C_G(x)|$.
   c) Jika xg dan xg^{-1} tidak konjugat ke x, maka deg(x) = |G|-1.

Dalam hal graf yang terkait dengan gelanggang, salah satu topik yang diteliti adalah graf Jacobson. Pada awalnya Azimi, Erfanian, dan Farrokhi (2013) memperkenalkan definisi awal dari graf Jacobson dan memberikan sifat diameter, sabuk, bilangan dominasi, bilangan independen, dan bilangan kromatik sisi. Misalkan R gelanggang komutatif dengan radikal Jacobson J(R) (yaitu, irisan semua ideal maksimal di R). Graf Jacobson dari R, $\Im_R$, adalah graf

dengan himpunan titiknya adalah R-J(R), dan x dan y tak nol bertetangga jika dan hanya jika 1-xy bukan unit.

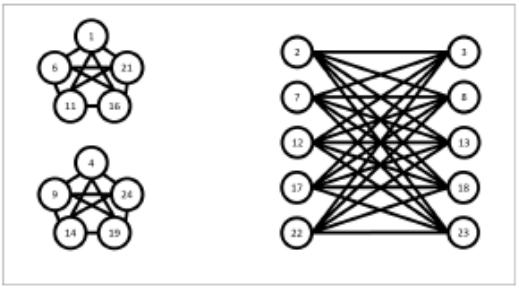
Aditya dan Muchtadi-Alamsyah (2021) membahas mengenai graf Jacobson atas Z_n yaitu sifat-sifat konektivitas, diameter, banyaknya tetangga, planaritas dan graf Hamilton. Gambar 2.15 dan Gambar 2.16, masing-masing memperlihatkan suatu graf Jacobson dari Z_6 , $\Im_{Z6}$ dan Z_{25}, $\Im_{Z25}$.



Gambar 2.15 Graf Jacobson dari Z_6 , $\Im_{Z6}$ (Aditya dan Muchtadi-Alamsyah, 2021).

Teorema 2.9 (Aditya dan Muchtadi-Alamsyah, 2021)

1) Untuk k bilangan asli, $\Im_{Z_{2^k}}$ adalah graf lengkap $K_{2^{k-1}}$.
2) Untuk p bilangan prima ganjil, $\Im_{Z_p}$ bersifat bipartit.
3) Untuk p prima ganjil dan k bilangan asli, bentuk dari $\Im_{Z_{p^k}}$ adalah 2 komponen disjoin $K_{p^{k-1}}$ dan (p-3)/2 komponen disjoin $K_{p^{k-1},p^{k-1}}$



Gambar 2.16 Graf Jacobson dari Z_{25} , $\Im_{Z25}$ (Aditya dan Muchtadi-Alamsyah, 2021)

Diameter dari suatu graf adalah jarak terbesar antar dua titik dalam graf tersebut.

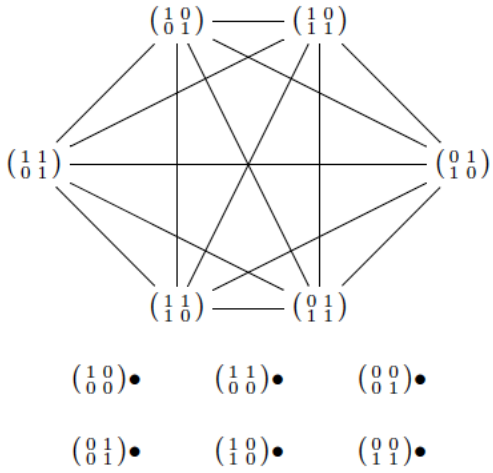
Teorema 2.9 (Aditya dan Muchtadi-Alamsyah, 2021)

1) Graf Jacobson atas gelanggang bilangan bulat modulo n berdiameter satu jika dan hanya jika $n = 2^k$ untuk $k \geq 2$.
2) Tidak ada n yang memenuhi sehingga diameter $\Im_{Z_n}$ adalah 2.

3) Graf Jacobson atas gelanggang bilangan bulat modulo n berdiameter 3 jika dan hanya jika n memiliki setidaknya dua faktor prima berbeda.
4) Graf Jacobson atas gelanggang Zn berdiameter tak hingga jika dan hanya jika $n = p^k$ untuk p bilangan prima ganjil dan $k \geq 1$.
5) Graf Jacobson atas gelanggang bilangan bulat modulo n planar jika dan hanya jika n = p, 4, 6, 8, 9 dengan p bilangan prima.

Penelitian graf Jacobson mulai diperumum oleh Ghayour dkk. (2017) dengan mendefinisikan graf Jacobson *n–array* dan membahas beberapa sifat graf dari perumuman ini, berupa diameter, keterhubungan, keplanaran dan sifat *perfect*.

Berdasarkan hal ini, telah dikembangkan graf Jacobson matriks yang pada awalnya didefinisikan untuk lapangan hingga (Humaira dkk., 2020); kemudian diperluas lebih lanjut dengan penelitian graf Jacobson matriks atas gelanggang komutatif hingga (Humaira dkk., 2022). Sifat-sifat yang diperoleh pada graf Jacobson matriks atas gelanggang berupa diameter, keplanaran, dan *perfectness*. Sebagai contoh, graf Jacobson matriks 2x2 dari Z_2 , $\Im_{Z2}{}^{2x2}$ ditunjukkan pada Gambar 2.17.

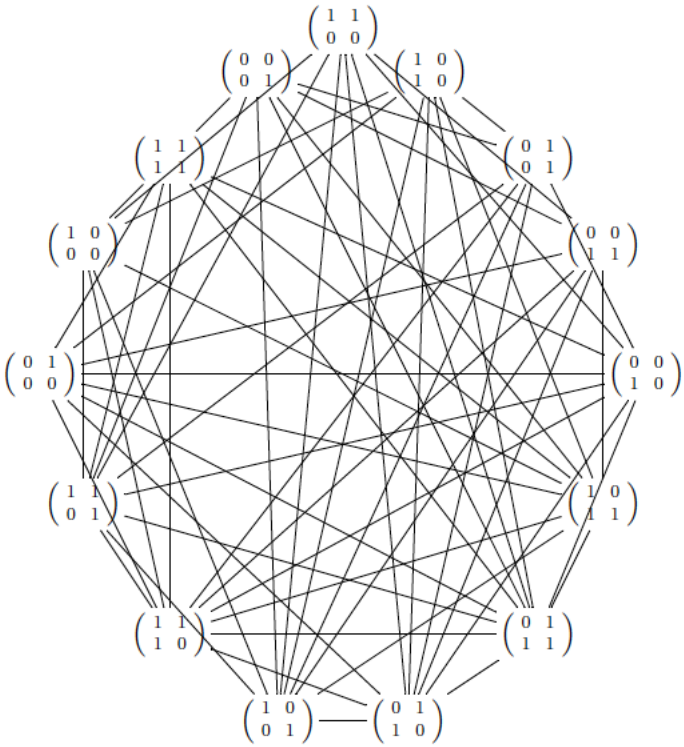


Gambar 2.17 Graf Jacobson matriks 2x2 dari Z_2 , $\Im_{Z2}{}^{2x2}$ (Humaira dkk., 2022).

Selanjutnya diselidiki juga graf Jacobson atas gelanggang non komutatif/ gelanggang matriks (Humaira, 2023), dan diperoleh sifat diameter dan hubungan antara rank titik yang berupa matriks dengan derajat titik tersebut. Sebagai contoh adalah graf Jacobson matriks $\Im_{M2(Z2)}$ pada Gambar 2.18.

Teorema 2.10 (Humaira, 2023) Misalkan R gelanggang non lokal hingga, maka

1) diameter $\Im_{Mn(R)} \leq 3$.
2) diameter $\Im_{Mn(R)} = 2$ jika dan hanya jika $R \cong R_1 \oplus R_2 \oplus \ldots \oplus R_k$, dimana terdapat $i \in \{1, \ldots, k\}$ sedemikian sehingga $R_i/J(R_i) \cong Z_2$.
3) diameter $\Im_{Mn(R)} = 3$ jika dan hanya jika $|R_i/J(R_i)| \geq 3$ untuk setiap $i \in \{1, \ldots, k\}$.



Gambar 2.18 Graf Jacobson matriks $\Im_{M2(Z2)}$ (Humaira, 2023).

Proposisi berikut menjelaskan derajat setiap titik di graf Jacobson dari gelanggang matriks atas gelanggang non-lokal.

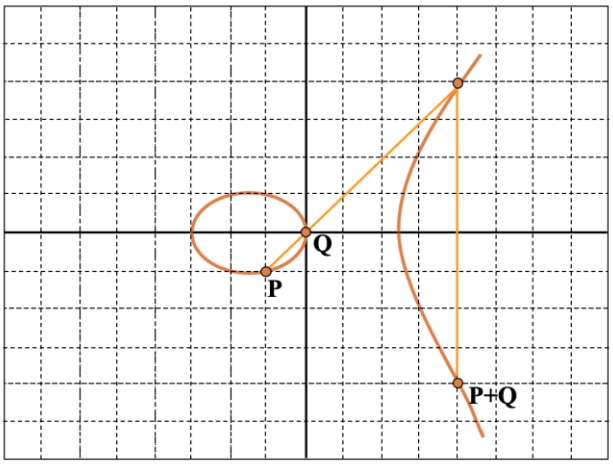
Proposisi 2.11 (Humaira, 2023)
Misalkan $R = R_1 \oplus R_2 \oplus \ldots \oplus R_k$ adalah gelanggang non lokal hingga. Untuk setiap titik $A \in \Im_{Mn(R)}$, $A = A_1 \times A_2 \times \ldots \times A_k$, dengan $A_i \in M_n(R_i)$. Tulis $\deg(A_i)$ sebagai derajat A_i di $\Im_{Mn(Ri)}$, maka

$$\deg(A) = \prod_{i=1}^{k} |R_i|^{n^2} - \prod_{i=1}^{k} \left(|R_i|^{n^2} - \deg(A_i)\right).$$

3. APLIKASI ALJABAR

3.1 Kriptografi

Kriptografi Kurva Eliptik pertama kali diperkenalkan oleh Neal Koblitz dan Victor Miller (Koblitz, 1987; Miller, 1986). Mereka secara terpisah memperkenalkan kurva eliptik untuk kriptografi kunci publik. Dibandingkan dengan metode kriptografi lainnya, kriptografi kurva eliptik memiliki beberapa keunggulan (Li dkk., 2001; Paryasto dkk., 2009): operasi aritmatika yang bersifat spesifik dan tidak dapat diprediksi dan panjang kunci yang lebih kecil untuk tingkat keamanan yang sama dibandingkan dengan metode lain. Gambar 3.1 memperlihatkan operasi penjumlahan titik-titik pada kurva eliptik.



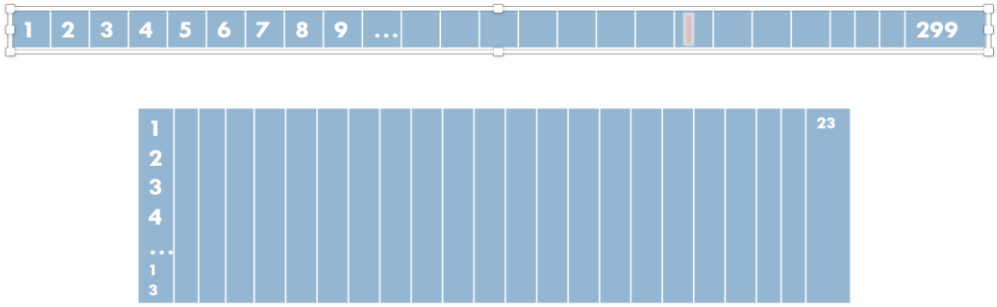
Gambar 3.1 Operasi penjumlahan titik-titik pada kurva eliptik.

Operasi dalam kriptografi kurva eliptik berkaitan dengan suatu struktur aljabar, yaitu struktur grup dari himpunan titik-titik di dalam kurva eliptik digabung dengan titik tak hingga. Tingkat keamanan kriptografi kurva eliptik bergantung pada Masalah Logaritma Diskrit Kurva Eliptik (ECDLP) (Rahardjo dkk., 2015)

Penelitian yang telah dilakukan dalam kriptografi kurva eliptik adalah pengembangan algoritma efisien untuk mempercepat operasi kurva pada kriptografi kurva eliptik yang dapat meminimalkan sumber daya. Mengingat operasi pada kurva eliptik dibangun oleh operasi pada lapangan hingga, telah

dihasilkan algoritma dan implementasi konversi basis lapangan hingga, dari basis polinomial ke basis normal dan sebaliknya (Paryasto dkk., 2010; Muchtadi-Alamsyah dkk., 2012). Penggunaan basis normal ini dapat mempercepat penghitungan untuk operasi kurva eliptik, mengingat pengkuadratan dapat dilakukan cukup dengan menggeser bit.

Kemudian Paryasto dkk. (2012) meneliti kriptografi kurva eliptik berbasis lapangan hingga komposit. Dalam segi komputasi, lapangan komposit lebih efisien karena komputasinya dapat dilakukan dengan membagi dalam sublapangan-sublapangan kecil yang paralel. Gambar 3.2 menunjukkan perbandingan lapangan prima GF(299) dan lapangan komposit GF$(2^{13})^{23}$.



Gambar 3.2 Gambaran perbandingan lapangan prima GF(299) dan lapangan komposit GF$(2^{13})^{23}$.

Lebih lanjut telah dihasilkan algoritma untuk konversi basis untuk lapangan komposit (Muchtadi-Alamsyah dan Yuliawan, 2013).

Algoritma 3.1 Konversi basis polinom ke basis normal optimal tipe I dan sebaliknya (Muchtadi-Alamsyah dan Yuliawan, 2013).

ALGORITHM PB-PONBI

Input: $A = (a_0, a_1, \ldots, a_{m-1})$, the representation in PB

Output: $B = (b_0, b_1, \ldots, b_{m-1})$, the corresponding representation in type I PONB

Procedure: $B \leftarrow \mathrm{LShift}\,(A) - (a_0, a_0, \ldots, a_0)$

ALGORITHM PONBI-PB

Input: $B = (b_0, b_1, \ldots, b_{m-1})$, representation in type-I PONB

Output: $A = (a_0, a_1, \ldots, a_{m-1})$, the corresponding representation in PB

Procedure: $A \leftarrow \mathrm{RShift}\,(B) - (b_{m-1}, b_{m-1}, \ldots, b_{m-1})$

Algoritma 3.2 Algoritma konversi basis polinom ke basis normal optimal tipe II (Muchtadi-Alamsyah dan Yuliawan, 2013).

ALGORITHM PB-PONBII

Input: $A = (a_0, a_1, \ldots, a_{m-1})$, the representation in PB

Output: $B = (b_0, b_1, \ldots, b_{m-1})$, the corresponding representation in type II PONB

Procedure:

$B \leftarrow (0, 0, \ldots, 0)$

$W \leftarrow (1, 1, \ldots, 1)$

for i from 0 to $m-1$ do

$B \leftarrow B + a_i \times W$

$W \leftarrow \mathrm{RShift}(W) + \mathrm{LShiftLL}(W)$

endfor

Salah satu keuntungan dari algoritma di atas adalah konversi dari lebih dari satu elemen sekaligus dapat dilakukan secara lebih efisien. Hanya diperlukan menghitung W sekali dan digunakan untuk setiap konversi. Untuk melakukan sebanyak k konversi sekaligus: dari A_1, A_2, ..., A_s dalam basis polinomial ke B_1, B_2, ..., B_s dalam basis normal optimal tipe 2, algoritmanya diberikan sebagai Algoritma 3.3.

Algoritma 3.3 Algoritma konversi basis polinom ke basis normal optimal tipe II secara simultan (Muchtadi-Alamsyah dan Yuliawan, 2013).

$B \leftarrow (0, 0, \ldots, 0)$

$W \leftarrow (1, 1, \ldots, 1)$

for i from 0 to $m-1$ do

for j from 1 to k do

$B_j \leftarrow B_j + A_j[i] \times W$

endfor

$W \leftarrow \mathrm{RShift}(W) + \mathrm{LShiftLL}(W)$

endfor

Untuk konversi dari basis normal optimal tipe II ke basis polinomial, pertama diberikan Algoritma Tali Sepatu (*Shoelace*), yang memberikan representasi dari elemen yang dikalikan dengan invers dari generator.

Algoritma 3.4. Algoritma *Shoelace* (Muchtadi-Alamsyah dan Yuliawan, 2013)

ALGORITHM SHOELACE

Input: $V = (v_0, v_1, \ldots, v_{m-1})$, the representation in type-II PONB

Output: $X = (x_0, x_1, \ldots, x_{m-1})$, the representation of $X = G^{-1} \times V$ in the same basis, where G^{-1} is the representation of the α^{-1}.

