RESEARCH ARTICLE • OPEN ACCESS

Konstruksi Lapangan Hasil Bagi dari Daerah Integral sebagai Landasan Aljabar Kriptografi Kurva Eliptik

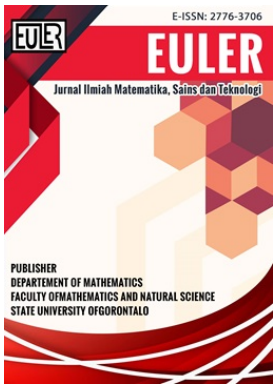
Miftah Sigit Rahmawati dan Muhammad Fadli Hasa

Volume 14, Issue 2, Pages 552–572, August 2026

Diterima 17 Juni 2026, Direvisi 6 Agustus 2026, Disetujui 17 Agustus 2026, Diterbitkan 24 Agustus 2026

To Cite this Article : M. S. Rahmawati dan M. F. Hasa, "Konstruksi Lapangan Hasil Bagi dari Daerah Integral sebagai Landasan Aljabar Kriptografi Kurva Eliptik", *Euler J. Ilm. Mat. Sains dan Teknol.*, vol. 14, no. 2, pp. 552–572, 2026, *https://doi.org/10.37905/euler.v14i2.40284*

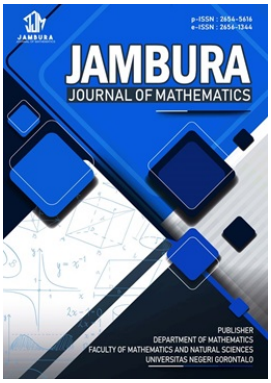
JOURNAL INFO • EULER : JURNAL ILMIAH MATEMATIKA, SAINS DAN TEKNOLOGI



Homepage	:	http://ejurnal.ung.ac.id/index.php/euler/index
Journal Abbreviation	:	Euler J. Ilm. Mat. Sains dan Teknol.
Frequency	:	Three times a year
Publication Language	:	English (preferable), Indonesia
DOI	:	https://doi.org/10.37905/euler
Online ISSN	:	2776-3706
License	:	Creative Commons Attribution-NonCommercial 4.0 International License
Publisher	:	Department of Mathematics, Universitas Negeri Gorontalo
Country	:	Indonesia
OAI Address	:	http://ejurnal.ung.ac.id/index.php/euler/oai
Google Scholar ID	:	QF_r-_gAAAAJ
Email	:	euler@ung.ac.id

JAMBURA JOURNAL • FIND OUR OTHER JOURNALS

Jambura Journal of Biomathematics



Jambura Journal of Mathematics

Jambura Journal of Mathematics Education

Jambura Journal of Probability and Statistics

Euler : Jurnal Ilmiah Matematika, Sains dan Teknologi, Volume 14, Issue 2, pp. 552–572, August 2026 *https://doi.org/10.37905/euler.v14i2.40284*

Research Article

Check for updates

Konstruksi Lapangan Hasil Bagi dari Daerah Integral sebagai Landasan Aljabar Kriptografi Kurva Eliptik

Miftah Sigit Rahmawati[1,*], **Muhammad Fadli Hasa**[1]

[1]*Program Studi Teknik Informatika, Universitas Muhammadiyah Sorong, Papua Barat Daya, 98416, Indonesia*

ARTICLE HISTORY
Diterima 17 Juni 2026
Direvisi 6 Agustus 2026
Disetujui 17 Agustus 2026
Diterbitkan 24 Agustus 2026

KATA KUNCI
Grup abelian
Daerah integral
Lapangan hasil bagi
Kriptografi
Kurva elliptik

KEYWORDS
Abelian group
Field
Integral domain
crypthography
Elliptic curve

ABSTRAK. *Artikel ini mengembangkan suatu kerangka konseptual yang menghubungkan konstruksi lapangan hasil bagi, struktur grup kurva eliptik, dan operasi simbolik Elliptic Curve Cryptography (ECC) sehingga mekanisme matematis ECC dapat dianalisis secara eksplisit sebelum diimplementasikan pada lapangan hingga. Meskipun implementasi praktis ECC menggunakan lapangan hingga, pemahaman mengenai konstruksi lapangan hasil bagi (quotient field) tetap penting sebagai landasan matematis operasi pada kurva eliptik. Artikel ini mengkaji struktur aljabar lapangan hasil bagi $\mathbb{Q}$ dan penerapannya dalam teori kurva eliptik, dengan fokus pada penjumlahan titik dan verifikasi sifat grup abelian dalam himpunan titik kurva $E(\mathbb{Q})$. Pendekatan ini memungkinkan setiap operasi aljabar direpresentasikan secara simbolik (symbolic computation) sehingga mekanisme operasi titik dapat dianalisis secara lebih eksplisit. Pemahaman tersebut membantu menjembatani konsep aljabar abstrak dengan struktur grup pada kurva eliptik. Oleh karena itu, kajian mengenai quotient field memberikan kerangka konseptual yang mendukung pemahaman teoritis terhadap ECC. Penulisan artikel ini bertujuan untuk memberikan pemahaman yang lebih dalam mengenai dasar matematis yang mendasari penggunaan kurva eliptik dalam kriptografi, sebagai langkah membangun framework konseptual dalam menjelaskan ECC.*