Procedure:

$x_i \leftarrow v_0$

$i \leftarrow 3$

while $i < m$ do

$x_i \leftarrow x_{i-2} + v_{i-1}$

$i \leftarrow i + 2$

endwhile

if $i = m - 1$ do

$x_{m-2} \leftarrow x_{m-1} + v_{m-1}$

$i \leftarrow m - 4$

else

$x_{m-1} \leftarrow x_{m-2} + v_{m-1}$

$i \leftarrow m - 3$

endif

while $i \geq 0$ do

$x_i \leftarrow x_{i+2} + v_{i+1}$

$i \leftarrow i - 2$

endwhile

Algoritma 3.4 Algoritma konversi basis normal optimal tipe II ke basis polinomial (Muchtadi-Alamsyah dan Yuliawan, 2013).

ALGORITHM PONBII-PB

Input: $B = (b_0, b_1, \ldots, b_{m-1})$, representation in type-II PONB

Output: $A = (a_0, a_1, \ldots, a_{m-1})$, the corresponding representation in PB

Procedure:

for i from 0 to $m - 1$ do

$a_i \leftarrow b_{m-1}$

$B \leftarrow B + (b_{m-1}, b_{m-1}, \ldots, b_{m-1})$

$B \leftarrow \text{Shoelace}(B)$

endfor

Konversi lapangan komposit telah dimanfaatkan untuk membangun algoritma konversi basis yang *storage-free* (Akyildiz, 2017), begitu juga kajian lapangan komposit dalam kriptografi kurva eliptik telah dimanfaatkan untuk membangun suatu arsitektur *co-processor* kriptografi kurva eliptik (Jagan dan Nagarajan, 2013) dan *symmetric crypto processor* (Su dkk., 2021).

Selanjutnya Susantio dan Muchtadi-Alamsyah (2016) mengembangkan skema enkripsi kriptografi kurva eliptik S-ECIES (*Simplified Elliptic Curve Integrated Encryption Scheme)* yang lebih efisien dalam segi penyimpanan.

Algoritma 3.6 Algoritma enkripsi S-ECIES (Susantio dan Muchtadi, 2016).

INPUT: kata-asal x.
OUTPUT: kata-sandi $(U(x_1, y_1), y)$
1: **for** $char \in x$ **do**
2: $char \leftarrow$ BINARYASCII($char$)
3: $char \leftarrow$ PADDING($char$)
4: **end for**
5: $blocklength \leftarrow \lfloor N/7 \rfloor$
6: $x \leftarrow$ BLOCK(x, $blocklength$)
7: $k \leftarrow$ RANDOM($[1, n-1]$)
8: $U(x_1, y_1) \leftarrow kP$
9: $V(x_2, y_2) \leftarrow kQ$
10: **for** $char \in x$ **do**
11: $cipher \leftarrow char \cdot x_2$
12: APPEND(y, $cipher$)
13: **end for**
14: **return** (U, y)

Algoritma 3.7 Algoritma dekripsi S-ECIES (Susantio dan Muchtadi, 2016).

INPUT: kata-sandi $(U(x_1, y_1), y)$.
OUTPUT: kata-asal x
1: $V(x_2, y_2) \leftarrow mU$
2: **for** $cipher \in y$ **do**
3: $char \leftarrow cipher/x_2$
4: $char \leftarrow$ PADDING($char$)
5: APPEND(x, $char$)
6: **end for**
7: $x \leftarrow$ SPLIT(x)
8: **for** $char \in x$ **do**
9: $char \leftarrow$ DEASCII($char$)
10: **end for**
11: **return** x

Implementasi tersebut telah dibahas juga dalam (Vincent dkk., 2020) untuk *mobile payment security,* (Duemong dan Preechaveerakul, 2021) untuk *key generation,* (Realpe-Munoz dkk., 2021) untuk desain *cryptoprocessor,* dan (Renita dkk., 2022) tentang implementasi kriptografi kurva eliptik dengan *multiplier* yang efisien.

Serangan terhadap kriptografi kurva eliptik yang pernah diteliti adalah serangan Pollard Rho. Modifikasinya, yang menggunakan Pemetaan Negasi,

Pemetaan Frobenius, basis normal dan *Brent Cycle Algorithm*, dapat mempercepat serangan Pollard Rho (Muchtadi-Alamsyah dkk., 2013; Muchtadi-Alamsyah dan Utomo, 2017; Muchtadi-Alamsyah dkk., 2016).

Dalam Tabel 3.1 diberikan perbandingan antara Pollard Rho standar dengan Pollard Rho yang menggunakan Algoritma Brent *Cycle Detection*. Dalam Tabel 3.2 diberikan perbandingan yang sama dengan kurva yang digunakan adalah kurva Koblitz tanpa pemetaan Frobenius, sedangkan perbandingan serupa untuk kurva Koblitz dengan pemetaan Frobenius diberikan pada Tabel 3.3.

Tabel 3.1 Perbandingan antara Pollard Rho standar dengan Pollard Rho yang menggunakan Algoritma Brent *Cycle Detection* (Muchtadi-Alamsyah dan Utomo, 2017).

Bit	Standard		Brent	
	Iteration	Time (second)	Iteration	Time (second)
17	352	0.156248	473	0.203124
19	895	0.453124	1571	0.765614
23	6098	3.765658	12555	7.656267
29	15689	12.687533	30471	23.515687
31	58678	51.593854	99505	83.578315
37	251950	290.188130	351431	364.672700
41	2310322	4993.765471	3869603	4943.581061

Tabel 3.2 Perbandingan antara Pollard Rho standar dengan Pollard Rho dengan Algoritma Brent *Cycle Detection* untuk kurva Koblitz tanpa pemetaan Frobenius (Muchtadi-Alamsyah dan Utomo, 2017).

Bit	Standard		Brent	
	Iteration	Time (second)	Iteration	Time (second)
7	16	0.015624	30	0.015626
11	43	0.015637	51	0.015624
13	130	0.062496	168	0.062498
17	89	0.046876	97	0.046874
19	1819	0.906245	3479	1.703126
23	398	0.249999	636	0.390642
41	1125258	2098.714221	3165644	4122.895303

Tabel 3.3 Perbandingan antara Pollard Rho standar dengan Pollard Rho dengan Algoritma Brent *Cycle Detection* untuk kurva Koblitz dengan pemetaan Frobenius (Muchtadi-Alamsyah dan Utomo, 2017)

Bit	Standard		Brent	
	Iteration	Time (second)	Iteration	Time (second)
7	3	0.015641	6	0.015625
11	21	0.046877	25	0.031263
13	12	0.031254	24	0.031230
17	131	0.218761	162	0.234359
19	123	0.265640	207	0.375001
23	861	2.125028	1065	2.359400
41	87869	648.544495	90326	558.360148

Berdasarkan eksperimen, penggunaan pemetaan Frobenius secara umum mereduksi banyaknya iterasi yang diberikan. Namun, waktu yang dibutuhkan tidak selalu lebih pendek. Hal ini dikarenakan adanya waktu tambahan yang diperlukan untuk membangun kelas ekuivalen dari setiap iterasi.

Dalam Tabel 3.4 diberikan perbandingan antara Pollard Rho dengan pemetaan Frobenius dan Pollard Rho tanpa pemetaan Frobenius untuk kurva Koblitz, keduanya menggunakan Algoritma Brent *Cycle Detention*. Dalam Tabel 3.5 diberikan perbandingan yang sama namun tanpa Algoritma Brent *Cycle Detention* dan tanpa pemetaan negasi. Perbandingan yang sama tanpa Algoritma Brent *Cycle Detention* dan menggunakan pemetaan negasi diberikan pada Tabel 3.6.

Berdasarkan eksperimen di atas, terlihat bahwa penggunaan pemetaan negasi secara umum mereduksi banyaknya iterasi yang diperlukan. Namun, jika pemetaan negasi digunakan tanpa pemetaan Frobenius, hampir 10 persen (276,344 dari of 2,773,726) iterasi berulang.

Tabel 3.4 Perbandingan antara Pollard Rho dengan pemetaan Frobenius dan Pollard Rho tanpa pemetaan Frobenius untuk kurva Koblitz, keduanya menggunakan Algoritma Brent *Cycle Detention* (Muchtadi-Alamsyah dan Utomo, 2017).

Bit	With Frobenius		Without Frobenius	
	Iteration	Time (second)	Iteration	Time (second)
7	30	0.015626	6	0.015625
11	51	0.015624	25	0.031263
13	168	0.062498	24	0.031230
17	97	0.046874	162	0.234359
19	3479	1.703126	207	0.375001
23	636	0.390642	1065	2.359400
41	3165644	4122.895303	90326	558.360148

Tabel 3.5 Perbandingan antara Pollard Rho dengan pemetaan Frobenius dan Pollard Rho tanpa pemetaan Frobenius untuk kurva Koblitz, keduanya tanpa Algoritma Brent *Cycle Detention* dan tanpa pemetaan negasi (Muchtadi-Alamsyah dan Utomo, 2017).

Bit	With Frobenius		Without Frobenius	
	Iteration	Time (second)	Iteration	Time (second)
7	30	0.015626	6	0.015625
11	51	0.015624	25	0.031263
13	168	0.062498	24	0.031230
17	97	0.046874	162	0.234359
19	3479	1.703126	207	0.375001
23	636	0.390642	1065	2.359400
41	3165644	4122.895303	90326	558.360148

Tabel 3.6 Perbandingan antara Pollard Rho dengan pemetaan Frobenius dan Pollard Rho tanpa pemetaan Frobenius untuk kurva Koblitz, keduanya tanpa Algoritma Brent *Cycle Detention* tetapi menggunakan pemetaan negasi (Muchtadi-Alamsyah dan Utomo, 2017).

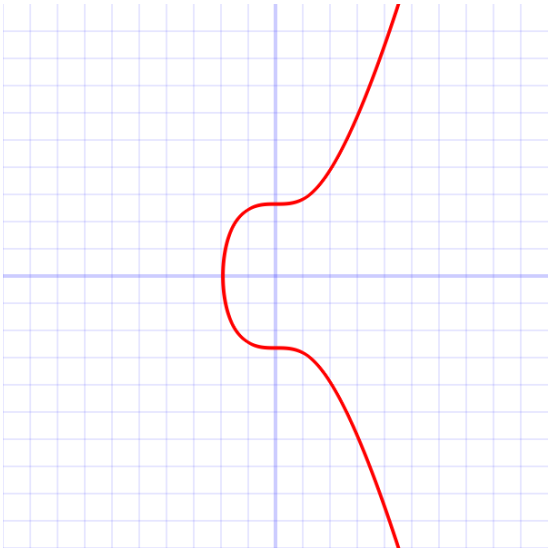
Bit	With Frobenius		Without Frobenius	
	Iteration	Time (second)	Iteration	Time (second)
7	11	0.015616	2	0.031252
11	25	0.015626	13	0.046874
13	113	0.062489	17	0.046894
17	411	0.218751	63	0.171890
19	495	0.296888	102	0.328139
23	3959	2.906526	696	2.609399
41	1142980	2449.223652	66879	666.827368

Kembali ke proses enkripsi dan dekripsi, Muchtadi-Alamsyah dan Tama (2020) mengimplementasikan kurva eliptik Curve25519 dalam S-ECIES untuk *instant messaging* (Gambar 3.3) sehingga menunjukkan bahwa kurva eliptik Curve25519 juga dapat melayani tujuan lain selain pertukaran kunci.

Gambar 3.3 Enkripsi dalam *Instant Messaging*.

Dalam (Muchtadi-Alamsyah dkk., 2020) diusulkan skema transaksi Ethereum berdasarkan protokol *group digital signature* sebagai langkah untuk mengurangi masalah pencucian uang di jaringan Ethereum. Secara khusus, skema ini bekerja dengan memberikan kemampuan otoritas grup terpilih untuk mengungkap informasi dari transaksi anonim sambil mencegah pengguna lain termasuk penambang untuk mendapatkannya. Pada Gambar 3.4 diperlihatkan kurva eliptik $y^2 = x^3 + 7$ yang digunakan dalam skema tanda tangan digital kurva eliptik (ECDSA), digambarkan untuk lapangan real.

Pencucian mata uang virtual (*cryptocurrency*) sulit dilacak karena tidak ada hubungan antara alamat dengan orang/identitas tertentu. Kecuali jika pihak yang terlibat dalam transaksi menyembunyikan informasinya, tidak ada artefak digital yang dapat digunakan sebagai bukti di persidangan untuk menegaskan argumen penyalahgunaan transaksi anonim.



Gambar 3.4 Kurva eliptik $y^2 = x^3 + 7$ yang digunakan dalam skema tanda tangan digital kurva eliptik (ECDSA), digambarkan untuk lapangan real.

Penelitian yang telah dilakukan (Muchtadi-Alamsyah dkk., 2020) menggunakan anonimitas terbatas dan pengambilan keputusan berdasarkan konsensus (pemilihan). Teknik ini memberikan beberapa usulan transaksi yang akan dilakukan secara pribadi yang dijamin dengan legitimasi masyarakat. Menemukan alamat penandatangan transaksi itu sulit secara matematis. Namun, otoritas dapat melihatnya dengan membandingkan identitas ID dan kunci grup pada database pembangkit kunci grup.

Kesulitan dan keterbatasan dalam implementasinya terkait dengan proses pendaftaran beberapa anggota yang tidak dikenal, yang dapat mengacaukan transaksi dengan mendaftarkan ID yang tidak sesuai dengan identitas pengguna. Dalam hal ini, otoritas kelompok hanya boleh mencakup anggota yang dia kenal dalam dirinya sendiri.

Namun, dengan adanya pengembangan komputer kuantum, kriptografi yang sering digunakan saat ini, seperti RSA dan kriptografi kurva eliptik diprediksi tidak akan aman lagi. Salah satu solusi yang ditawarkan adalah dengan menggunakan kriptografi berbasis Teori Koding. Kriptografi berbasis kode yang sejauh ini paling aman adalah skema McEliece yang memanfaatkan kode Goppa dalam proses enkripsi dan dekripsinya (Cayrel dkk., 2011). Dalam (Irwansyah dkk., 2019) telah dikembangkan suatu skema kode permutasi LDPC (*Low-Density Parity Check*) dalam kriptosistem McEliece.

3.2 Teori Koding

Sejak pertama kali diperkenalkan pada akhir tahun 1940-an, Teori Koding Aljabar menggunakan lapangan hingga sebagai alfabet. Kemudian, pada awal tahun 1990-an, termotivasi dengan aplikasi teknik, seperti desain untuk CDMA, muncullah penggunaan kode atas gelanggang, yang puncaknya adalah paper (Hammons dkk., 1994) yang mendapatkan *Best Paper Award* tahun 1994 dari IEEE Information Theory Society, karena berhasil memecahkan teka-teki 20 tahun, dualitas formal dari kode Kerdock dan Preparata. Mereka menggunakan dualitas dari kode atas Z_4, suatu gelanggang dengan jumlah elemen 4 yang bukan lapangan hingga. Kode siklik memiliki aplikasi dalam sistem penyimpanan data (*data storage system*) dan sistem komunikasi *(communication system)* karena kode siklik memiliki algoritma *encoding* dan *decoding* yang efisien.

Penggunaan Teori Gelanggang dalam Teori Koding adalah dengan memandang kode sebagai ideal dari suatu gelanggang. Seperti misalnya kode siklik dengan panjang n atas alfabet A dengan struktur gelanggang, adalah kode linier atas A dengan panjang n yang invarian terhadap pergeseran. Kode siklik dapat dipandang sebagai ideal dari gelanggang faktor $R_n = A[X]/(X^n-1)$, himpunan polinom-polinom dengan koefisien A dikuosien dengan ideal yang dibangun oleh X^n-1. Kuosien dengan ideal X^n-1 diperlukan supaya penggeseran katakode berkorespondensi dengan perkalian polinom dengan X. Konstruksi kode siklik dengan menggunakan barisan periodik telah dilakukan dalam (Syarifuddin dan Muchtadi-Alamyah, 2018; Nopendri dkk., 2021), dan kode siklik atas gelanggang hingga perluasan dari Z_{2^m} dalam (Rosdiana dkk., 2021).

Diberikan suatu kode C atas sebarang gelanggang R. Definisikan hasil kali dalam Euclid pada R_n sebagai berikut

$$(x_0,x_1,\ldots,x_n) \cdot (y_0,y_1,\ldots,y_n) = x_0y_0 + x_1y_1 + \ldots + x_ny_n \tag{3.1}$$

Definisikan kode dual dari C, $C^{\perp} = \{\mathbf{x} \in R^n: \mathbf{x.c} = 0$ untuk setiap $\mathbf{c} \in C\}$. Kode C dikatakan *self orthogonal* jika $C \subseteq C^{\perp}$ dan dikatakan *self dual* jika $C = C^{\perp}$.

Berikut adalah sebuah syarat perlu dan cukup suatu kode menjadi kode linier *Euclidean self-dual* atas gelanggang $R = Z_{2^m} + vZ_{2^m}$, dengan $v^2 = v$.

Misalkan $R = Z_{2^m} + vZ_{2^m}$, dengan $v^2 = v$, dan definisikan

$C_1 = \{\mathbf{x} \in Z_{2^m}^n : \exists \mathbf{y} \in Z_{2^m}^n , v\mathbf{x} + (1-v)\mathbf{y} \in C\}$ dan

$C_2 = \{\mathbf{y} \in Z_{2^m}^n : \exists \mathbf{x} \in Z_{2^m}^n , v\mathbf{x} + (1-v)\mathbf{y} \in C\}$. (3.2)

Kode C_1 dan C_2 keduanya bersifat Z_{2^m}-linier dengan panjang n. Suatu kode linier C atas R dapat dinyatakan secara tunggal sebagai

$C = vC_1 \oplus (1-v)C_2$. (3.3)

Proposisi 3.1 (Rosdiana dkk., 2021) Misalkan C kode linier atas $R = Z_{2^m} + vZ_{2^m}$, dengan panjang n, maka

1) kode dual dari C, $C^{\perp} = vC_1^{\perp} \oplus (1-v)C_2^{\perp}$
2) kode C Euclidean self dual jika dan hanya jika C_1 dan C_2 Euclidean self dual atas Z_{2^m}.

Dengan demikian kajian kode *Euclidean self dual* atas $R = Z_{2^m} + vZ_{2^m}$, dengan $v^2 = v$, dapat dilakukan melalui kajian kode *Euclidean self dual* atas Z_{2^m}.

Untuk memperoleh kode-kode optimal baru, telah diupayakan penggunaan gelanggang polinom miring. Terkait penelitian gelanggang polinom miring, telah dikaji metode mempertahankan sifat suatu gelanggang jika diganti dengan gelanggang polinom miring.

Pertama, dengan memotong gelanggang polinom miring dengan ideal primanya sehingga struktur dapat dipertahankan (Amir dkk., 2011). Kedua, dengan perumuman gelanggang prima Dedekind dan gelanggang prima Asano, yang dapat mempertahankan struktur G-Dedekind dan G-Asano pada gelanggang polinom miringnya (Marubayashi dkk., 2013; Suwastika dkk., 2015). Telah dikaji juga gelanggang polinom miring dari gelanggang Morita *context* (Hamonangan dan Muchtadi-Alamsyah, 2022).

Irwansyah dkk. (2021) memberikan algoritma untuk menghitung banyaknya kode siklik miring (kode θ-siklik) dengan panjang n atas F_q, dengan n genap dan $\gcd(n,|\theta|) = 1$. Dalam Tabel 3.7 diberikan banyaknya kode θ- siklik *Euclidean self dual* atas F_8, dengan $\theta(y) = y^2$ untuk setiap y di F_8.

Selanjutnya, telah diperoleh suatu konstruksi kode optimal untuk kode siklik miring atas suatu aljabar berdimensi hingga $B_k = F_p{}^r[v_1,v_2,..,v_k]/\langle v_iv_j - v_jv_i,$

v_i^2-v_i> yang menggunakan metode-metode pada gelanggang polinom miring (Irwansyah, 2016; Irwansyah dkk., 2016; Irwansyah dkk., 2021).

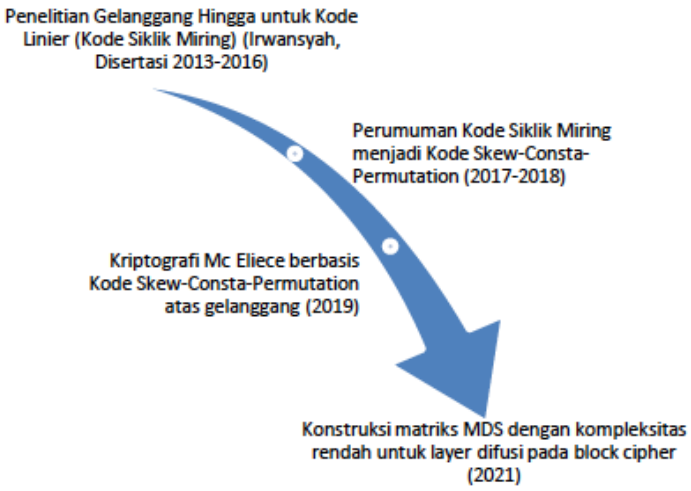
Kajian kode siklik miring (Gambar 3.5) telah dimanfaatkan untuk membangun kode kuantum asimetrik (Muchtadi-Alamsyah dan Irwansyah, 2019) dan dijadikan referensi juga dalam membangun kode kuantum dalam (Suprijanto dan Tang, 2022). Selain itu, telah dikembangkan perumuman kode siklik (*generalized cyclic codes)* dengan meninjau Teori Modul (Muchtadi-Alamsyah dkk., 2022).

Tabel 3.7 Banyaknya kode θ- siklik *Euclidean self dual* atas F_8, dengan $\theta(y) = y^2$ (Irwansyah dkk., 2021).

n	♯ E.S.D. θ-cyclic codes
10	1
14	3
20	1
28	5
40	1
56	9
80	1
112	17
160	1
224	33
320	1
448	65

Tabel 3.8 Kode-kode θ-siklik *self-dual* Euclid optimal atas gelanggang B_k dengan panjang n dan jarak d (Irwansyah, 2016).

n	d	Polinom pembangun	B_k	θ
4	3	$x^2 + \alpha^2 x + \alpha$	B_2	$v_2 \mapsto 1 - v_2$ $v_1 \mapsto 1 - v_1$
12	6	$x^6 + x^5 + \alpha^2 x^4 + x^3 + \alpha x^2 + x + 1$	B_3	$v_1 \mapsto 1 - v_1$ $v_2 \mapsto 1 - v_2$ $v_3 \mapsto 1 - v_3$
20	8	$x^{10} + \alpha^2 x^9 + \alpha x^8 + x^7 + x^6$ $+x^4 + x^3 + \alpha x^2 + \alpha x + 1$	B_4	$v_1 \mapsto 1 - v_1$ $v_2 \mapsto 1 - v_2$ $v_3 \mapsto 1 - v_3$ $1 - v_4 \mapsto v_4$
36	11	$x^{18} + x^{16} + \alpha^2 x^{15} + \alpha x^{14} + \alpha^2 x^{13} + x^{12}$ $+\alpha x^{10} + \alpha x^9 + \alpha x^8 + \alpha^2 x^6 + x^5 + \alpha x^4$ $+x^3 + \alpha^2 x^2 + \alpha^2$	B_6	$v_1 \mapsto 1 - v_1$ $1 - v_2 \mapsto v_2$ $v_3 \mapsto 1 - v_3$ $v_4 \mapsto 1 - v_4$ $v_5 \mapsto 1 - v_5$ $v_6 \mapsto 1 - v_6$
40	12	$x^{20} + x^{17} + \alpha^2 x^{15} + \alpha x^{14} + \alpha^2 x^{13} + \alpha^2 x^{12}$ $+x^{11} + x^9 + \alpha x^8 + \alpha x^7 + \alpha^2 x^6 + \alpha x^5 + x^3 + 1$	B_7	$v_1 \mapsto 1 - v_1$ $1 - v_2 \mapsto v_2$ $v_3 \mapsto 1 - v_3$ $v_4 \mapsto 1 - v_4$ $v_5 \mapsto 1 - v_5$ $v_6 \mapsto 1 - v_6$ $v_7 \mapsto 1 - v_7$



Gambar 3.5 Diagram alir penelitian kode atas gelanggang.

Pengkajian kode siklik miring atas aljabar B_k telah dimanfaatkan lebih lanjut untuk mengkaji struktur kode linier atas aljabar B_k (Irwansyah dan Suprijanto, 2018), dan atas gelanggang R_k (Irwansyah dan Suprijanto, 2023); pengkajian kode *self-dual,* dan LCD *double circulant* dan *double nega circulant* dalam (Dinh dkk., 2023); serta pengkajian kode-G miring (Dougherty dkk., 2023).

Pendekatan lain telah dilakukan untuk mempelajari kode siklik yang memiliki jarak minimum terbesar dibandingkan dengan kode linier lainnya dengan panjang dan dimensi yang sama, atau yang lebih dikenal dengan kode siklik MDS (*Maximum Distance Separable*). Hal ini dilakukan dengan mempelajari matriks sirkulan MDS. Matriks MDS adalah matriks yang setiap submatriksnya memiliki invers.

Pada tahun 1996 matriks MDS pertama kali digunakan dalam chiper SHARK (Rijmen dkk., 1996) dan kemudian diikuti SQUARE (Daemen dkk., 1997) dan AES (Daemen dkk., 2022). Proses enkripsi AES memiliki empat langkah yaitu SubBytes, ShiftRows, MixColumns, dan AddRoundkey (Daemen dkk., 2022). Matriks MDS digunakan dalam MixColumns.

Karena proses dekripsi biasanya menggunakan invers dari matriks yang digunakan dalam proses enkripsi, maka penggunaan matriks yang inversnya mudah dicari akan lebih baik. Salah satu pilihannya adalah menggunakan matriks MDS ortogonal atau involutori.

Khoo dkk. (2014) memperkenalkan metrik yang disebut *XOR-count* untuk mengukur biaya implementasi perangkat keras dari difusi matriks. Semakin kecil nilai *XOR-count* dari sebuah matriks, semakin baik matriks dalam implementasi perangkat keras. Matriks dengan jumlah *XOR-count* kecil belum tentu memiliki invers dengan *XOR-count* kecil. Namun, matriks ortogonal atau involutori dan inversnya memiliki jumlah *XOR-count* yang sama. Oleh karena itu matriks MDS ortogonal atau involutori lebih disukai di beberapa *cipher* blok.

AES menggunakan matriks MDS sirkulan di lapisan difusi. Satu keuntungan dari matriks sirkulan adalah bahwa matriks sirkulan berorde n memiliki maksimum n komponen yang berbeda. Jelas bahwa menyimpan n elemen lebih baik daripada menyimpan n^2 elemen. Daemen dkk. (1997) membuktikan bahwa peluang menemukan matriks MDS sirkulan lebih signifikan dibandingkan dengan matriks persegi random. Penelitian kemudian diarahkan untuk kajian matriks MDS sirkulan involutori atau ortogonal.

Dalam (Irwansyah dkk., 2021) telah diberikan konstruksi matriks MDS involutori dan Adhiguna dkk. (2022) mengkaji eksistensi matriks MDS sirkulan ortogonal, dan juga memberikan syarat perlu dan cukup untuk matriks bersifat MDS, θ-sirkulan, dan ortogonal. Matriks MDS θ-sirkulan ini juga berkaitan dengan kode siklik miring MDS.

Teorema 3.2 (Adhiguna dkk., 2022)

1) Misalkan $m = 4n$, dengan n bilangan asli, maka tidak terdapat matriks MDS ortogonal sirkulan berorde m atas lapangan berkarakteristik 2.
2) Tidak terdapat matriks MDS sirkulan ortogonal berorde genap m atas lapangan berkarakteristik $p > 2$.

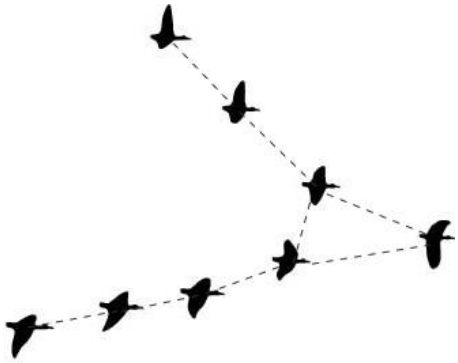
3.3 Aljabar Linier

3.3.1 Konektivitas Aljabar

Dalam (Erfianto dkk., 2016), fungsi kontrol Lyapunov digunakan untuk mengonstruksi input kontrol *flocking* dengan menjaga konektivitas pada sekelompok jaringan agen robot bergerak. Agen dimodelkan sebagai massa titik dinamis, dan strategi kontrol yang diusulkan melibatkan kekuatan

potensial dan konsensus kecepatan. Beberapa kekuatan potensial dirancang untuk mengarahkan agen *neighbor* ke jarak yang telah ditentukan sambil menghindari tabrakan di antara mereka sehingga keterhubungan topologi jaringan dapat dijamin. Di bawah asumsi bahwa topologi *flocking* awal terhubung, keseluruhan topologi berkelompok dipertahankan untuk terhubung, sementara penghindaran rintangan dan tabrakan juga dijamin.

Untuk menjamin tercapainya tujuan dari *flocking multiagent*, konektivitas tetap terjaga dengan menjaga nilai eigen terkecil kedua dari topologi *flocking*.



Gambar 3.6 Model analisis perilaku berkelompok burung (Erfianto dan Muchtadi-Alamsyah, 2019).

Lebih lanjut dalam (Erfianto dan Muchtadi-Alamsyah, 2019) model analisis perilaku berkelompok burung disajikan menggunakan graf dan teori kontrol (Gambar 3.6). Diperoleh bahwa model yang dihasilkan stabil secara asimtotik. Dengan mengamati nilai eigen terkecil kedua dari matriks Laplacian dari topologi *flocking*, kekokohan perilaku berkelompok burung juga dapat diamati. Namun, karena nilai eigen terkecil kedua dari matriks Laplacian hanya mengukur keterhubungan, kerentanan topologi *flocking* tidak dapat ditentukan. Penggunaan matriks Laplace *perturbed* dari topologi *flocking* tereduksi merepresentasikan adanya gangguan pada perilaku *flocking*, dan nilai eigen terkecil ketiga dari matriks Laplacian *perturbed* dapat digunakan untuk mengukur kerentanan seluruh formasi *flocking*.

3.3.2 Kuadrat Terkecil *Fitting* Dimensi Tiga

Ellipsoid atau anisotropi geometrik adalah metode yang banyak digunakan dalam analisis geostatistik untuk mendapatkan variogram dengan rentang yang berbeda dalam arah yang berbeda (azimuth) dan varian *sill* yang relatif sama. Anisotropi elipsoida sangat diperlukan dalam penambangan untuk

memahami kontinuitas spasial variabel yang terkait dengan kontrol geologis dari mineralisasi. Misalnya ketika berhadapan dengan mineralisasi yang terkait dengan endapan tabular, endapan porfiritik dengan pola lubang bor yang tidak beraturan (pengeboran kipas).

Dalam (Muchtadi-Alamsyah dkk., 2022a), metode kuadrat terkecil 3D digunakan untuk *fitting* anisotropi elipsoida 3D kadar seng (Zn) yang terkait dengan pola lubang bor yang tidak beraturan.

Pertama, untuk mencocokkan data dalam bentuk tiga dimensi, bentuk umum dari persamaan permukaan kuadratik berikut digunakan

$$f(x,y,z) \coloneqq a_{11}x^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz + a_{22}y^2 + a_{33}z^2 + b_1x + b_2y + b_3z + c = \mathbf{u}\cdot\mathbf{x} = 0 \qquad (3.4)$$

dengan: $\mathbf{u} = (a_{11} \;\; 2a_{12} \;\; 2a_{13} \;\; 2a_{23} \;\; a_{22} \;\; a_{33} \;\; b_1 \;\; b_2 \;\; b_3 \;\; c)^T$

$$\mathbf{x} = (x^2 \;\; xy \;\; xz \;\; yz \;\; y^2 \;\; z^2 \;\; x \;\; y \;\; z \;\; 1)^T.$$

Kemudian, untuk memperoleh koefisien dari persamaan umum, langkah-langkah berikut dilakukan:

Langkah 1: Dari data, konstruksi matriks berikut:

$$S = \begin{pmatrix} x_1 & y_1 & z_1 & 1 & {x_1}^2 & \sqrt{2}x_1y_1 & \sqrt{2}x_1z_1 & \sqrt{2}y_1z_1 & {y_1}^2 & {z_1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_n & y_n & z_n & 1 & {x_n}^2 & \sqrt{2}x_ny_n & \sqrt{2}x_nz_n & \sqrt{2}y_nz_n & {y_n}^2 & {z_n}^2 \end{pmatrix} \qquad (3.5)$$

dengan n adalah banyaknya data

Langkah 2. Gunakan faktorisasi QR untuk memperoleh $S = QR$, dengan Q matriks ortogonal dan R matriks segitiga atas.

Langkah 3. Tulis $R = \begin{pmatrix} R_{11} & R_{12} \\ 0 & R_{22} \end{pmatrix}$ dan definisikan vektor $\mathbf{v} = (b_1 \;\; b_2 \;\; b_3 \;\; c)^T$ dan $\mathbf{w} = \left(a_{11} \;\; \sqrt{2}a_{12} \;\; \sqrt{2}a_{13} \;\; \sqrt{2}a_{23} \;\; a_{22} \;\; a_{33}\right)^T$.