ABSTRACT. *This article develops a conceptual framework that connects quotient field construction, elliptic curve group structures, and symbolic operations in Elliptic Curve Cryptography (ECC), enabling the mathematical mechanisms of ECC to be analyzed explicitly before being implemented over finite fields. Although practical implementations of ECC employ finite fields as the basis for arithmetic operations, understanding quotient field construction from an integral domain remains important as the mathematical foundation of elliptic curve operations. This article investigates the algebraic structure of the quotient field $\mathbb{Q}$ and its application to elliptic curve theory, focusing on point addition and the verification of the Abelian group properties of the point set $E(\mathbb{Q})$. This approach allows every algebraic operation to be represented symbolically (symbolic computation), enabling elliptic curve point operations to be analyzed more explicitly. Such an understanding bridges the concepts of abstract algebra and elliptic curve group structures. Therefore, the study of quotient fields provides a conceptual framework that supports the theoretical understanding of ECC. This article aims to provide a deeper understanding of the mathematical foundations underlying the use of elliptic curves in cryptography as a step toward developing a conceptual framework for explaining ECC.*

1. Pendahuluan

Kriptografi modern memanfaatkan konsep-konsep matematika yang kuat dan struktural untuk membangun sistem yang aman. Konsep penting dalam kriptografi adalah struktur aljabar seperti *ring*, daerah integral, dan lapangan. Kriptografi modern mengandalkan teori bilangan dan aljabar abstrak untuk membangun sistem enkripsi yang aman. Dalam kriptografi, konsep lapangan sangat penting, terutama dalam sistem seperti kriptografi eliptik dan kriptografi berbasis lapangan hingga (*finite field cryptography*) [1–7]. Penggunaan kurva eliptik secara

*Penulis Korespondensi.

Email : *miftahsigit.rahmawati@gmail.com* (M. S. Rahmawati)
Homepage : http://ejurnal.ung.ac.id/index.php/euler/index / E-ISSN : 2776-3706

signifikan berkontribusi dalam berbagai algoritma enkripsi, tanda tangan digital, dan protokol keamanan. Secara klasik, setiap daerah integral dapat diperluas menjadi suatu lapangan melalui konstruksi lapangan hasil bagi (*quotient field*), sehingga seluruh operasi aljabar memenuhi aksioma lapangan [8, 9]. Salah satu konsep fundamental dalam aljabar adalah daerah integral, yaitu suatu *ring* komutatif dengan elemen kesatuan yang tidak memiliki pembagi nol. Namun, tidak semua daerah integral memiliki sifat sebagai lapangan, yaitu himpunan dengan operasi penjumlahan dan perkalian di mana setiap elemen tak nol memiliki invers perkalian [10]. Sebagian besar literatur hanya membahas konstruksi *quotient field* sebagai hasil teoritis dalam Aljabar Abstrak tanpa mengaitkannya dengan struktur kurva eliptik maupun mekanisme dasar *Elliptic Curve Cryptography* (*ECC*). Sebaliknya, literatur mengenai kurva eliptik umumnya menjelaskan struktur grup dan operasi titik dengan mengasumsikan keberadaan suatu lapangan tanpa menjelaskan bagaimana lapangan tersebut dikonstruksi dari daerah integral [11, 12]. Berdasarkan kesenjangan tersebut, artikel ini bertujuan memberikan pemahaman yang lebih mendalam mengenai pembentukan lapangan dari daerah integral, khususnya konstruksi lapangan hasil bagi $\mathbb{Q}$ dari $\mathbb{Z}$, serta menganalisis bagaimana struktur tersebut menjadi dasar pembentukan kurva eliptik $E(\mathbb{Q})$. Berbeda dengan penelitian terdahulu yang berfokus pada pembuktian teori *quotient field* atau implementasi *ECC* pada lapangan hingga, penelitian ini menyusun suatu *framework* konseptual yang mengintegrasikan konstruksi *quotient field*, representasi koordinat rasional, validasi kurva melalui diskriminan, analisis operasi *point addition*, serta verifikasi sifat grup *Abelian* menggunakan pendekatan simbolik. Pendekatan ini tidak dimaksudkan untuk menggantikan implementasi *ECC* berbasis *finite field*, tetapi untuk menjelaskan secara eksplisit mekanisme matematis yang mendasari operasi pada kurva eliptik sebelum direpresentasikan dalam bentuk aritmetika modular.

Perkembangan penelitian *ECC* dalam beberapa tahun terakhir juga lebih banyak diarahkan pada peningkatan efisiensi implementasi menggunakan lapangan hingga. Penelitian [13] mengembangkan optimasi algoritma *ECC* untuk meningkatkan performa komputasi, sedangkan [14] mengusulkan arsitektur prosesor *ECC* berkecepatan tinggi pada kurva Weierstrass di atas $GF(p)$. Penelitian-penelitian tersebut menunjukkan bahwa fokus riset modern didominasi oleh optimasi algoritma, efisiensi komputasi, dan implementasi perangkat keras berbasis *finite field*. Dengan demikian, belum ada kajian yang secara sistematis menghubungkan konstruksi *quotient field*, representasi koordinat rasional, struktur grup kurva eliptik, dan operasi titik dalam satu kerangka konseptual sebagai landasan matematis sebelum implementasi *ECC* pada *finite field*.