Langkah 4. Tulis $\left\|S\begin{pmatrix}\mathbf{v}\\ \mathbf{w}\end{pmatrix}\right\| = \left\|QR\begin{pmatrix}\mathbf{v}\\ \mathbf{w}\end{pmatrix}\right\| = \left\|R\begin{pmatrix}\mathbf{v}\\ \mathbf{w}\end{pmatrix}\right\|$. *Problem*-nya menjadi menentukan $\min\|R_{22}\mathbf{w}\|$ dengan batasan $\|\mathbf{w}\| = 1$.

Langkah 5. Gunakan Dekomposisi Nilai Singular (SVD) pada R_{22} sehingga $R_{22} = U\Sigma V^T$.

Langkah 6. Berdasarkan Teorema SVD (Teorema 2.3 dalam (Gander, 2008)), solusi dari $\min\|R_{22}\mathbf{w}\|$ dengan batasan $\|\mathbf{w}\| = 1$ adalah $\mathbf{w} = \mathbf{v}_n$, dengan $\mathbf{v}_n$ adalah kolom terakhir matriks V.

Langkah 7. Hitung $\mathbf{v} = -R_{11}{}^{-1}R_{12}\mathbf{w}$, lalu **u** diperoleh dengan menyubstitusikan vektor **v** dan **w**.

Selanjutnya, substitusikan koefisien pada vektor **u** ke dalam persamaan umum f(x,y,z) untuk mendapatkan fitting elipsoida atau hiperboloida. Untuk mendapatkan dataset bentuk elipsoida, dilakukan dua langkah:

1. jika persamaan f(x,y,z) yang diperoleh merupakan persamaan elipsoida, maka telah diperoleh hasil yang diinginkan;
2. jika hasil yang diperoleh adalah persamaan hiperboloida, maka lanjutkan proses dengan langkah-langkah berikut.

Dari hasil perhitungan, koefisien **w'** dan **v'** ditetapkan sebagai berikut:

$$\mathbf{w}' = \begin{pmatrix} a'_{11} \\ 0 \\ 0 \\ 0 \\ a'_{22} \\ a'_{33} \end{pmatrix} \quad \text{and} \quad \mathbf{v}' = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ c \end{pmatrix} \text{dengan kondisi:}$$

- jika $c > 0$, maka $a'_{11} = -|a_{11}|$, $a'_{22} = -|a_{22}|$, $a'_{33} = -|a_{33}|$; dan
- jika $c < 0$, maka $a'_{11} = |a_{11}|$, $a'_{22} = |a_{22}|$, $a'_{33} = |a_{33}|$.

Sehingga diperoleh persamaan

$$a'_{11}x^2 + a'_{22}y^2 + a'_{33}z^2 + b_1x + b_2y + b_3z + c = 0. \tag{3.6}$$

Persamaan (3.6) dapat disederhanakan sebagai berikut:

$$a'_{11}x^2 + b_1x + a'_{22}y^2 + b_2y + a'_{33}z^2 + b_3z + c = 0$$

$$\Leftrightarrow a'_{11}(x + \frac{b_1}{2a'_{11}})^2 - \frac{b_1^2}{4a'^2_{11}} + a'_{22}\left(y + \frac{b_2}{2a'_{22}}\right)^2 - \frac{b_2^2}{4a'^2_{22}} + a'_{33}(z + \frac{b_3}{2a'_{33}})^2 - \frac{b_3^2}{4a'^2_{33}} + c = 0$$

$$\Leftrightarrow a'_{11}(x + \frac{b_1}{2a'_{11}})^2 + a'_{22}\left(y + \frac{b_2}{2a'_{22}}\right)^2 + a'_{33}(z + \frac{b_3}{2a'_{33}})^2 = \frac{b_1^2}{4a'^2_{11}} + \frac{b_2^2}{4a'^2_{22}} + \frac{b_3^2}{4a'^2_{33}} - c.$$

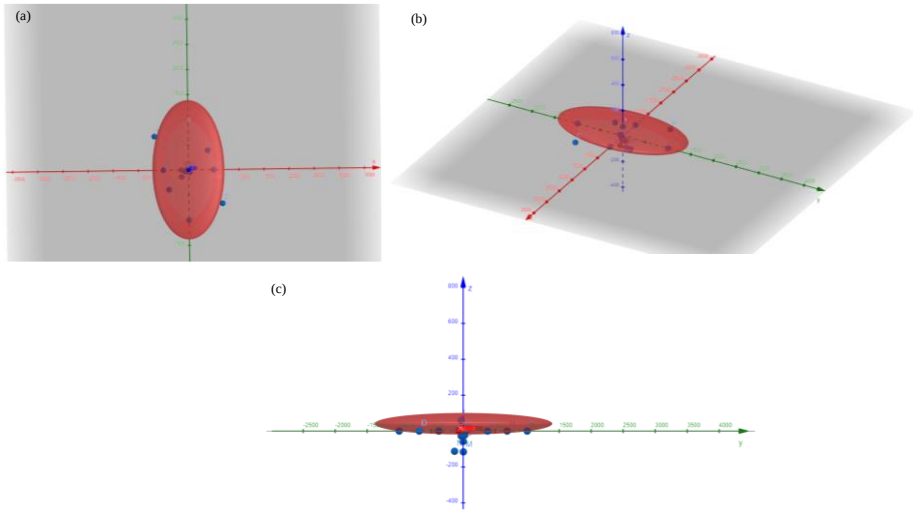
Misalkan $\frac{b_1}{2a'_{11}} = \alpha, \frac{b_2}{2a'_{22}} = \beta, \frac{b_3}{2a'_{33}} = \gamma, \frac{b_1^2}{4a'^2_{11}} + \frac{b_2^2}{4a'^2_{22}} + \frac{b_3^2}{4a'^2_{33}} - c = p$, maka

$$a'_{11}(x + \alpha)^2 + a'_{22}(y + \beta)^2 + a'_{33}(z + \gamma)^2 = p$$
$$\Leftrightarrow \frac{a'_{11}(x + \alpha)^2}{p} + \frac{a'_{22}(y + \beta)^2}{p} + \frac{a'_{33}(z + \gamma)^2}{p} = 1.$$

Misalkan $\frac{a'_{11}}{p} = q, \frac{a'_{22}}{p} = r, \frac{a'_{33}}{p} = s$, maka diperoleh persamaan elipsoida sebagai berikut:

$$\frac{(x+\alpha)^2}{q} + \frac{(y+\beta)^2}{r} + \frac{(z+\gamma)^2}{s} = 1. \quad (3.7)$$

Dalam Gambar 3.7 diperlihatkan hasil anisotropi elipsoida 3D dilihat dari atas, depan dan samping.



Gambar 3.7 Hasil anisotropi elipsoida 3D dilihat dari (a) atas (b) depan, dan (c) samping (Muchtadi-Alamsyah dkk., 2022a).

Model anisotropi dari radius pencarian lebih realistis diterapkan untuk estimasi geostatistik 3D dari mineralisasi skarn Zn, yang biasanya menunjukkan model pelapisan. Sementara model isotropi radius pencarian (yaitu, model bola, yang biasanya digunakan untuk sistem porfiritik) kurang realistis untuk badan bijih skarn, karena estimasi geostatistik 3D-nya cenderung menghasilkan model kolom atau tabular.

3.4 Wavelet dan Transformasi Paket Gelombang (*Wave Packet Transform*)

Analisis data dimensi hingga dan pemrosesan sinyal adalah dasar dari digital pemrosesan sinyal, teori informasi, dan analisis data berskala besar. Dalam pengolahan data, analisis frekuensi-waktu (*time-scale*) terdiri atas teknik yang menganalisis vektor dalam domain waktu dan frekuensi (waktu dan skala) secara bersamaan, disebut metode atau representasi frekuensi-waktu (*time-scale*) (Casazza dan Kutyniok, 2013). Biasanya metode terstruktur yang digunakan untuk analisis frekuensi waktu disebut analisis Gabor (Feichtinger dkk., 2009), untuk analisis skala waktu disebut analisis wavelet (Strang dan Nguyen, 1996), dan untuk skala waktu-frekuensi, analisis ini disebut metode paket gelombang (Farashahi, 2014).

Dalam (Wanditra dkk., 2020), dengan menggunakan transformasi paket gelombang pada grup siklik, dipelajari transformasi paket gelombang pada grup abelian hingga. Dalam kasus grup siklik, ini merupakan transformasi pada ruang Banach yang dibentuk oleh representasi grup siklik. Hasil ini diperumum untuk transformasi yang dibentuk oleh representasi grup komutatif.

Selanjutnya dalam (Wanditra dkk., 2021) dengan menggunakan wavelet dan coding Python, jumlah total padatan tersuspensi (*Total Suspended Solid*) di Sungai Cikapundung dapat diperkirakan secara *time series*. Dataset TSS di Sungai Cikapundung dari tahun 2017 hingga 2018 digunakan untuk membuat model dari *Total Suspended Solid* yang bergantung pada waktu. Transformasi wavelet digunakan untuk penskalaan dan penentuan frekuensi dari dataset TSS. Hasil transformasi dapat digunakan sebagai masukan untuk model ARIMA. Diperoleh bahwa model dari wavelet ARIMA cukup baik untuk peramalan TSS di Sungai Cikapundung.

4. APLIKASI REPRESENTASI KUIVER

4.1 Kecerdasan Buatan (*Artificial Intelligence*)

Saat ini kecerdasan buatan ditemui di setiap aspek kehidupan. Kecerdasan buatan dalam pertandingan sepak bola sebagai video *assistant referee,* atau muncul sebagai mobil otonom (Zhang dan Wang, 2020). Kecerdasan buatan digunakan untuk pengenalan dan pelacakan objek, dan biasanya algoritma yang digunakan adalah jaringan saraf tiruan (*Artificial Neural Network*) (Scholler dkk., 2020).

Jaringan syaraf tiruan bekerja seperti otak manusia. Di otak manusia, informasi diproses dengan mentransfer sinyal antar neuron. Neuron dapat digambarkan sebagai titik dalam saraf tiruan jaringan. Model matematika untuk jaringan syaraf tiruan dibangun menggunakan representasi kuiver dengan node sebagai titik dan transfer informasi sebagai busurnya.

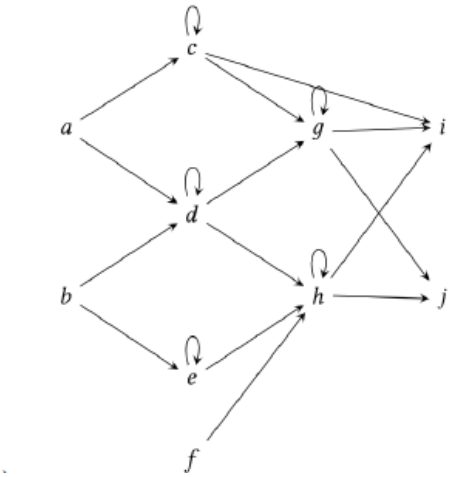
Suatu kuiver dapat menggambarkan konektivitas antar-neuron, dan representasi kuiver dapat menggambarkan transfer informasi antara neuron. Dalam jaringan syaraf tiruan, fungsi aktivasi digunakan untuk mengukur pentingnya informasi yang dilanjutkan dalam neuron.

Misalkan Q suatu kuiver. Suatu representasi tipis (*thin*) $M = (M_a, \varphi_\alpha)$ adalah suatu representasi kuiver dengan M_a adalah $\mathbb{C}$ untuk setiap a di Q_0. Suatu kuiver Q dikatakan diatur dengan *layer* jika dapat digambarkan dari kiri ke kanan dengan diatur titiknya dalam kolom, sedemikian rupa sehingga tidak ada busur dari titik di sebelah kanan ke titik di sebelah kiri, dan tidak ada busur antara titik dalam kolom yang sama, selain loop dan sisi dari titik bias.

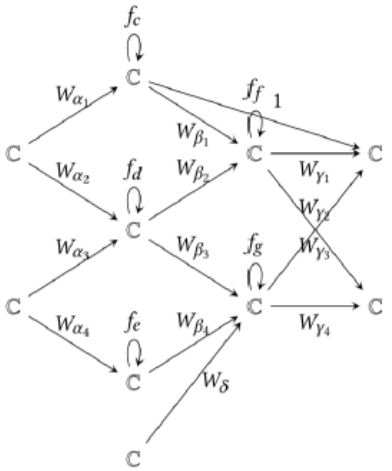
Layer pertama di sebelah kiri, yang disebut *input layer,* dibentuk oleh d titik *input*. *Layer* terakhir di sebelah kanan, yang disebut *output layer,* dibentuk oleh k titik *output*. *Layer* yang bukan *input layer* atau *output layer* disebut *layer* tersembunyi (*hidden layer*).

Suatu kuiver jaringan (*network quiver*) Q merupakan kuiver yang diatur oleh *layer* sedemikian sehingga tidak ada *loop* di sumber (yaitu, *input* dan bias) juga tidak ada di titik *sink* dan terdapat tepat satu loop di setiap titik di *layer* tersembunyi (Gambar 4.1). Suatu jaringan syaraf (*neural network*) atas kuiver jaringan Q adalah pasangan (W,f) dengan W representasi tipis (Gambar 4.2)

dari kuiver tanpa loop Q^0 dan $f = (f_v)$, $v \in Q_0$ adalah fungsi aktivasi yang berkaitan dengan loop dari Q. Jika (W,f) adalah suatu jaringan syaraf atas kuiver jaringan Q, fungsi jaringan (*network function*) dari jaringan syaraf (W,f) adalah fungsi $\psi(W, f): \mathbb{C}^d \rightarrow \mathbb{C}^k$ dengan koordinat dari $\psi(W, f)(x)$ adalah *output* aktivasi dari titik *output* dari (W,f) terhadap vektor *input* $x \in \mathbb{C}^d$.



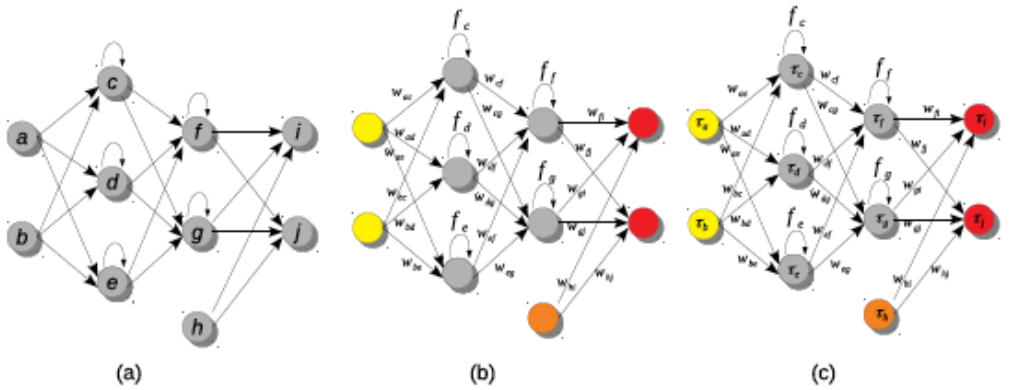
Gambar 4.1 Contoh kuiver jaringan (Armenta dan Jodoin, 2021).



Gambar 4.2 Contoh representasi tipis dari suatu kuiver jaringan (Armenta dan Jodoin, 2021).

Dengan menggunakan pendekatan representasi kuiver, Armenta, dan Jodoin (2021) membuktikan bahwa ada tak hingga banyak jaringan syaraf dengan fungsi jaringan yang sama, terlepas dari arsitektur dan fungsi aktivasi. Dengan demikian, untuk mempelajari jaringan syaraf tertentu, cukup dipelajari jaringan syaraf yang lebih "sederhana" yang isomorfik dengan

jaringan syaraf tersebut. Gambar 4.3 secara berurutan menunjukkan kuiver jaringan Q, jaringan syaraf (*neural network*) berdasar pada Q dengan bobot W dan fungsi aktivasi f, dan jaringan syaraf yang sama tetapi dengan perubahan basis pada setiap neuron (titik).



Gambar 4.3 (a) Kuiver jaringan *(network quiver)* Q (b) Jaringan syaraf (*neural network*) berbasis pada Q dengan bobot W dan fungsi aktivasi f (c) Jaringan syaraf yang sama tapi dengan perubahan basis pada setiap neuron (titik) (Armenta dkk., 2023).

Sebagai pengembangan dari (Armenta dan Jodoin, 2021) digunakan aljabar grup dalam representasi kuiver (sebagai titik, menggantikan himpunan bilangan kompleks). Aljabar grup $\mathbb{C}G$ adalah objek matematika yang dibentuk oleh pemetaan-pemetaan dari grup G ke lapangan $\mathbb{C}$. Secara khusus diambil G yang merupakan grup siklik berhingga. Aljabar grup digunakan karena, dalam beberapa kasus, diperlukan neuron untuk bekerja dengan informasi yang berdimensi lebih dari satu, misalnya warna. Dengan menggunakan representasi aljabar grup kuiver, akan dibandingkan beberapa jaringan saraf tiruan menggunakan representasi kuiver.

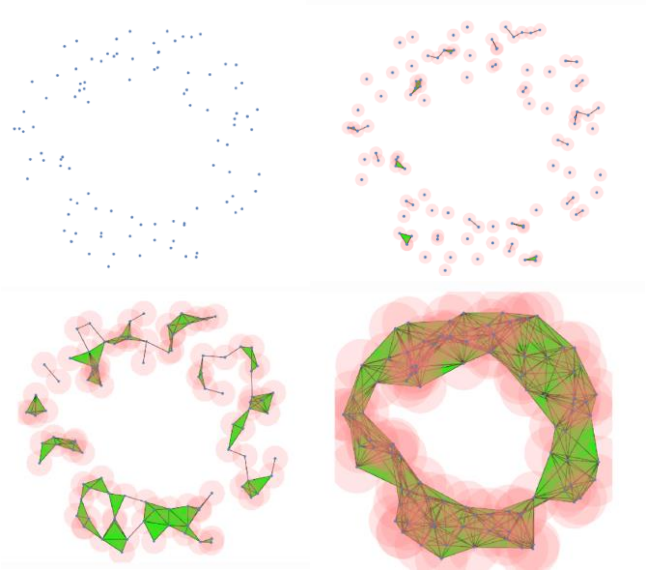
4.2 Analisis Data Topologi (*Topological Data Analysis*)

Dalam era big data saat ini, data dari berbagai sumber mudah untuk diperoleh. Namun, data tersebut tidak berarti jika tidak dapat diolah untuk memperoleh informasi yang bermanfaat. Pengolahan data akan memudahkan suatu individu, organisasi, atau perusahaan untuk membuat keputusan yang tepat. Saat ini kumpulan data yang perlu diolah tidak hanya data berupa angka atau teks, tetapi sebagian besar data dapat bervariasi dari gambar/foto, kumpulan objek tertentu, profil dinamis dari sistem yang

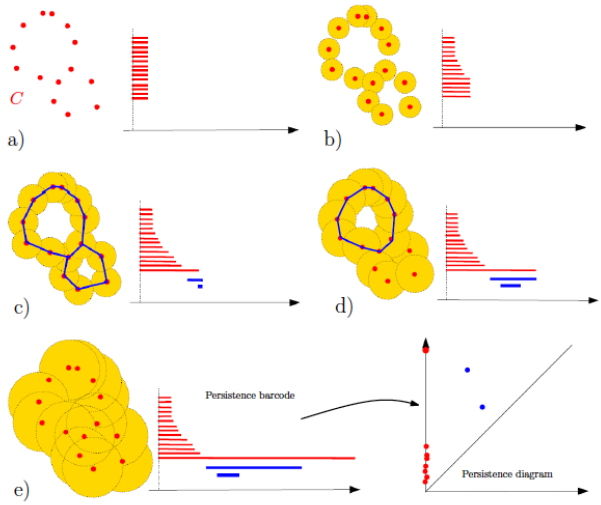
berkembang, suara rekaman, atau rekaman video. Tentu tidak semua metode statistik bisa menangani berbagai tipe data yang disebutkan di atas. Diperlukan pendekatan lain untuk mengekstrak data dan mendapatkan kesimpulan. Salah satu metode tersebut adalah Analisis Data Topologi (*Topological Data Analysis* -TDA) (Chazal dan Michel, 2021).

Analisis Data Topologi (TDA) adalah metode yang relatif baru dalam data sains. Lahir dari topologi aljabar, TDA mengekstrak kumpulan data dengan melihat pada bentuk data. Bentuk data yang dimaksud di sini adalah topologi fitur, yang lebih dikenal sebagai invarian topologi, misalnya, *cluster*, loop, dan bentuk sulur yang muncul dari titik data.

Bagaimana topologi aljabar digunakan untuk mempelajari fitur geometris data? Topologi menawarkan alat untuk menghitung jumlah lubang dan *path component* dalam suatu ruang. Namun, jika X terdiri dari n titik dalam ruang yang memiliki n komponen dan tidak ada lubang sama sekali, maka topologi tidak dapat menyimpulkan sesuatu yang menarik dari hal ini. Untuk ini, tidak digunakan topologi X secara langsung, melainkan menggunakan fitur topologi penebalan dari X (Gambar 4.4). Dalam sudut pandang aljabar: data dibuat menjadi menjadi ruang topologi atau ruang metrik terlebih dahulu.



Gambar 4.4 Contoh fitur penebalan dari X (Laha, 2019).



Gambar 4.5 Filtrasi sublevel dan konstruksi *persistent barcode* saat jari-jari bola meningkat (Chazal dan Michel, 2021).

Alat TDA adalah homologi persisten (*persistent homology*) dan modul persisten (*persistent module)*. Homologi persisten menghitung jarak dua titik dalam suatu ruang dan melihat bagaimana jarak berkembang seiring waktu. Modul persisten merupakan representasi dari proses filtrasi dalam bentuk struktur aljabar yang menyimpan informasi "*survival*" tentang kelas-kelas homologi yang muncul secara berurutan. Modul persisten digunakan untuk mendefinisikan diagram *barcode* yang nantinya akan digunakan untuk mengkomunikasikan fitur topologi yang muncul dari pengolahan data menggunakan homologi persisten. Filtrasi sublevel dan konstruksi *persistent barcode* saat jari-jari bola meningkat ditunjukkan oleh Gambar 4.5.

Modul persisten dapat didekomposisikan menjadi jumlah langsung modul interval I(b,d) berbentuk

$$0 \to \cdots \to 0 \to K \xrightarrow{1_K} \ldots \xrightarrow{1_K} K \to 0 \to \cdots \to 0 \qquad (4.1)$$

dengan K pertama berawal di titik b dan K terakhir berakhir di titik d.

Teorema Krull-Remak-Schmidt (Azumaya, 1950) mengatakan bahwa setiap representasi kuiver M dari kuiver Q atas K dapat didekomposisikan menjadi jumlah langsung representasi-representasi yang *indecomposable*. Lebih lanjut Teorema Gabriel (Gabriel, 1972) menyebutkan bahwa jika Q adalah kuiver tipe A_n seperti pada Gambar 2.8 (kuiver garis), maka setiap

representasi *indecomposable* dari Q atas K isomorfik dengan suatu representasi interval I(b,d) (4.1) seperti di atas.

Dalam banyak kasus, modul persisten dapat didekomposisi menjadi jumlah langsung modul-modul interval I(b,d). Oleh karena itu pemahaman tentang dekomposisi representasi kuiver dapat membantu untuk memahami modul persisten dan persisten diagram.

Beberapa penelitian mengenai hal ini dapat dilihat pada (Lindell, 2017), tentang metode-metode dekomposisi untuk representasi kuiver; dalam (Takeuchi, 2012), tentang homologi persisten dari *sampled map*; di (Carlsson dkk., 2021), tentang homologi persistent dan zigzag; dalam (Hiraoka dkk., 2022), tentang teorema stabilitas aljabar untuk kategori bentukan dari modul persisten zigzag; dalam (Asashiba dkk., 2022), tentang dekomposisi interval dari modul-modul persisten berdimensi 2. Detail lebih lanjut mengenai Analisis Data Topologi dan representasi kuiver dapat dilihat dalam (Oudot, 2015). Untuk penelitian lebih lanjut, akan diselidiki modul persisten berdimensi yang lebih tinggi melalui representasi kuiver.

5. PENUTUP

Perkembangan ilmu pengetahuan dan teknologi membutuhkan penguasaan ilmu-ilmu dasar yang semakin kuat. Penelitian representasi aljabar yang dilakukan di ITB telah dibawa ke arah penggunaan representasi aljabar, pertama untuk mengklasifikasi aljabar itu sendiri; memperkaya Teori Graf dengan membentuk graf dari grup dan gelanggang sekaligus mempelajari sifat-sifatnya.

Kemudian penelitian dilanjutkan terkait berbagai penerapan aljabar dalam bidang Kriptografi khususnya untuk *instant messaging* dan mata uang virtual; bidang Teori Koding, pemodelan menggunakan metode kuadrat terkecil 3D dan pemodelan dinamika robot/ *flocking bird*, serta penggunaan wavelet untuk memprediksi *total suspended solid.*

Penelitian-penelitian terkini menunjukkan bahwa teori representasi kuiver dapat juga digunakan untuk ilmu-imu baru yang sedang berkembang saat ini, di antaranya kecerdasan buatan dan sains data, di mana representasi kuiver digunakan dalam jaringan syaraf tiruan (*artificial neural network*) dan analisis data topologi (*topological data analysis*). Akhir kata, perjalanan ini masih terus berlanjut, dan semoga memberikan manfaat sebesar-besarnya bagi kemajuan ilmu pengetahuan dan teknologi, demi bangsa, Tuhan dan almamater.

6. UCAPAN TERIMA KASIH

Segala puji syukur kami panjatkan ke hadirat Allah Swt. atas segala rahmat dan karunia-Nya. Perkenankan kami mengucapkan terima kasih sebesar-besarnya kepada yang terhormat Rektor dan Pimpinan ITB, Pimpinan dan seluruh Anggota Forum Guru Besar ITB yang telah memberi kesempatan untuk menyampaikan orasi ilmiah pada forum yang terhormat ini.

Ucapan terima kasih yang tak terhingga bagi Ayahanda yang sudah berpulang Prof. Deddy Muchtadi, dan Ibunda Prof. Tien Ruspriatin Muchtadi serta Bapak dan Ibu mertua, H. Samsuri Hardjito, S.H. dan Hj. Suwarsih atas semua pengorbanan, dukungan dan doa tulus hingga pencapaian hari ini. Terima kasih sebesar-besarnya bagi guru-guru kami sejak TK sampai Pasca Doktor, atas ilmu yang bermanfaat yang telah diajarkan kepada kami. Secara khusus kami mengucapkan terima kasih kepada Prof. Hendra Gunawan, Alm. Prof. Ahmad Arifin, Prof. Alexander Zimmermann (Universite de Picardie), Prof. Steffen Koenig (Stuttgart University), Prof. Idun Reiten (NTNU), sebagai pembimbing kami saat kami baru mengenal Matematika. Terima kasih juga pada dosen-dosen kami Prof. Ansjar, Prof. Bernhard Keller (Univ. de Paris 6), Prof. Wono S. Budhi, Prof. Edy Soewono, Prof. Irawati, Prof. Kuntjoro Sidarto, Prof. Iwan Pranoto, Prof. R.K. Sembiring, Dr. Bana Kartasasmita, Prof. Maman Djauhari, Alm.Prof. Moedomo,Alm.Prof Sunardi, Alm. Prof. Nababan, Almh. Dr. Sri Wulan Adji, Alm. Koko Martono,M.Si., Dr. Ahmad Muchlis, Muliana A.,M.Si., Nyoman Susila, M.Si., Dr.Nana N.Gaos, E. Hutahaean, M.Si., Hidayat Sardi, M.Si., Samyoeto, M.Si., Dra. Samsiah, Sumanto, M.Si., dll.

Penghargaan dan apresiasi setinggi-tingginya bagi Pimpinan Senat FMIPA ITB Prof. Akhmaloka dan segenap anggota senat, Dekan FMIPA ITB Prof. Wahyu Srigutomo beserta Wakil Dekan Prof. Rukman Hertadi dan Dr. Hanni Garminia. Terima kasih juga kepada para pemberi rekomendasi Prof. Pudji Astuti, Prof. Edy Tri Baskoro, Prof. Bambang Riyanto, Prof. Bethany Marsh, dan Prof. Karin Baur (University of Leeds) dan Prof. Indah Emilia Wijayanti (UGM); dan penelaah Prof. Udjianna Pasaribu dan Prof. Emir Husni.

Ucapan terima kasih juga untuk kolaborator dalam dan luar negeri Dr. Aleams Barra, Dr. Fajar Yuliawan, Dr. Dellavitha Nasution, Dr. Gantina Rachmaputri, Dr. Budi Rahardjo, Prof. Kuspriyanto, Prof. M. Nur Heriawan,

Dr. Sarwono Sutikno, Dr. Djoko Suprijanto, Dr. Khreshna I.A. Syuhada, Dr. Erma Suwastika, Dr. Aditya P. Santika, Dr. Dasapta E. Irawan, Dr. Hafiz Ahmad, Dr. Masoumeh Ganjali (Iran), Dr. Mahboube Nasiri (Iran), Prof. Ahmad Erfanian (Iran), Dr. Parimala (India), Dr. Madeline Al-Tahan (Lebanon), Dr. Yann Palu (Prancis), Dr. Rasool Hafezi (Iran), Dr. Manimaran (India), Dr. Udhayakumar Ramalingan (India), Prof. C. Selvaraj (India), Prof. Patrick Sole (Prancis), Prof. Hidetoshi Marubayashi (Jepang), Prof. Nor Haniza Sarmin (Malaysia), Dr. Irwansyah, Dr. Hafiz Khusyairi, Dr. Bayu Erfianto, Dr. Nopendri, Dr. Siti Humaira, Dr. Risnawita, Dr. Sri Rosdiana, Dr. Delsi Kariman, Dr. Gustina Elfiyanti, Dr. Yudi Mahatma, Dr. Faisal, Dr. Khaerudin Saleh, Dr. I G. Adhitya W. Wardhana, Dr. Darmajid, Dr. Marisa Paryasto, Prof. Amir K. Amir, Dr. Mulia Astuti, Dimitrij Ray Susantio, Taufik Utomo, Yoshua Hamonangan, Yanuar B. W. Tama, Imdad Thufaili, Ichlas Adhiguna, Salsabila Arifin, Yuniarti Rahayu, Lucky Cahya Wanditra, Valerian Pratama, Faisal Zaidan, Siddiq Wira, Devi Fitri Ferdania, Fariz Maulana, Nur Ain Supu dan Abdul Gazir. Secara khusus ucapan terima kasih kepada Dr. Frederic Ezerman (Singapura), Dr. Nguyen Van Sanh (Thailand), Prof. Guodong Zhou dan Dr. Zhengfang Wang (China) untuk berbagai diskusi yang intensif.

Terima kasih juga disampaikan untuk semua kolega dosen dan tenaga kependidikan di Komunitas Matematika terutama para Kaprodi Dr. Nuning Nuraini, Dr. Novriana Sumarti, Dr. Utriweni Mukhaiyar, dan Dr. M. Apri, terima kasih juga kepada Prof. Roberd Saragih, Prof. L.H. Wiryanto, Prof. Sri Redjeki P., Prof. Janson Naiborhu, Prof. M.Salman, Dr. Ikha Magdalena, Dr. Hilda Assiyatoen, Dr. Sapto W.Indratno, Dr. Rinovia Simanjuntak, Dr. Saladin Uttunggadewa, Dr. Janny Lindiarni, Dr. Oki Neswan, Dr. Johan Tuwankotta, Dr. Jalina Wijaya, Dr. Yudi Soeharyadi, Warsoma Djohan, M.Si., Dr. Dumaria Tampubolon, Dr.Agus Gunawan, Alm.Dr.M.Syamsuddin, Dr.Rieske Hadianti, Dr. Elvira Kusniyanti, Dr. Pritta E.Putri, Dr. Rizal Afgani, Dr. Dewi Handayani, Dr. Novry Erwina, Dr. Eric, Dr. Rudi Kusdiantara, Defita, M.Si., Ning Farida, M.Si., dan Afif Humam, M.Si., Dr. Denny I. Hakim, Ifronika,M.Si., Yuli Sri Afrianti, M.Si., Dr. Finny Oktariani, Dr. Kurnia Novita Sari, Dr. Sandy Vantika, Dr. Suhadi W. Saputro, Dr. Dila Puspita, dan lainnya. Terima kasih kepada staf TU FMIPA Listiarini Muhtari, Ira Purwaningsih, Noi Sukmawati, Novita Anggraeni, Yunita Fatmawati, dll., dan murid-murid kami Euis Asriani, Angga Wijaya, Nurul Syafithri, Irfan Hidayat, dll.

Penulis juga mengucapkan terima kasih kepada Tim LAMSAMA, Prof. Mitra Djamal, Prof. Abdul Harris, Prof. Roto, Prof. Muktiningsih, Prof. Retno Widowati, Dr. Melania Muntini, Dr. Muhammad A. Martoprawiro, Vinanda Hayuning Sukma, Dr. Atthar Ivansyah, dll.. Ucapan terima kasih juga kepada pengurus lama dan baru IndoMS dan Komunitas Peminat Aljabar, terutama kepada Prof. Syafrizal Sy, Prof. Agus Suryanto, Prof. Budi Waluyo, Dr. Sisilia Sylviani, Prof. Sri Wahyuni, Prof. Budi Nurani, Prof. Kiki Sugeng, Prof. Ch. Rini Indrati, Prof. Basuki Widodo, juga kepada pengurus SEAMS, Prof. Ngo Viet Trung (Vietnam), Prof. Maslina Darus (Malaysia), Dr. Victor Tan (Singapura), Prof. Wanida Hemakul (Thailand), Prof. Jose Maria Balmaceda (Philippines), dll.. Ucapan terima kasih juga untuk dosen-dosen di Pusat *Artificial Intelligence* ITB, dan di Forum Peneliti Muda Indonesia (ForMIND).