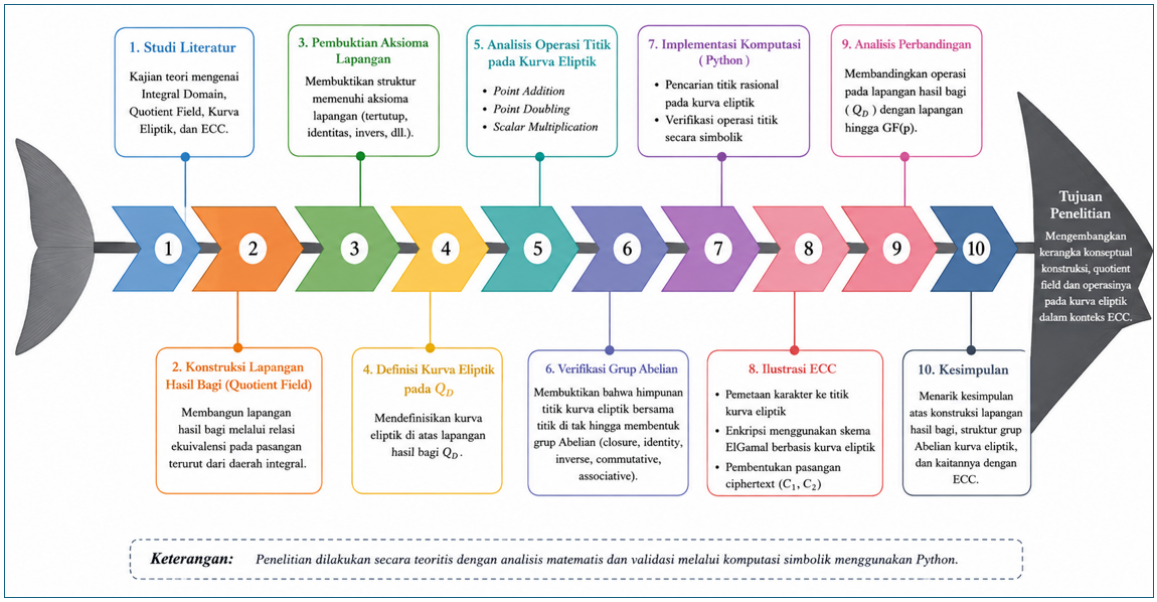
Daerah integral $D = \mathbb{Z}$ yang terdiri dari bilangan bulat menjadi dasar dari konstruksi lapangan $\mathbb{Q}$ yang mencakup bilangan pecahan. Pembentukan lapangan ini mengarah pada struktur aljabar yang lebih luas, yang memungkinkan pembagian dan operasi lain yang lebih kompleks. Dengan membangun lapangan hasil bagi $\mathbb{Q}$, didapatkan struktur yang mendasari operasi dalam kurva eliptik dan memiliki peran penting dalam kriptografi modern. Kriptografi sering bekerja pada lapangan hingga [3]. Analisis terhadap himpunan titik $E(\mathbb{Q})$ memungkinkan proses penjumlahan titik dan pembentukan struktur grup *Abelian* diamati secara simbolik. Dengan memverifikasi bahwa operasi penjumlahan titik memenuhi aksioma grup, dapat dipastikan bahwa kurva eliptik ini valid dan dapat digunakan dalam *ECC*, di mana keamanan sistem terutama bergantung pada kesulitan menyelesaikan *Elliptic Curve Discrete Logarithm Problem* (*ECDLP*) [4], termasuk dalam penerapan skema seperti *Elliptic Curve Digital Signature Algorithm* (*ECDSA*) [5].

Motivasi penulisan artikel ini muncul dari kebutuhan untuk menjelaskan dan menghubungkan matematika dasar dengan aplikasi kriptografi, terutama dengan menghadirkan pen-

dekatan yang secara eksplisit menghubungkan struktur aljabar abstrak dalam dunia kriptografi melalui kajian kurva eliptik dan pengembangan pemahaman yang lebih dalam mengenai konstruksi lapangan hasil bagi $\mathbb{Q}$. Berbeda dengan literatur sebelumnya, melalui pendekatan tersebut, artikel ini tidak hanya menjelaskan konstruksi matematis lapangan hasil bagi dari daerah integral, tetapi juga menghubungkannya dengan struktur kurva eliptik dalam suatu kerangka konseptual yang utuh. Artikel ini memberikan kerangka konseptual yang menghubungkan konstruksi *quotient field* dengan operasi simbolik pada kurva eliptik sebagai media untuk memahami struktur aljabar *ECC*. Kontribusi penelitian ini diharapkan dapat memperkuat pemahaman teoritis mengenai hubungan antara Aljabar Abstrak dan *ECC*, sekaligus menjadi dasar konseptual bagi pengembangan analisis simbolik, pembelajaran matematika kriptografi, dan penelitian lanjutan mengenai struktur aljabar kurva eliptik.

2. Metode

Penelitian ini bersifat teoretis-konseptual dengan dukungan eksperimen simbolik. Penulisan ini dilakukan berdasarkan studi literatur berupa buku-buku yang berhubungan dengan daerah integral, grup, dan lapangan. Diawali dengan mengingat definisi *ring* dan lapangan, selanjutnya membentuk lapangan hasil bagi dari daerah integral dengan mendefinisikan himpunan pasangan serta menelaah struktur aljabar kurva eliptik pada suatu lapangan. Penelitian ini juga menganalisis struktur kurva eliptik pada Q_D dengan menyusun operasi penjumlahan titik $P + Q$ dan penggandaan $2P$, serta memverifikasi sifat grup *Abelian* dari himpunan titik $E(Q_D)$, termasuk keberadaan identitas dan invers. Selanjutnya, penelitian ini mencakup implementasi numerik untuk memvalidasi konsep-konsep yang dibahas. Metode penelitian digambarkan dalam *workflow* pada Gambar 1.



Gambar 1. *Workflow* penelitian.

3. Hasil dan Pembahasan

Bagian ini menyajikan hasil kajian teoretis dan analisis matematis mengenai konstruksi lapangan hasil bagi dari suatu daerah integral, serta penerapannya pada kriptografi kurva eliptik. Pembahasan diawali dengan studi literatur konseptual yang menguraikan teori dasar mengenai daerah integral, lapangan, dan kurva eliptik sebagai landasan penelitian. Selanjutnya, dibahas proses konstruksi teoretis lapangan hasil bagi beserta pembuktian sifat-sifat alja-

barnya sehingga diperoleh suatu struktur lapangan yang memenuhi aksioma-aksioma dasar. Berdasarkan struktur tersebut, analisis terhadap kurva eliptik dilakukan dengan mendefinisikan lapangan bilangan rasional, dilanjutkan operasi penjumlahan titik, penggandaan titik (*point doubling*), serta verifikasi sifat grup Abelian yang menjadi dasar matematis ECC. Sebagai bentuk validasi konseptual, pembahasan diakhiri dengan analisis numerik menggunakan implementasi komputasi untuk menunjukkan kesesuaian antara hasil teoretis dan operasi aritmetika pada kurva eliptik.