Tidak lupa ucapan terima kasih untuk komunitas berlari Run93run, Ganesha Number Runners, x/Kaprodirunners, Mamah Gajah Berlari, KBP Runners, G10 Runners, ITBerlari, TimikTimik, RP Bogor Runners, sebagai penyemangat kami untuk *just keep running*. Juga Alumni SD Budi Mulia Bogor, SMP& SMA Regina Pacis Bogor, Kost Tubis 43, S2 MA 1997, KPA ITB, dan ITB1993, khususnya sahabat-sahabat kami Sophi Damayanti, Yunita Warastuti, Mia Samiaji, dan Niknik Pramanik, MA93, dosen-dosen ITB 1993, pengurus IA/Yayasan ITB 1993: M. Reza, Mulia Amri, Jupriyanto, Dian D. Chandra, dan Didik Fotunadi. Terima kasih juga untuk Alumni ITB Garis Lucu (AIGL), Ibu Nobar/ Pasar *Online,* Arisan Matematika, dan *Line Dance* ITB.

Terima kasih sebesar-besarnya bagi suami tercinta Dr. Andry Alamsyah, serta putri-putri kami Sandra Samara dan Marita Almira Sarah atas segala pengorbanan dan dukungan doa. Ucapan terima kasih juga untuk Keluarga Alm. Deddy Muchtadi, Keluarga Samsuri Hardjito, Keluarga Besar Suria Saputra, Keluarga Besar Marpuan dan Keluarga Besar Arifin.

Akhir kata, penulis juga menyampaikan terima kasih kepada seluruh pihak yang tidak dapat disebutkan satu per satu atas semua perhatian, bantuan, doa dan kerja samanya dalam pencapaian akademik ini.

DAFTAR PUSTAKA

Abdollahi, A., 2007, Engel graph associated with a group, *J Algebra* 318, 680-691.

Abdollahi, A., Akbari, S., Maimani, H.R., 2006, Non-commuting graph of a group, *J Algebra 298*, 468-492.

Abdollahi, A., Mohammadi Hassanabadi, A., 2007, Non-cyclic graph of a group, *Comm. Algebra* 35, 2057-2081

Abe, H., 2017, The diagram for endomorphism algebras of two-term tilting complexes over self-injective algebras, *Communication in Algebra* Vol 45 Issue 9, 3917-3928.

Abrams, G., 2015, Leavitt path algebras: the first decade, *Bull. Math. Sciences* Vol 5 Issue 1, 59-120.

Abrams, G., Pino, G.A., 2005, The Leavitt path algebra of a graph, *Journal of Algebra* Vol 293, 319-334.

Adhiguna, I., Arifin, I.S.N., Yuliawan, F., Muchtadi-Alamsyah, I., 2022, On orthogonal circulant MDS Matrices, *International Journal of Mathematics and Computer Science* Vol 17 No 4, 1619-1637.

Aditya, M.Z., Muchtadi-Alamsyah, I., 2021, Jacobson graph over Z_n, *J.Phys. Conf. Ser.* 1722, 012027.

Akyildiz, E., Haroldi, N.Y., Sinak, A., 2017, Free storage basis conversion over finite fields, *Turkish J Math* 41, 96-109.

Amir, A.K., Marubayashi, H., Astuti, P., Muchtadi-Alamsyah,I., 2011, Corrigendum to minimal prime ideals of Ore extension over a commutative Dedekind domain and its application, *JP Journal of Algebra, Number Theory and Applications,* vol 21 No 1, 41-44.

Ara, P., Moreno, M.A., Pardo, E., 2007, Nonstable theory for graph algebras, *Algebra Represent. Theory* Vol 10 No 2, 157-178.

Armenta, M., Jodoin, P.M., 2021, The representation theory of neural networks, *Mathematics* Vol 9 No 24, 3216.

Armenta, M., Judge, T., Painchaud, N., Skandarani, Y., Lemaire, C., Sanchez, G.G., Spino, P., Jodoin, P.M., 2023, Neural teleportation, *Mathematics* Vol 11 No 2, 480.

Asashiba, H., Buchet, M., Escolar, E.G., Nakashima, K., Yoshiwaki, M., 2022, On Interval Decomposability of 2D Persistence Modules, *Comp. Geom: Theory and Appl* 105-106,101879.

Assem, I., Simson, D., Skowronski, A., 2006, Elements of the representation theory of associative algebras 1, London Math. Soc. Student Texts 65, Cambridge University Press, Cambridge.

Azimi, A., Erfanian, A., Farrokhi, M., 2013, The Jacobson graph of commutative rings, *Journal of Algebra and its Applications* Vol 12 No 3, 1250179.

Azumaya, G., 1950, Corrections and Supplementatires to My Paper Concerning Krull-Remak-Schmidt's theorem, *Nagoya Mathematical Journal* 1, 117-124.

Barati, Z., Erfanian, A., Khashyarmanesh, K., Nafar, Kh., 2014, A generalization of non commuting graph via automorphisms of a group, *Comm Algebra* Vol 42 No 1, 174-185.

Baur, K., Mahatma, Y., Muchtadi-Alamsyah, I., 2019, The U-projective resolution of modules over path algebra of type An and An-tilde, *Comm Korean Math. Soc.* Vol 34 No 3, 701-718.

Baur, K., Torkildsen, H.A., 2020, A geometric interpretation of categories of type A-tilde and of morphisms in the infinite radical, *Alg and Rep Theory* 23, 657-692.

Carlsson, G., Dwaraknath, A., Nelson, B.J., 2021, Persistent and zigzag homology a matrix factorization viewpoint, arxiv:1911.10693v2.

Casazza, P., Kutyniok, G., 2013, Finite Frames Theory and Applications, Applied and Numerical Harmonic Analysis, Springer-Birkhauser, Boston.

Cayrel, P., Hoffmann, G., Meziani, M., Niebuh, R., 2011, Recent progress in code based cryptography, *International Journal of Security and Its Application* Vol 5 No 4, 133-144.

Chazal, F., Michel, B., 2021, An Introduction to Topological Data Analysis: Fundamental and Practical Aspects for Data Scientists, *Frontiers in Artificial Intelligence* 4, 667963.

Daemen, J., Knudsen, L. R., and Rijmen, V., 1997, The block cipher SQUARE, in 4th Fast Software Encryption Workshop, LNCS, 1267, 149-165.

Daemen, J. and Rijmen, V., 2002, The Design of Rijndael: AES – The Advanced Encryption Standard, Springer-Verlag, Berlin, 20-21.

Darmajid, Muchtadi-Alamsyah, I., Irawati, 2012, The degenerations for modules and dual modules, *JP Journal of Algebra Number Theory and Applications* Vol 26 Issue 1, 65-73.

Darmajid, Muchtadi-Alamsyah, I., 2013, Open condition on variety of complexes, *East West Journal of Mathematics* Vol 15 No 1, 37-42.

Davvaz, B., Shabani-Solt, H., 2002, A generalization of homological algebra, *J. Korean Math. Soc.* No. 6, Vol 39, 881 – 898.

Deligne, P., 1977, Cohomologie etale, Seminaire de Geometrie Algebrique du Bois-Marie SGA 4 12. Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin-NewYork.

Dinh, H.Q., Yadav, B.P., Bag, T., Panario, D., Upadhyay, A.K., 2023, Self-dual and LCD double circulant and double negacirculant codes over a family of finite rings Fq[v1,v2,...,vt], *Cryptography and Communications* Vol 15 N0 3, 529-551.

Duemong, F., Preechaveerakul, L., 2021, A large scalar multiplication algorithm using modified pell numbers for key generation, *ECTI Transactions on Computer and Information Technology* Vol 15 No 2, 220-231.

Dougherty, S.T., Sahinkaya, S., Yildiz, B., 2023, Skew G-codes, *Journal of Algebra and Its Applications* Vol 22 No 2, 2350056.

Eisele, F., 2022, Bijections of silting complexes and derived Picard groups, *J. London Math. Soc.* Vol 106 Issue 2, 1008-1060.

Elfiyanti, G., Muchtadi-Alamsyah, I., Nasution, D., Amartiwi, U., 2016, Abelian property of the category of U-complexes, *Int. J. Math. Analysis* Vol 10 No 17, 849-853.

Elfiyanti, G., Muchtadi-Alamsyah, I., Yuliawan, F., Nasution, D., 2020, On the category of weakly U-complexes, *European Journal of Pure and Applied Math.* Vol 13 No 2, 323-345.

Erfianto, B., Bambang, R.T., Hindersah, H., Muchtadi-Alamsyah, I., 2016, Design of connectivity preserving flocking using control Lyapunov function, *Journal of Robotic*, Vol 2016.

Erfianto, B., Muchtadi-Alamsyah, I., 2019, Stability and Vulnerability of Bird Flocking Behaviour: A Mathematical Analysis, *Hayati Journal of Biosciences* vol 26 No. 4, 179-184.

Faisal, Muchtadi-Alamsyah, I., 2013, On cyclic Nakayama m-cluster tilted algebra of type An, Proc. Int. Conf. on Math. Research, Education and Appl., Ho Chi Minh City, 119-127.

Faisal, Muchtadi-Alamsyah, I., 2016, Characterization of Nakayama m-cluster tilted algebra of type An, *J. Indonesian Math. Soc.* Vol 22 No 2, 93-130.

Farashahi, A.G., 2014, Cyclic wave packet transform on finite Abelian groups of prime order, *Int. J. Wavelets Multiresolut. Inf. Process.*, 12 1450041.

Feichtinger, H.G., Kozek, W., Luef, F., 2009, Gabor analysis over finite Abelian groups, *Appl. Comput. Harmon. Anal.* 26 230–248.

Gabriel, P., 1972, Unzerlegbare Darstellungen I, *Manuscripta Mathematica* 6, 71-103.

Gander, W., 2008, The Singular Value Decomposition, Lecture Notes ETH Zurich.

Ghayour, H., Erfanian, A., Azimi, A., 2018, Some results on the Jacobson graph of a commutative ring, *Rendiconti del Circolo Matematico di Palermo Series* 2 67 No 1, 33-41.

Hafezi, R., Muchtadi-Alamsyah, I., 2021, Different exact structures on the monomorphism categories, *Applied Categorical Structures* Vol 29, 31-68.

Hammons Jr., A.R., Vijay Kumar, P., Calderbank, A.R., Sloane, N.J.A., Sole, P., 1994, The Z4 linearity of Kerdock Preparata Goethals and related codes, *IEEE Trans. Information Theory* 40, 301-319.

Hamonangan, Y.Y., Muchtadi-Alamsyah, I., 2022, Skew polynomial ring of the ring of Morita context, *Jordan Journal of Mathematics and Statistics* 15 (3A), 541-557.

Happel, D., 1988, Triangulated categories in the representation theory of finite dimensional algebras. London Mathematical Society Lecture Notes Series 110. Cambridge University Press, Cambridge.

Hiraoka, Y., Ike, Y., Yoshiwaki, M., 2022, Algebraic stability theorem for derived categories of zigzag persistence modules, *Journal of Topology and Analysis* https://doi.org/10.1142/S1793525322500091

Humaira, S., 2023, Generalisasi graf Jacobson atas gelanggang, Disertasi Program Doktor, Institut Teknologi Bandung.

Humaira, S., Astuti P., Muchtadi-Alamsyah, I., Erfanian, A., 2020, The matrix Jacobson graph of fields, *J. Phys. Conf Series,* Vol. 1538, 012008.

Humaira, S., Astuti P., Muchtadi-Alamsyah, I., Erfanian, A., 2022, The matrix Jacobson graph of finite commutative rings, *Electronic Journal of Graph Theory and Applications,* Vol 10 No 1, 181-197.

Irwansyah, 2016, Konstruksi kode siklik miring atas aljabar atas lapangan hingga, Disertasi Program Doktor, Institut Teknologi Bandung.

Irwansyah, Barra, A., Dougherty, S.T., Muchlis, A., Muchtadi-Alamsyah, I., Sole, P., Suprijanto, D., Yemen, O., 2016, Theta$_s$-cyclic codes over A_k, *International Journal of Computer Mathematics: Computer System Theory* , Vol 1 Issue 1, 14-31

Irwansyah, Muchtadi-Alamsyah, I., Yuliawan, F., 2019, Permutation LDPC codes in McEliece cryptosystem, AIP Conf. Proc 2192, 040005.

Irwansyah, Suprijanto, D., 2018, Structure of linear codes over the ring Bk, *J of Applied Mahtematics and Computing* Vol 58, 755-775.

Irwansyah, Muchtadi-Alamsyah, I., Muchlis, A., Barra, A., Suprijanto, 2021, A note on the construction and enumeration of Euclidean self-dual skew-cyclic codes, *Applicable Algebra in Engineering, Communication and Computing* 32, 345-358.

Irwansyah, Muchtadi-Alamsyah, I., Yuliawan, F., 2021, A construction of MDS involutory matrics using MDS self-dual codes: a preliminary result, *J. Phys. Conf. Series* 1722, 012030.

Irwansyah, Suprijanto, D., 2023, Linear codes over a general infinite family of rings and MacWilliams-type relations, *Discret Mathematics Letter* 11, 53-50.

Jagan, A., Nagarajan, V., 2013, A comprehensive performance investigation on ingenious ECC co-processor architecture for different multipliers, *Przeglad Elektrotechniczny* 89 No 8, 157-161.

Kariman, D., Irawati, Muchtadi-Alamsyah, I., 2019, Modul herediter atas aljabar lintasan Leavitt dari graf A-tak hingga, *Jurnal Matematika Integratif* Vol 15 No 1, 63-68.

Kariman, D., Irawati, Muchtadi-Alamsyah, I., 2021, The U-projective resolution of simple modules over Leavitt path algebras, AIP Conf Proc 2192, 040006.

Keller, B., 1993, A remark on tilting theory and DG-algebras, *Manuscripta Mathematica* 79, 247-253.

Khoo, K., Peyrin, T., Poschmann, A.Y., and Yap, H.,2014, FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison, Cryptographic Hardware and Embedded Systems (CHES 2014), LNCS, vol. 8731, 433-450.

Koblitz, N., 1987, Elliptic Curve Cryptosystem, *Mathematics of Computation* 48, 203-209.

Koenig, S., Zimmermann, A., 1998, Derived equivalences for group rings, Lecture Notes in Mathematics 1685, Springer-Verlag, Berlin.

Laha, A., 2019, Topological Data Analysis, slide presentation, available at https://www.cs.columbia.edu/~suman/avik_slides.pdf

Li, X., Chong, A. W., 2017, The technology and economic determinants of cryptocurrency exchange rates: The case of Bitcoin, *Decision Support Systems* 95, 49-60.

Lindell, E., 2017, Decomposition Methods for Representations of Quivers appearing in Topological Data Analysis, Project, Royal Inst of Technology (KTH) Sweden.

Mahatma, Y., Muchtadi-Alamsyah, I., 2017, Construction of U-extension module, AIP Conf. Proc, 1867, 020025-1 – 020025-9.

Marubayashi, H., Muchtadi-Alamsyah, I., Ueda, A., 2013, Skew Polynomial Rings which are Generalized Asano Prime Rings, *Journal of Algebra and Its Applications* vol 12 No 7, 1350024, 8 pages.

Miller, V.S., 1985, Use of Elliptic Curves in Cryptography, Advances in Cryptology CRYPTO 85, LNCS 218, 417-426.

Muchtadi-Alamsyah, I., 2005, Homomorphisms of complexes via homologies, *Journal of Algebra* 294, 321-345.

Muchtadi-Alamsyah, I., 2008, Braid action on derived category of Nakayama algebras, *Communication in Algebra* Vol 36 Issue 07, 2455-2569.

Muchtadi-Alamsyah, I., Yuliawan, F., Muchlis, A., 2012, Finite Field Basis Conversion and Normal Basis in Characteristic Three, in Advances in Algebraic Structures, Proceeding International Conference in Algebra, World Scientific, 439-447.

Muchtadi-Alamsyah, I., Yuliawan, F., 2013, Basis Conversion in Composite Field, *International Journal of Mathematics and Computation* **vol 16** No 2, 11-17.

Muchtadi-Alamsyah, I., Ardiansyah, T., Carita, S.S., 2013, Pollard Rho Algorithm for Elliptic Curves over GF(2^n) with Negation Map, Frobenius Map and Normal Basis, *Far East Journal of Mathematical Sciences*, Special Volume, No 4, 385-402.

Muchtadi-Alamsyah, I., Susantio, D.R., Utomo, T.A., 2016 *Implementasi Pengiriman Pesan dan Serangan pada Kriptografi Kurva Eliptik,* dalam Bunga Rampai FORMIND, 37-47, Penerbit ITB.