3.1. Landasan Konseptual

Kriptografi modern dibangun di atas berbagai konsep matematika yang saling berkaitan, terutama teori bilangan, aljabar abstrak, dan geometri aljabar. Struktur aljabar seperti *ring*, *integral domain*, dan *field* merupakan fondasi yang memungkinkan operasi aritmetika dilakukan secara konsisten dalam berbagai sistem kriptografi [15]. Dalam konteks tersebut, ECC berkembang sebagai salah satu skema kriptografi kunci publik yang memberikan tingkat keamanan tinggi dengan ukuran kunci relatif kecil dibandingkan sistem kriptografi klasik [3, 4]. Berbagai standar internasional, seperti NIST SP 800-186 [7], juga menetapkan bahwa implementasi praktis ECC menggunakan kurva eliptik yang didefinisikan pada *finite field* sebagai dasar operasi aritmetika.

Secara matematis, operasi pada ECC tidak dapat dipisahkan dari konsep lapangan (*field*). Literatur Aljabar Abstrak menjelaskan bahwa setiap *integral domain* dapat diperluas menjadi suatu lapangan melalui konstruksi *quotient field* atau *field of fractions*, sehingga setiap elemen tak nol memiliki invers perkalian [8, 16, 17]. Konstruksi ini merupakan hasil klasik dalam Aljabar Abstrak dan menjadi dasar bagi berbagai pengembangan teori aljabar komutatif. Namun, pembahasan tersebut umumnya berhenti pada pembentukan struktur lapangan tanpa mengaitkannya dengan pembentukan kurva eliptik maupun aplikasi pada kriptografi.

Di sisi lain, teori kurva eliptik berkembang sebagai cabang matematika yang menjelaskan bagaimana himpunan titik pada suatu kurva membentuk grup Abelian melalui operasi penjumlahan titik (*point addition*) dan penggandaan titik (*point doubling*) [11, 12, 15]. Penelitian [11] menitikberatkan pada aspek aritmetika kurva eliptik, sedangkan [12] menghubungkan teori tersebut dengan penerapan pada kriptografi berbasis kurva eliptik. Meskipun demikian, kedua referensi tersebut mengasumsikan keberadaan suatu lapangan sebagai domain koordinat tanpa membahas bagaimana lapangan tersebut dibangun dari suatu daerah integral melalui konstruksi *quotient field*.

Perkembangan penelitian terbaru mengenai ECC lebih banyak diarahkan pada peningkatan efisiensi implementasi. Penelitian [5] membahas optimasi implementasi perangkat lunak ECC, sedangkan [18] mengembangkan percepatan operasi *scalar multiplication* pada *prime field*. Penelitian yang lebih mutakhir juga menunjukkan kecenderungan serupa. Penelitian [13] mengusulkan optimasi algoritma ECC untuk meningkatkan performa komputasi, sementara [14] mengembangkan arsitektur prosesor berkecepatan tinggi pada kurva Weierstrass di atas GF(p). Seluruh penelitian tersebut memperlihatkan bahwa fokus utama riset ECC modern berada pada optimasi algoritma, efisiensi komputasi, dan implementasi perangkat keras berbasis *finite field*, bukan pada penguatan fondasi matematis pembentukan struktur aljabarnya.

Sementara itu, beberapa penelitian mulai mengkaji aspek formal dari struktur matematika ECC. Penelitian [19] menyajikan pembuktian formal hukum grup pada kurva Weierstrass menggunakan pendekatan *formal verification*, sedangkan [20] menunjukkan bahwa pengembangan skema kriptografi modern, termasuk kriptografi berbasis isogeni, tetap bergantung pada pemahaman mendalam terhadap struktur matematika kurva eliptik. Akan tetapi,

penelitian-penelitian tersebut tetap memulai analisis dari kurva eliptik yang telah terdefinisi pada suatu lapangan dan belum menghubungkan proses konstruksi lapangan hasil bagi dengan struktur grup kurva eliptik secara konseptual.

Berdasarkan kajian literatur tersebut, masih terdapat kesenjangan penelitian (*research gap*) berupa belum adanya kajian yang mengintegrasikan konstruksi *quotient field*, *embedding integral domain*, validasi kurva melalui diskriminan, struktur grup Abelian, verifikasi komputasi simbolik, dan mekanisme dasar operasi ECC ke dalam satu kerangka konseptual yang utuh. Sebagian besar penelitian hanya membahas salah satu aspek, yaitu teori *quotient field*, teori kurva eliptik, atau implementasi ECC pada *finite field*, tanpa menjelaskan hubungan konseptual antarbagian tersebut.

Oleh karena itu, penelitian ini tidak bertujuan mengembangkan algoritma ECC baru ataupun menggantikan implementasi berbasis *finite field*. Kontribusi utama penelitian ini adalah menyusun suatu *framework* konseptual yang menghubungkan konstruksi *quotient field* dari daerah integral, proses *embedding* ke dalam Q_D, pembentukan kurva eliptik $E(Q_D)$, validasi kurva menggunakan diskriminan, analisis operasi *point addition* dan *point doubling*, verifikasi sifat grup Abelian melalui pendekatan simbolik, serta ilustrasi komputasi menggunakan Python. *Framework* ini diharapkan dapat menjembatani teori Aljabar Abstrak dengan dasar matematis ECC, sehingga memberikan pemahaman yang lebih sistematis mengenai mekanisme aljabar yang mendasari implementasi ECC.

3.2. Konstruksi Lapangan Hasil Bagi sebagai Fondasi Struktur Kurva Eliptik

Didefinisikan kurva eliptik secara umum [21]

$$E : y^2 = x^3 + ax + b. \tag{1}$$

Dalam teori kurva eliptik, terdapat titik tak hingga $\mathcal{O}$ yang dianggap sebagai "titik di ujung" dari kurva, secara geometris dapat dibayangkan sebagai titik "di tak hingga" dalam bidang koordinat. Dengan demikian, berlaku definisi

$$\forall P \in E, \qquad P + \mathcal{O} = P. \tag{2}$$

Dari pers. (1) didapatkan

$$y = \sqrt{x^3 + ax + b},$$

yang merupakan kurva yang simetris terhadap sumbu horizontal x. Titik potong antara kurva dan sumbu x dicari dengan menggunakan diskriminan dari persamaan kubik

$$x^3 + ax + b = 0. \tag{3}$$

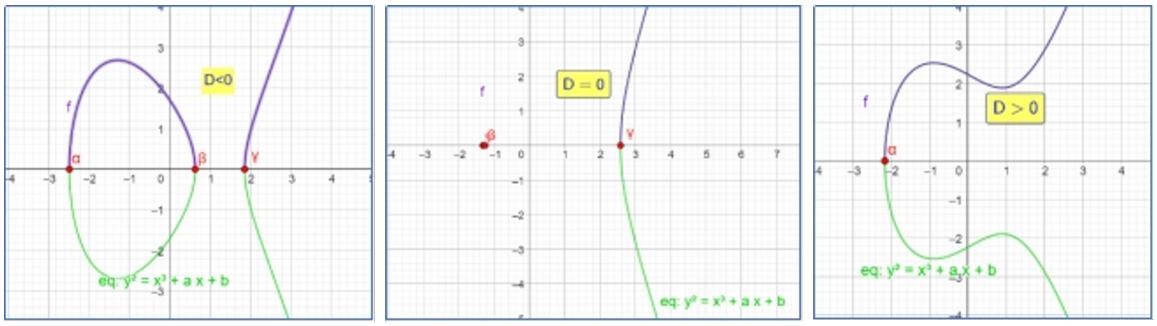
Dengan menggunakan Metode Cardano [22] dalam penyelesaian persamaan kubik dalam bentuk akar real atau kompleks, diskriminan dari pers. (3) dituliskan sebagai

$$\Delta_c = -4a^3 - 27b^2. \tag{4}$$

Berdasarkan nilai diskriminan tersebut, berlaku:

- Jika $\Delta_c > 0$, maka pers. (3) memiliki tiga akar real berbeda, α, β, dan γ.
- Jika $\Delta_c = 0$, maka pers. (3) memiliki tiga akar real dengan setidaknya dua akar yang sama.
- Jika $\Delta_c < 0$, maka pers. (3) memiliki satu akar real α dan dua akar kompleks konjugat.

Ketiga kondisi diskriminan tersebut diilustrasikan pada Gambar 2.



Gambar 2. Kurva dengan nilai diskriminan yang berbeda.

Gambar 2 bagian kiri menunjukkan kurva singular yang memiliki dua garis singgung pada titik singular, sedangkan dua gambar berikutnya menunjukkan kondisi lainnya dengan perbedaan bentuk kurva yang disebabkan oleh nilai diskriminan yang berbeda.

Beberapa ketentuan matematis harus dipenuhi agar kurva dapat digunakan dalam konteks kriptografi, sehingga diperlukan uji validitas kurva eliptik. Langkah-langkah untuk menguji validitas kurva eliptik dalam keamanan algoritma kriptografi adalah sebagai berikut.

1. **Memeriksa persamaan kurva.**
   Artikel ini menggunakan persamaan Weierstrass [23] karena dapat digunakan untuk menentukan kesingularan kurva. Dengan demikian, dipastikan persamaan kurva berada dalam bentuk persamaan Weierstrass.
2. **Menghitung diskriminan.**
   Diskriminan kurva eliptik dihitung dengan rumus
   $$\Delta = -16\left(4a^3 + 27b^2\right), \tag{5}$$
   dengan a dan b merupakan parameter dari persamaan kurva eliptik.
   - Jika $\Delta \neq 0$, maka kurva eliptik valid atau nonsingular.
   - Jika $\Delta = 0$, maka kurva eliptik singular dan tidak valid sebagai kurva eliptik untuk operasi grup ECC.
3. **Memeriksa tidak adanya titik singular.**
   Titik singular adalah titik pada kurva yang tidak memiliki gradien atau turunan yang terdefinisi dengan baik. Jika diskriminan Δ tidak sama dengan nol, maka kurva tersebut bebas dari titik singular. Jika kurva memiliki titik singular, kondisi tersebut dapat menyebabkan masalah dalam operasi aljabar pada kurva eliptik, seperti penjumlahan titik dan penerapan algoritma kriptografi.

Uji validitas tersebut memastikan bahwa kurva eliptik yang digunakan memiliki struktur matematika yang kokoh, sehingga mendukung keamanan algoritma kriptografi. Selain itu, agar kurva eliptik dapat digunakan dalam kriptografi secara efisien dan aman [10], nilai a dan b harus dipilih sedemikian rupa sehingga kurva memiliki sifat aljabar yang baik, seperti menghindari serangan matematika yang mungkin terjadi pada kurva tertentu.