Muchtadi-Alamsyah, I., Utomo, T.A., 2017, Implementation of Pollard Rho over binary fields using Brent Cygle Algorithm, J of Physics Conf. Series 893, 012043.

Muchtadi-Alamsyah, I., Sayyidatunnisa, N.U., Samra, R., 2018, Survey on finding indecomposable quiver representation for algebra of finite representation type, *Asia Mathematika* Vol 2 Issue 2, 73-87.

Muchtadi-Alamsyah, I., Irwansyah, 2019,Asymmetric Quantum Codes from Skew Cyclic Codes over B_1, AIP Conference Proceedings 2192, 040008.

Muchtadi-Alamsyah, I., Imdad, M.T., Sutikno, S., 2020, Group Signature Based Ethereum Transaction, *International Journal on Electrical Engineering and Informatics* Vol 12 No 1, 19-32.

Muchtadi-Alamsyah, I., Tama, Y.B.W., 2020, Implementation of Elliptic Curve25519 in Cryptography, Book Chapter Theorizing STEM Education in 21st Century doi: 10.5772/intechopen.88614.

Muchtadi-Alamsyah, I., Palu, Y., 2021, The relation between tau_n-tilting modules and n-term silting complexes, *Int. J. Maths and Comp. Sciences* Vol 16 No 3, 885-896.

Muchtadi-Alamsyah, I., Irwansyah, Barra, A., 2022, Generalized Quasi-Cyclic Codes with Arbitrary Block Lengths, *Bull. of Malay Math. Sci. Soc.* 45, 1383-1407.

Muchtadi-Alamsyah, I., Heriawan, M.N., Rachmaputri, G., Rahmadiantri, E., Lawiyuniarti, M.P., 2022 Application of Three-Dimensional Direct Least Square Method for Ellipsoid Anisotropy Fitting Model of Highly Irregular Drill Hole Patterns, *Applied Sciences* 12, 7848.

Nasiri, M., Erfanian, A., Ganjali, M., Jafarzadeh, A., 2016, g-noncommuting graph of some finite groups, *J Prime Research Math* 12, 16-23.

Nasiri, M., Erfanian, A., Ganjali, M., Jafarzadeh, A., 2017, Isomorphic g-noncommuting graph of some finite groups, *Publ Math Debrecen* 91, 1-2.

Nasiri, M., Erfanian, A., Farawi, Y.A., Muchtadi-Alamsyah, I., 2020, A kind of graph associated to a fixed element and a subgroup of group, *Southeast Asian Bull. of Maths* Vol 44, 813-818.

Nopendri, Muchtadi Alamsyah, I., Suprijanto, D., Barra, A., 2021, Cyclic Codes from A Sequence over Finite Fields, *European Journal of Pure and Applied Mathematics* Vo. **14 No 3,** 685-694.

Oudot, S.Y., 2015, Persistence Theory: Form Quiver Representations to Data Analysis, Mathematical Surveys and Monographs vol 209, American Math. Society.

Paryasto, M.W., Kuspriyanto, Sutikno, S., Sasongko, A., 2009, Issues in Elliptic Curve Cryptography Implementation, *Internetworking Indonesia Journal* Vol. I No.1, 29-33.

Paryasto, M.W., Rahardjo, B., Muchtadi-Alamsyah, I., Khusyairi, M.H., 2010, Implementation of Polynomial Basis-Optimal Normal Basis I Basis Conversion, *Jurnal Ilmiah Teknik Komputer* Vol.1 no.2, 148-160.

Paryasto, M., Rahardjo, B., Yuliawan, F., I. Muchtadi-Alamsyah, Kuspriyanto, 2012, Composite Field Multiplier based on Look-Up Table for Elliptic Curve Cryptography Implementation, *ITB Journal of Information and Communication Technology* Vol 6 No 1, 63-81.

Rahardjo, B., Kuspriyanto, Paryasto, M., Muchtadi-Alamsyah, I., Yuliawan, F., Nopendri, 2015, Pengantar Kurva Eliptik dan Lapangan Hingga dan Aplikasinya untuk Kriptografi, Penerbit ITB.

Realpe-Munoz, P., Velasco-Medina, J., Adolfo-David, G., 2021, Design of an S-ECIES cryptoprocessor using Gaussian normal bases over GF(2^m), *IEEE Transactions on Very Large Scale Integration (VLSI) Systems* Vol 29 No 4, 9359519, 657-666

Renita, J., Edna, E.N., Asokan, N., 2022, Implementation and performance analysis of elliptic curve cryptography using an efficient multiplier, *Journal of Semiconductor Technology and Science* Vol 22 No 2, 53-60.

Rickard, J., 1991, Derived equivalences as derived functors, *J. London Math. Soc* 43, 37-48.

Rijmen, V., Daemen, J., Preneel, B., Bosselaers A., and Win, E. D., 1996, The cipher SHARK, In 3rd Fast Software Encryption Workshop, LNCS, 1039, 99-111.

Risnawita, Irawati, Muchtadi-Alamsyah, I., 2021, Primeness of simple modules over path algebras and Leavitt path algebras, *Khayyam J. Math.* Vol 7 no 2, 219-231.

Rosdiana, S., Muchtadi-Alamsyah, I., Suprijanto, D., Barra, A., 2021, On Linear Codes over $Z_2^m + vZ_2^m$, *IAENG International Journal of Applied Mathematics* Vol 51 No. 1, 133-141.

Saleh, K., Astuti, P., Muchtadi-Alamsyah, I., 2016, On the structure of finitely generated primary modules, *JP Journal of Algebra, Number Theory and Applications* Vol 38 Issue 5, 519-533.

Santika, A.P., Muchtadi-Alamsyah, I., 2012, The p-regular subspaces of symmetric Nakayama algebras and algebras of dihedral and semi-dihedral type, *JP Journal of Algebra Number Theory and Applications* Vol 27 Number 2, 131-142.

Schaps, M., Zakay-Illouz, E., 2002, Braid group action on the refolded tilting complex of the Brauer star algebra, Proceedings ICRA IX (Beijing) vol. 2, 434-449.

Scholler, F., Blanke, M., Plenge-Feidenhans, M., Nalpantidis, L., 2020,Vision-based Object Tracking in Marine Environments using Features from Neural Network Detections, IFAC-PapersOnLine 53(2), 14517–14523. 21st IFAC World Congress.

Strang G., Nguyen, T., 1996, Wavelets and Filter Banks. Wellesley-Cambridge Press, Wellesley, 1996.

Su, Y., Yang, B.L., Yang, C., He, J.Y., 2021, High flexible hardware and instruction of composite Galois field multiplication targeted at symmetric crypto processor, *Journal of Ambient Intelligence Humanized Computing* Vol 12 No 7, 7727-7743.

Suprijanto, D., Tang, H.C., 2022, Quantum codes constructed from cyclic codes over a finite non-chain ring, *IAENG Int. J. of Comp Sciences* Vol 49 No. 3.

Susantio, D.R., Muchtadi-Alamsyah, I., 2016, Implementation of Elliptic Curve Cryptography in Binary Field, Journal of Physics Conference Series 710, 012022.

Suwastika, E., Muchtadi-Alamsyah, I., Garminia,H., Irawati, 2015, Ore Extension over Generalized Asano Prime Rings, *International Journal of Applied Mathematics and Statistics* vol 53 No 4, 116-124.

Syarifuddin, A., Muchtadi-Alamsyah, I., 2018, Construction of Cyclic Codes over Ternary Fields from Periodic Sequences, *Southeast Asian Bulletin of Mathematics*, vol 42, 773-780.

Takeuchi, H., 2021, The Persistent Homology of a Sampled Map: from a Viewpoint of Quiver Representations, *J. Appl Comp. Top* 5,179-213.

Tolue, B., Erfanian, A., 2013, Relative non-commuting graph of a finite group, *J. Algebra Appl* Vol 12, 1250157-1-12.

Tolue, B., Erfanian, A., Jafarzadeh, A., 2014, A kind of noncommuting graph of finite groups, *J.Sci. Islam Rep Iran* Vol 25 No 4, 379-384.

van der Waerden, B.L., 1985, A history of algebra: from al-Khwarizmi to Emmy Noether. Springer Verlag, Berlin.

Vincent, O.R., Okediran, T.M., Abayomi-Alli, A.A., Adeniran, O.J., 2020, An identity-based cryptography for mobile payment security, *SN Computer Science* Vol 1 No 2, 112.

Verdier, J.L., 1996, Des categories derivees des categories abeliennes. *Asterisque* No 239.

Volkov, Y., Zvonareva, A., 2007, Derived Picard groups of selfinjective Nakayama algebras, *Manuscripta Mathematica* Vol 152 Issue 1-2, 199-222.

Wanditra, L.C., Muchtadi-Alamsyah, I., Rachmaputri, G., 2020, Wave packet transform on finite abelian group, *Southeast Asian Bulletin of Mathematics* Vol 44 853-857.

Wanditra, L.C., Muchtadi-Alamsyah, I., Rachmaputri, G., Irawan, D.E., 2021, Forecasting total suspended solid using wavelet ARIMA model, AIP Conference Proceedings **2423,** 020020.

Wardati, K., Wijayanti, I.E., Wahyuni, S., 2014, On primeness of path algebras over a unital commutative ring, *JP Journal of Algebra Number Theory and Appl.* Vol 34 No 2, 121-138.

Wardhana, I.G.A.W., Astuti, P., Muchtadi-Alamsyah, I., 2016, On almost prime submodules of a module over principal ideal domain, *JP Journal of Algebra Number Theory and Appl.,* Vol 38 Issue 2 (2016).

Zhang, Q., Wang, Y., 2020, Construction of composite mode of sports education professional football teaching based on sports video recognition technology, in 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), 1889–1893.

Zvonareva, A., 2015, Mutations and the derived Picard group of the Brauer star algebra, *Journal of Algebra* Vol 433, 270-299.

Zvonareva, A., 2015, Two term tilting complexes over Brauer tree algebras, *Journal of Mathematical Sciences* Vol 202 Issue 3, 333-345.

CURRICULUM VITAE

Nama	:	Prof. Dr. Muchtadi Intan Detiena, S.Si., M.Si.
Tempat/tgl lahir	:	Bogor/ 25 November 1975
Kel. Keahlian	:	Aljabar
Alamat Kantor	:	Jl. Ganesha No.10 Bandung
Nama Suami	:	Dr. Andry Alamsyah, S.Si., M.Sc.
Nama Anak	:	1. Sandra Samara Alamsyah 2. Marita Almira Sarah Alamsyah

I. RIWAYAT PENDIDIKAN

- Docteur de Mathematiques (Dr.), Universite de Picardie Jules Verne, Amiens, Prancis, 2001-2004
- Diplome d'Etudes Approfondies (D.E.A.) Methodes Algebriques, Universite de Picardie Jules Verne, Amiens, Prancis, 2000-2001
- Magister Sains (M.Si.), Matematika, Institut Teknologi Bandung, 1997-1999
- Sarjana Sains (S.Si.), Matematika, Institut Teknologi Bandung, 1993-1997
- SMA Regina Pacis Bogor, 1990-1993
- SMP Regina Pacis Bogor, 1987-1990
- SD Budi Mulia Bogor, 1982-1987
- Ecole d'Assas Montpellier, Prancis 1980-1982

II. RIWAYAT KERJA DI ITB

- Staf Pengajar Matematika FMIPA ITB, 1998-sekarang
- Ketua Program Studi Magister Matematika dan Doktor Matematika ITB, 2016-2020
- Anggota Senat FMIPA ITB Periode 2013-2018
- Anggota Tim Pengembangan Program Studi Sarjana Aktuaria FMIPA ITB 2017
- Anggota Tim Akreditasi Internsional Prodi di Lingkungan FMIPA ITB 2014-2015

III. RIWAYAT KEPANGKATAN

- Penata Muda, III/a — 1 Februari 1998
- Penata, III/c — 1 Oktober 2008
- Penata Tk. 1, III/d — 1 April 2013
- Pembina, IV/a — 1 April 2015

IV. RIWAYAT JABATAN FUNGSIONAL

- Asisten Ahli Madya — 1 Juni 1999
- Asisten Ahli — 1 Januari 2001
- Lektor — 1 April 2008
- Lektor Kepala — 1 Desember 2012
- Profesor/Guru Besar — 1 November 2022

V. KEGIATAN PENELITIAN

- Graduate School Grant DGHE (Hibah Pascasarjana DIKTIRISTEK) 2023: Multiparty Computation based on Secret Sharing Schemes and Skew Polynomial Rings (principal investigator), Circulant Matrices as Weight Matrices on Transformer (principal investigator)
- ERCE Postdoc Grant 2023: Graph Associated to Lie Algebras (principal investigator, postdoc fellow: Dr . Afsaneh Shamsaki)
- ITB Research Grant 2023 (P2MI): Gradient Descent using MDS Cyclic Codes (principal investigator), Topological Data Analysis (member), Optimization of Environmental Carrying Capacity with Least Square Method (member)
- ITB Research Grant 2022: Matrix Modification on BERT Transformer Scheme for Natural Language Processing (principal investigator), On Circulant MDS Matrices (principal investigator, P2MI)
- ITB International Research Grant 2021: A Fundamental Research on Computing the Topological Indices of Zero Divisor Graph for a Finite Commutative Ring (principal investigator, in collaboration with Prof. Nor Haniza Sarmin, UTM)
- ITB Research Grant 2021: Algorithm for Security of Cryptocurrency Risk (principal investigator), Derived Category of U-complexes (principal investigator, P2MI)
- Research Grant Bank Indonesia 2021: Stochastic Modeling for Predicting Risk of Stablecoins and Bitcoin (member)

- WCU ITB Postdoc Program 2020: Simple Minded Systems (member, postdoc fellow: Dr. Mohsen Shekari)
- ITB Research Grant 2020: Alpha-noncommuting Graphs from Groups and Automorphism (principal investigator), Graded Modules over Leavitt Path Algebras (principal investigator, P3MI), Neural Network-Based Cryptography (principal investigator, P3MI), Canonical Form and Groebner Basis of Neural Ideal (member, P3MI)
- Outstanding Doctoral Program (PMDSU) 2019-2021: Matrix Jacobson Graph (member)
- Competence Grant DGHE (HIBAH KOMPETENSI DIKTI) 2017-2019: Representation of Leavitt Path Algebras (principal investigator)
- Basic Science Research Grant DGHE (HIBAH RISET DASAR DIKTI) 2019: Skew-Consta-Permutation Code-Based Cryptography (principal investigator)
- ITB Research Grant 2019: Wave Packet Analysis and Its Application in Predicting Total Suspended Solid (principal investigator), On The Representation Theory of Gorenstein Projective Modules over Triangular Matrix Rings (principal investigator, P3MI)
- WCU ITB Postdoc Program 2019: On Nilpotent Groups Associated to an Automorphism (member, postdoc fellow: Dr. Masoumeh Ganjali), g-noncommuting Graph of Finite Groups and Its Generalizations (member, postdoc fellow: Dr. Mahboube Nasiri)
- Asahi Glass Foundation Research Grant August 2018-July 2019: Construction of Hybrid Quantum Codes from Nested Linear Codes (principal investigator)
- ITB Research Grant 2018: Signature Algorithm for Cryptocurrency and Analysis of Bitcoin Investment (principal investigator), Skew-Consta-Permutation Codes over Ring (member, P3MI)
- International Cooperation and Publication Grant DGHE (KERJASAMA LUAR NEGERI DAN PUBLIKASI INTERNASIONAL DIKTI) 2016-2018: Derived Equivalence for Hopf Algebra (principal investigator)
- Outstanding Doctoral Program (PMDSU) Batch 2, 2016-2018: Skew Polynomial Rings over Triangular Matrices (principal investigator)
- ITB Research Grant 2017: Efficient Algorithm for Elliptic Curve Cryptography in Instant Messaging (principal investigator), Generalization of Projective Modules via U-Exact Sequences (member),

Code-Based Cryptography with Skew Cyclic Codes (principal investigator, P3MI), Optimal Least Square Fitting (member, P3MI)