Dalam teori Aljabar Abstrak, setiap daerah integral dapat diperluas menjadi suatu lapangan melalui konstruksi *quotient field*. Pembuktian mengenai keberadaan lapangan hasil bagi telah dibahas secara luas dalam literatur klasik Aljabar Abstrak [8, 9, 24]. Oleh karena itu, penelitian ini tidak bertujuan mengembangkan kembali pembuktian tersebut, melainkan memanfaatkan hasil konstruksi tersebut sebagai fondasi matematis untuk membangun representasi koordinat rasional pada kurva eliptik. Dengan demikian, konstruksi *quotient field* diposisikan sebagai langkah awal dalam kerangka konseptual yang menghubungkan daerah integral dengan struktur grup pada kurva eliptik.

Definisi 1. Misalkan D merupakan suatu daerah integral dan $D^* = D \setminus \{0\}$. Didefinisikan

$$Q_D = \left\{ \frac{p}{q} \,\middle|\, (p,q) \in D \times D^* \right\}.$$

Kemudian Q_D dapat dibentuk menjadi lapangan, dengan kata lain membentuk *ring* komutatif dengan elemen kesatuan dan setiap elemen tak nol mempunyai invers. Sebelumnya didefinisikan terlebih dahulu operasi penjumlahan $(+)$ dan operasi perkalian $(\cdot)$ pada Q_D sebagai berikut. Untuk $\frac{p_1}{q_1}$ dan $\frac{p_2}{q_2}$ kelas ekuivalensi di Q_D,

$$\frac{p_1}{q_1} + \frac{dp_2}{q_2} = \frac{p_1q_2 + p_2q_1}{q_1q_2}. \tag{Definisi 1a}$$

Selanjutnya,

$$\frac{p_1}{q_1} \cdot \frac{p_2}{q_2} = \frac{p_1p_2}{q_1q_2}. \tag{Definisi 1b}$$

Berdasarkan konstruksi standar pada teori Aljabar Abstrak, operasi tersebut memenuhi aksioma lapangan sehingga Q_D merupakan suatu *field*. Lapangan

$$Q_D = (Q_D, +, \cdot)$$

disebut lapangan hasil bagi dari daerah integral D. Untuk menunjukkan bahwa daerah integral D dapat disisipkan ke dalam lapangan Q_D, digunakan pemetaan

$$f : D \longrightarrow Q_D$$

yang didefinisikan sebagai berikut.

Definisi 2. Misal $f(p) = \frac{p}{1},\ \forall p \in D$, dengan

$$\frac{p}{1} = \{(x,y) \in D \times D^* \,|\, (x,y) \sim (p,1)\}.$$

Jika D dapat disisipkan ke lapangan Q_D, maka D isomorfik dengan citranya $f(D) \subseteq Q_D$. Oleh karena itu,

$$D \cong f(D).$$

Dengan menggunakan Teorema Utama Homomorfisme *Ring*, akan ditunjukkan bahwa pemetaan f merupakan homomorfisme, injektif, dan memiliki

$$\ker(f) = \{0\}.$$

1. f homomorfisme. Ambil sebarang $p_1, p_2 \in D$. Akan ditunjukkan

$$f(p_1 + p_2) = f(p_1) + f(p_2)$$

dan

$$f(p_1p_2) = f(p_1)f(p_2).$$

Berdasarkan Definisi 1b,

$$\begin{aligned} f(p_1 + p_2) &= \frac{p_1 + p_2}{1} \\ &= \frac{p_1}{1} + \frac{p_2}{1} \\ &= f(p_1) + f(p_2), \end{aligned}$$

dan

$$\begin{aligned} f(p_1 p_2) &= \frac{p_1 p_2}{1} \\ &= \frac{p_1}{1} \cdot \frac{p_2}{1} \\ &= f(p_1) f(p_2). \end{aligned}$$

Terbukti bahwa f merupakan homomorfisme, yaitu

$$\forall p_1, p_2 \in D,$$

berlaku

$$f(p_1 + p_2) = f(p_1) + f(p_2)$$

dan

$$f(p_1 p_2) = f(p_1) f(p_2).$$

2. f **injektif.** Ambil sebarang $p_1, p_2 \in D$. Akan ditunjukkan bahwa

$$f(p_1) = f(p_2) \Longrightarrow p_1 = p_2.$$

Berdasarkan pers. (Definisi 1b),

$$f(p_1) = \frac{p_1}{1}, \qquad f(p_2) = \frac{p_2}{1}.$$

Jika $f(p_1) = f(p_2)$, maka

$$\frac{p_1}{1} = \frac{p_2}{1} \Longleftrightarrow p_1 \cdot 1 = p_2 \cdot 1 \Longleftrightarrow p_1 = p_2.$$

Dengan demikian, terbukti bahwa f merupakan pemetaan injektif.

3. Kernel f **adalah** $\{0\}$. Misalkan

$$p_1 \in \ker(f).$$

Berdasarkan definisi kernel,

$$\ker(f) = \{p_1 \in D \mid f(p_1) = 0\}.$$

Dengan demikian,

$$f(p_1) = 0 \Longrightarrow \frac{p_1}{1} = 0 \Longrightarrow p_1 = 0.$$

Oleh karena itu,

$$\ker(f) = \{0\}.$$

Proposisi 1. *Misalkan D merupakan suatu daerah integral dan Q_D adalah lapangan hasil bagi*

yang dibangun dari D. Berdasarkan homomorfisme injektif

$$f : D \longrightarrow Q_D, \qquad f(p) = \frac{p}{1},$$

maka D dapat diidentifikasi sebagai subring dari Q_D. Oleh karena Q_D memenuhi seluruh aksioma lapangan, Q_D dapat digunakan sebagai domain koordinat dalam pendefinisian kurva eliptik $E(Q_D)$.

Bukti. Pemetaan

$$f : D \longrightarrow Q_D$$

merupakan homomorfisme dengan

$$\ker(f) = \{0\}.$$

Menurut Teorema Homomorfisme *Ring*, diperoleh

$$D \cong f(D).$$

Karena

$$f(D) \subseteq Q_D,$$

maka D dapat dipandang sebagai *subring* dari Q_D. Selanjutnya, karena Q_D merupakan lapangan, koordinat titik pada kurva eliptik dapat dipilih sebagai

$$(x, y) \in Q_D \times Q_D.$$

Dengan demikian, kurva eliptik

$$E(Q_D) = \left\{(x, y) \in Q_D^2 \,\middle|\, y^2 = x^3 + ax + b,\ \Delta \neq 0\right\}$$

terdefinisi dengan baik sehingga Q_D dapat digunakan sebagai domain koordinat dalam analisis struktur grup. □

Berdasarkan hasil konstruksi tersebut, lapangan Q_D selanjutnya digunakan sebagai domain koordinat untuk membangun kurva eliptik $E(Q_D)$. Pada bagian berikutnya dianalisis bagaimana struktur lapangan ini mendukung definisi operasi penjumlahan titik, pembentukan grup Abelian, serta representasi simbolik yang menjadi dasar konseptual dalam memahami mekanisme ECC. Kontribusi penelitian ini bukan terletak pada pembuktian kembali konstruksi lapangan hasil bagi, melainkan pada pemanfaatan hasil konstruksi tersebut sebagai fondasi pembentukan struktur kurva eliptik.

Setelah diperoleh lapangan Q_D, setiap titik pada kurva eliptik dapat direpresentasikan sebagai pasangan bilangan rasional sehingga operasi penjumlahan titik dapat dianalisis secara simbolik tanpa reduksi modulo. Hasil konstruksi lapangan hasil bagi beserta *embedding* kanonik menunjukkan bahwa setiap elemen daerah integral dapat direpresentasikan sebagai elemen lapangan Q_D. Representasi ini menjadi dasar dalam mendefinisikan koordinat titik pada kurva eliptik yang dianalisis. Oleh karena itu, pembentukan Q_D pada penelitian ini tidak diposisikan sebagai tujuan akhir, tetapi sebagai fondasi konseptual untuk membangun struktur $E(Q_D)$ dan menganalisis operasi titik secara simbolik.

3.3. Analisis Struktur Kurva Eliptik pada Lapangan Bilangan Rasional

Kurva eliptik harus bekerja dalam suatu lapangan karena lapangan merupakan fondasi utama dalam penerapan ECC [25]. Oleh karena itu, ketika bekerja pada daerah integral diperlukan pembentukan lapangan Q_D dari daerah integral tersebut. Lapangan hasil bagi memastikan setiap elemen tak nol memiliki invers perkalian [26].

3.3.1. Struktur Aljabar dalam Kurva Eliptik

Titik-titik pada $E(Q_D)$ dilengkapi dengan operasi penjumlahan titik menggunakan geometri garis singgung dan membentuk grup Abelian. Operasi ini tetap terdefinisi dengan baik meskipun menggunakan aritmetika pecahan. Dalam hal ini, Teorema Bézout [27] digunakan untuk menjelaskan perpotongan antara garis dan kurva eliptik yang menjadi dasar geometris operasi penjumlahan titik.

3.3.2. Analisis Penjumlahan Titik pada Kurva Eliptik

Operasi penjumlahan titik merupakan dasar pembentukan struktur grup pada kurva eliptik. Rumus *point addition* telah dibahas secara luas dalam literatur ECC. Oleh karena itu, penelitian ini tidak mengembangkan kembali rumus tersebut, melainkan menganalisis perilaku operasi ketika seluruh koordinat titik direpresentasikan pada lapangan hasil bagi Q_D.

Misalkan terdapat dua titik pada kurva eliptik,

$$P = (x_1, y_1) \qquad \text{dan} \qquad Q = (x_2, y_2).$$

Penjumlahan titik P dan Q menghasilkan titik

$$R = (x_3, y_3),$$

yang juga berada pada kurva eliptik. Terdapat dua kasus utama dalam proses penjumlahan titik pada kurva eliptik [28].

1. $P \neq Q$ (titik yang berbeda).
   Garis yang menghubungkan titik P dan Q akan memotong kurva eliptik di titik ketiga. Refleksi titik ketiga tersebut terhadap sumbu x menghasilkan titik $P + Q$.
2. $P = Q$ (titik yang sama).
   Dengan menggunakan garis singgung pada titik P, garis singgung akan memotong kurva eliptik di titik ketiga. Refleksi titik ketiga tersebut terhadap sumbu x menghasilkan titik $P + P = 2P$.

Langkah-langkah Penjumlahan Titik $(P \neq Q)$.

1. **Menghitung gradien garis yang menghubungkan** P **dan** Q.
   Gradien m dari garis yang menghubungkan

   $$P = (x_1, y_1) \qquad \text{dan} \qquad Q = (x_2, y_2)$$

   dihitung menggunakan

   $$m = \frac{y_2 - y_1}{x_2 - x_1}.$$

2. **Menentukan koordinat titik hasil.**
   Koordinat x_3 dihitung dengan

   $$x_3 = m^2 - x_1 - x_2,$$

   sedangkan koordinat y_3 dihitung dengan

   $$y_3 = m(x_1 - x_3) - y_1,$$

atau secara ekuivalen,

$$y_3 = m(x_2 - x_3) - y_2.$$

3. **Menentukan hasil penjumlahan.**
   Titik yang diperoleh dari proses tersebut merupakan

$$P + Q = R.$$

Langkah-langkah Penjumlahan Titik $(P = Q)$**.**

1. **Menghitung gradien** m**.**
   Gradien garis singgung pada titik

$$P = (x_1, y_1)$$

   dihitung dengan

$$m = \frac{3x_1^2 + a}{2y_1}.$$

   Rumus ini berasal dari turunan persamaan

$$y^2 = x^3 + ax + b$$

   yang digunakan untuk mencari gradien garis singgung pada kurva.
2. **Menentukan koordinat titik** R**.**
   Koordinat x_3 dihitung dengan