- ASEA-UNINET (ASEAN-European Academic University Network) 2016, ITB - University of Graz Joint Research: Algebra via Combinatorial Geometry (principal investigator)
- ITB Research Grant 2016: Derived Equivalence with U-Tilting Modules (principal investigator)
- WCU Postdoc Program 2016: Gorenstein Homological Algebra with respect to Semidualizing Modules (member, postdoc fellow: Dr. Udhayakumar Ramalingan)
- Decentralization Grant DGHE (HIBAH DESENTRALISASI DIKTI) 2015-2016: Characterization of prime Dedekind modules and applications of modules in coding theory (principal investigator), Variety of U-complexes (member)
- ITB Research Grant 2015: Derived Equivalence of U-Complexes (principal investigator)
- Asahi Glass Foundation Research Grant August 2014- July 2015: Implementation Of Accelerated Pollard RHO For Security Of Elliptic Curve Cryptography (principal investigator)
- Decentralization Grant DGHE (HIBAH DESENTRALISASI DIKTI) 2014: Almost prime and strongly prime submodules of a finitely generated module over principal ideal domain (member), Geostatistic Modelling (member)
- ITB Research Grant 2014: Skew Polynomial Rings in Coding Theory (principal investigator), Network Hardening Model and Simulation (member)
- STIC-ASIE 2013-2014 Project (sciences et technologies de lɒnformation et de la communication), financed by the French Ministry of Foreign Affairs and linking the LAMFA for France, ITB and UGM for Indonesia, Beijing Normal University and East China Normal University for China (Indonesian coordinator)
- ITB Research Grant 2013: Generalization of Dedekind Prime Rings and HNP Rings (principal investigator), Noise-Based Stego-ECC (member), Normal Basis in Codes over Finite Rings (member), Multiple Attack Graph Based Security Metrics for Network Security (member)

- Asahi Glass Foundation Research Grant August 2012- July 2013: Accelerating Parallelized Pollard Rho to Identify Weak Class Elliptic Curves (principal investigator)
- Competence Grant DGHE 2010-2012: Efficient Algorithms for Elliptic Curve Cryptography based on Composite Field (member)
- Competitive Grant (HIBAH BERSAING) 2011-2012: On Blocks with Commutative Defect Group (principal investigator)
- ITB Research Grant 2011: Nakayama Algebras with Mutations (principal investigator)
- Outstanding Doctoral Fellowship IMHERE 2011: Finite Rings in Cryptography and Coding Theory, Batch III (member)
- Graduate Grant (HIBAH PASCASARJANA) 2009-2011: Efficient Algorithms for Determining Suitable Elliptic Curves for Cryptography (member)
- Fundamental Grant (HIBAH FUNDAMENTAL) 2009-2010: On Path Algebras and Path Coalgebras (principal investigator)
- ITB Research Grant 2010: Polynomial Rings over HNP Rings (member), Skew Polynomial Rings over Dedekind Domain (member)
- Outstanding Doctoral Fellowship IMHERE 2010: Complex Projective Varieties and Polydule Varieties, Batch II 2010 (principal investigator), Invariance of Subalgebra of Center of Group Algebras, Batch I 2010 (member)
- ITB Research Grant 2009: Identification of Weak Class Elliptic Curves for Security of Cryptography (principal investigator), Characterization of Prime and Maximal Ideal in Skew Polynomial Ring over Dedekind Domain (member)
- RISTEK Grant 2008-2009: Using the Algebra of Hypergraphs for the Reconstruction of Phylogenetic Trees (member)

VI. PUBLIKASI

A. Dalam jurnal internasional (*selected*)

- F.Zaidan, **I.Muchtadi-Alamsyah**, *Simulation of Modular Exponential Circuit via Quantum Fourier Transform in Qiskit,* Kongzhi yu Juece/Control and Decision **38** Issue 03 2023, 1183-1195.
- Y.Y.Hamonangan, **I.Muchtadi-Alamsyah**, *Skew polynomial ring of the ring of Morita context,* Jordan Journal of Mathematics and Statistics **15 (3A)** 2022, 541-557.

- **I. Muchtadi-Alamsyah**, M.N. Heriawan, G. Rachmaputri, E. Rahmadiantri, M.P. Lawiyuniarti, *Application of Three-Dimensional Direct Least Square Method for Ellipsoid Anisotropy Fitting Model of Highly Irregular Drill Hole Patterns,* Applied Sciences **2022** (12) 7848.
- I. Adhiguna, I.S.N. Arifin, F.Yuliawan, **I. Muchtadi-Alamsyah**, *On orthogonal circulant MDS Matrices,* International Journal of Mathematics and Computer Science **17** (4) 2022, 1619-1637.
- M.Ganjali, A.Erfanian, **I.Muchtadi-Alamsyah**, *Finite p-groups which are non-inner nilpotent,* Mathematica **64 (87)** 2022, 75-82.
- S.Humaira, P.Astuti, **I.Muchtadi-Alamsyah**, A.Erfanian, *The Matrix Jacobson Graph of Finite Commutative Rings,* Electronic Journal of Graph Theory and Applications **10** (1) 2022, 181-197.
- **I. Muchtadi-Alamsyah**, Irwansyah, A.Barra, *Generalized Quasi-Cyclic Codes with Arbitrary Block Lengths,* Bull. of Malay Math. Sci. Soc. 45 2022 1383-1407
- K. Syuhada, A. Hakim, D. Suprijanto, **I. Muchtadi-Alamsyah**, L.Arbi, *Is Tether a safe haven of safe haven amid COVID-19? An assessment against Bitcoin and oil using improved measures of risk,* Resources Policy 2022 Article number 103111
- M. Parimala, **I. Muchtadi-Alamsyah**, M. Al-Tahan, *On Picture Fuzzy Ideals of Near-Rings,* International Journal of Fuzzy Logic and Intelligent Systems **21(3)** (2021) 259-268.
- Nopendri, **I. Muchtadi Alamsyah**, D. Suprijanto, A. Barra, *Cyclic Codes from A Sequence over Finite Fields*, European Journal of Pure and Applied Mathematics **14 (3)** (2021) 685-694
- **I.Muchtadi-Alamsyah**, Y.Palu, *The Relation between tau$_n$-Tilting Modules and n-term Silting Complexes*, Int. Journal of Maths and Computer Sciences **16 (3)** (2021) 885-896.
- Risnawita, Irawati**, I.Muchtadi-Alamsyah**, *Primeness of Simple Modules over Path Algebras and Leavitt Path Algebras,* Khayyam J. Math. **7 no 2** (2021), 219-231 DOI: 10.22034/KJM.2021.203331.1578
- Irwansyah, **I.Muchtadi-Alamsyah**, A. Muchlis, A.Barra, D.Suprijanto, *A note on the construction and enumeration of Euclidean self-dual skew-cyclic codes*, Applicable Algebra in Engineering, Communication and Computing **32** (2021) 345-358

- S. Rosdiana, **I.Muchtadi-Alamsyah**, D.Suprijanto, A.Barra, *On Linear Codes over* $Z_2^m + vZ_2^m$, IAENG International Journal of Applied Mathematics **51 (1)** (2021) 133-141
- R. Hafezi, **I. Muchtadi-Alamsyah**, *Different exact structures on the monomorphism categories,* Applied Categorical Structures **29** (2021) 31-68.
- M.Ganjali, A.Erfanian, **I.Muchtadi-Alamsyah**, *Some notes on non-inner nilpotent groups,* Southeast Asian Bulletin of Mathematics **vol 44** (2020) 797-802
- M.Nasiri, A.Erfanian, Y.A.Farawi, **I.Muchtadi-Alamsyah**, *A kind of graph associated to a fixed element and a subgroup of group,* Southeast Asian Bulletin of Mathematics **vol 44** (2020) 813-818
- L.C. Wanditra, **I. Muchtadi-Alamsyah**, G. Rachmaputri, *Wave packet transform on finite abelian group,* Southeast Asian Bulletin of Mathematics **vol 44** (2020) 853-857.
- B. Praba, A. Manimaran, G. Deepa, **I. Muchtadi-Alamsyah**, *A note on principal rough ideals of a rough monoid,* Adv. In Maths: Scientific Journal **vol 9 (9)** (2020), 6855-6861.
- G. Elfiyanti, **I. Muchtadi-Alamsyah**, F.Yuliawan, D.Nasution, *On the Category of Weakly U-Complexes,* European Journal of Pure and Applied Mathematics **vol 13 (2)** (2020) 323-345.
- **I. Muchtadi-Alamsyah**, M.T. Imdad, S.Sutikno, *Group Signature Based Ethereum Transaction,* International Journal on Electrical Engineering and Informatics **vol 12 (1)** (2020) 19-32.
- K. Baur, Y.Mahatma, **I.Muchtadi-Alamsyah**, *The U-Projective Resolution of Modules over Path Algebras of Types An and An~,* Communication of the Korean Mathematical Society **vol 34 (3)** (2019) 701-718
- B.Erfianto, **I.Muchtadi-Alamsyah**, *Stability and Vulnerability of Bird Flocking Behaviour: A Mathematical Analysis,* Hayati Journal of Biosciences **vol 26 (4)** (2019) 179-184.
- R. Udhayakumar, **I. Muchtadi-Alamsyah**, C. Selvaraj, *Some results of* G_C*-flat dimension of modules,* Comment.Math.Univ.Carolin. **vol 60 (2)** (2019) 187-198.
- R. Udhayakumar, **I. Muchtadi-Alamsyah**, *Stability of Gorenstein Graded Flat Modules*, Palestine Journal of Mathematics **vol 8 (2)** (2019) 70-77.

- A. Syarifuddin, **I. Muchtadi-Alamsyah**, *Construction of Cyclic Codes over Ternary Fields from Periodic Sequences,* Southeast Asian Bulletin of Mathematics, **vol 42** (2018) 773-780.
- Irwansyah, A. Barra, **I. Muchtadi-Alamsyah**, A. Muchlis, D. Suprijanto, *Skew-cyclic codes over* B_k, Journal of Applied Mathematics and Computing **vol 57** Issue 1-2 (2018) 69-84
- Irwansyah, **I.Muchtadi-Alamsyah**, A.Muchlis, A.Barra, D. Suprijanto, *Codes over an Infinite Family of Algebras,* Journal of Algebra Combinatorics Discrete Structures and Applications, **vol 4** No. 2 (2017) 131-140.
- B. Erfianto, R.T. Bambang, H. Hindersah, **I. Muchtadi-Alamsyah**, *Design of connectivity preserving flocking using control Lyapunov function,* Journal of Robotic, Vol 2016 (2016),
- Irwansyah, A. Barra, S.T. Dougherty, A. Muchlis, **I. Muchtadi-Alamsyah**, P. Sole, D. Suprijanto, O. Yemen, *Theta*$_S$*-cyclic codes over* A_k, International Journal of Computer Mathematics: Computer System Theory , **Vol 1 Issue 1** (2016) 14-31
- Faisal, **I. Muchtadi-Alamsyah**, *Characterization of Nakayama m-Cluster Tilted Algebras of Type An,* Journal of Indonesian Math Society, **vol 22** No.2 (2016) 93-130.
- B. Erfianto, R.T. Bambang, H. Hindersah, **I. Muchtadi-Alamsyah**, *Convergence analysis of cooperative Q-learning using discrete-time Lyapunov approach,* ICIC Express Letters, **Vol 9** Issue 12 (2015) 3153-3161.
- Irwansyah**, I. Muchtadi-Alamsyah**, A. Muchlis, A.Barra, *Self-Dual Normal Basis of a Galois Ring,* Journal of Mathematics, **vol 2014** (2014) doi:10.1155/2014/258187
- H. Marubayashi, **I. Muchtadi-Alamsyah** and A. Ueda, *Skew Polynomial Rings which are Generalized Asano Prime Rings,* Journal of Algebra and Its Applications **vol 12** No 7 (2013) 1350024, 8 pages.
- Faisal, Irawati and **I.Muchtadi-Alamsyah**, *Auslander-Reiten Quiver of Nakayama Algebra type Dynkin Graph An,* Journal of Mathematical and Fundamental Sciences, **vol 45** No 1 (2013) 1-16.
- Darmajid and **I. Muchtadi-Alamsyah**, *Open Condition on Variety of Complexes,* East West Journal of Mathematics, **vol 15** No 1 (2013) 37-42.
- M. W. Paryasto, B. Rahardjo, F. Yuliawan, **I. Muchtadi-Alamsyah** and Kuspriyanto, *Composite Field Multiplier based on Look-Up Table for Elliptic*

Curve Cryptography Implementation, ITB Journal of Information and Communication Technology **Vol 6** No 1 (2012) 63-81.

- **I.Muchtadi-Alamsyah** and H. Garminia, *Quiver of Bounded Path Algebras and Bounded Path Coalgebras*, ITB J. Sci. **vol 42 A**, No 2 (2010) 153-162
- M.Astuti, Irawati, **I. Muchtadi-Alamsyah**, A.Muchlis, A.Akbar, *Using the Algebra of Hypergraphs for the Reconstruction of Phylogenetic Trees,* International Journal of Tomography and Statistics **vol 12** no F09 (2009) 105-110.
- **I.Muchtadi-Alamsyah**, *Braid action on derived category of Nakayama algebras,* Communication in Algebra **vol 36** No 07 (2008) 2455-2569.
- **I. Muchtadi-Alamsyah**, *Homomorphisms of complexes via homologies*, Journal of Algebra **294** (2005) 321-345.

B. Dalam buku/book chapter

- **I.Muchtadi-Alamsyah**, *Kriptografi Kurva Eliptik dalam Keamanan Pesan Instan dan Mata Uang Virtual,* in Genggam Asa dalam Karsa dan Karya, ITB Press 2023.
- **I.Muchtadi-Alamsyah**, *AI dan Kriptografi sebuah survei*, in Artificial Intelligence di Masa Pandemi, ITB Press, 2021
- **I.Muchtadi-Alamsyah**, Y.B.W. Tama, *Implementation of Elliptic Curve25519 in Cryptography,* in Theorizing STEM Education in 21st Century edited by K.G. Fomunyam, pp 301, Intechopen, UK, 2020 doi: 10.5772/intechopen.88614
- **I.Muchtadi-Alamsyah**, D. Ray Susantio, T.A.Utomo, *Implementasi Pengiriman Pesan dan Serangan pada Kriptografi Kurva Eliptik,* in Bunga Rampai FORMIND edited by K.Wikantika, 37-47, Penerbit ITB, 2016,.
- B. Rahardjo, Kuspriyanto, M. Paryasto, **I. Muchtadi-Alamsyah**, F. Yuliawan, Nopendri, *Pengantar Kurva Eliptik dan Lapangan Hingga dan Aplikasinya untuk Kriptografi,* Penerbit ITB, 2015

VII. PATEN

- Bersama Yuniarti Rahayu, Program Komputer -Super Aritmetika Permainan Edukasi Matematika (No: EC00202289645, 16 November 2022)

VIII. ORGANISASI PROFESI

- Vice President of South East Asian Mathematical Society (SEAMS) 2018-2019, 2020-2021, 2022-2023

- President of Indonesian Mathematical Society (IndoMS) 2016-2018
- Head of Indonesian Algebra Society (Komunitas Peminat Aljabar - KPA) 2011-2018
- Secretary of SEAMS 2014-2015
- Member of Centre International de Mathematiques Pures et Appliquees (CIMPA)
- Member of University Centre of Excellence on Artificial Intelligence ITB
- Member of Indonesian Young Researcher Forum (FORMIND)
- Member of European Mathematical Society (EMS)
- Member of American Mathematical Society (AMS)

IX. PENGHARGAAN

- Adjunct Professor di Vellore Institute of Technology, India (mulai 2023)
- Peneliti terbaik KK Aljabar tahun 2022 dari FMIPA ITB
- Satya Lencana Karya Sapta 20 tahun, Agustus 2020
- Best Paper Award untuk artikel berjudul *Three Dimensional Least-Squares Fitting of Ellipsoids and Hyperboloids* dipresentasikan pada The 1stInternational Conference on Applied & Industrial Mathematics and Statistics, Kuantan, Pahang Malaysia 8-10 Agustus 2017
- Best Paper Award untuk artikel berjudul *Implementation of Elliptic Curve Cryptography in Binary Field*, dipresentasikan pada The 4th International Conference on Science & Engineering in Mathematics, Chemistry and Physics, Bali, 30-31 Januari 2016
- Junior Associate ICTP 2010-2016
- Matsumae Foundation Fellowship untuk pascadoktoral di Tokushima Bunri University, Jepang, Mei-September 2010
- Satya Lencana Karya Sapta 10 tahun, Agustus 2010
- NTNU Research Fellowship untuk pascadoktoral di NTNU, Norwegia, 2005-2006
- EPSRC Research Fellowship dan Leverhulme Trust Visiting Fellowship untuk pascadoktoral (*postdoc*) di University of Leicester, UK, 2004-2005
- Prix Mahar Schutzenberger dari The AFIDES (The Association Franco-Indonesian for Development of Sciences), Juni 2004.

ITB PRESS
Gedung STP ITB, Lantai 1,
Jl. Ganesa No. 15F Bandung 40132
+62 22 20469057
www.itbpress.id
office@itbpress.id
Anggota Ikapi No. 043/JBA/92
APPTI No. 005.062.1.10.2018

Forum Guru Besar
Institut Teknologi Bandung
Jalan Dipati Ukur No. 4, Bandung 40132
E-mail: sekretariat-fgb@itb.ac.id
Telp. (022) 2512532
fgb.itb.ac.id FgbItb FGB_ITB
@fgbitb_1920 Forum Guru Besar ITB

ISBN 978-623-297-325-1
9 786232 973251