$$x_3 = m^2 - 2x_1,$$

   dan

$$y_3 = m(x_1 - x_3) - y_1.$$

3. **Menentukan hasil penggandaan titik.**
   Diperoleh

$$P + P = 2P = R.$$

Operasi penjumlahan titik yang sama disebut *point doubling* [29]. Tanpa garis singgung, tidak ada cara geometris untuk mendefinisikan penjumlahan titik dengan dirinya sendiri. Dalam kriptografi, hal ini penting untuk memastikan bahwa operasi pada titik-titik kurva eliptik dapat dihitung dengan benar. Dengan kata lain, peran garis singgung sangat penting dalam mendefinisikan operasi penjumlahan titik dalam grup Abelian pada kurva eliptik sebagai dasar operasi kriptografi [30].

Implementasi numerik penjumlahan titik pada kurva eliptik menggunakan GeoGebra ditunjukkan pada Gambar 3 dan Gambar 4.

3.3.3. Verifikasi Struktur Grup Abelian

Himpunan $E(Q_D)$ dengan operasi $+$ membentuk grup Abelian. Diberikan dua titik

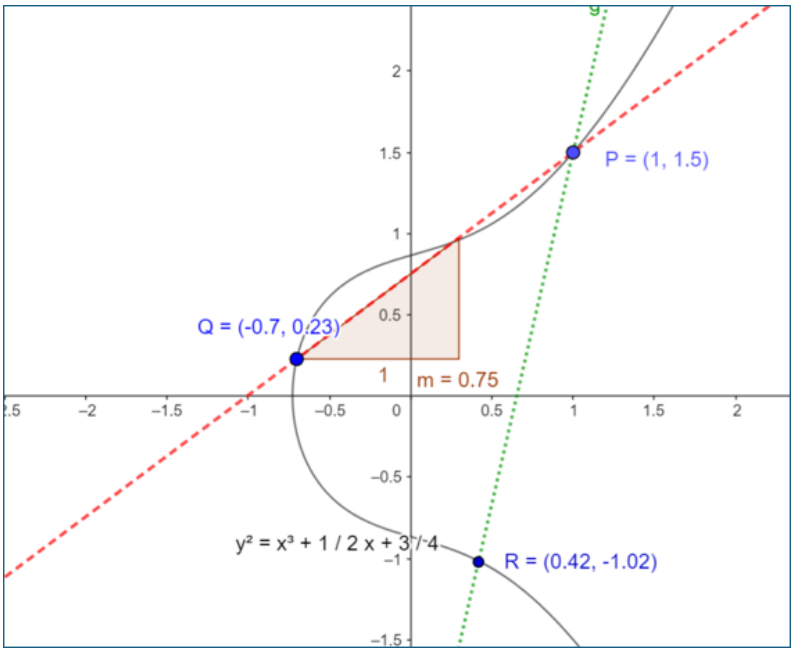
$$P = (x_1, y_1) \qquad \text{dan} \qquad Q = (x_2, y_2),$$

dengan $P, Q \in E(Q_D)$. Sesuai pers. (2), titik $\mathcal{O}$ adalah titik tak hingga dan digunakan sebagai elemen identitas.

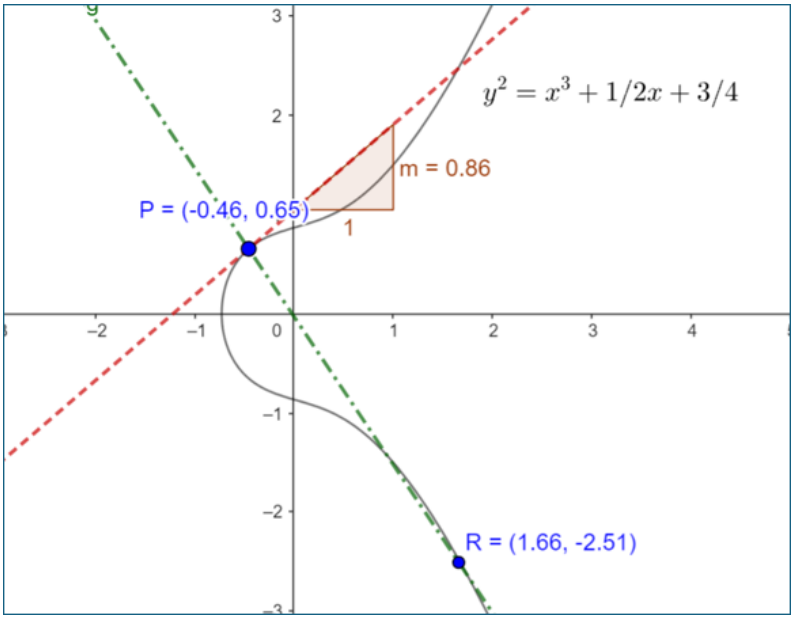
Selanjutnya, didefinisikan:

- Jika $P = \mathcal{O}$, maka

$$P + Q = Q.$$



Gambar 3. Penjumlahan titik $P + Q = R$.



Gambar 4. *Point doubling* $P + P = 2P = R$.

- Jika $Q = \mathcal{O}$, maka
$$P + Q = P.$$
- Jika $x_1 = x_2$ dan $y_1 = -y_2$, maka
$$P + Q = \mathcal{O}.$$
- Jika $P \neq Q$, maka garis yang melalui P dan Q memotong kurva di titik ketiga R, dan hasil penjumlahan didefinisikan sebagai
$$P + Q = -R,$$
yaitu refleksi R terhadap sumbu x.

Teorema 1. *Misalkan E adalah kurva eliptik atas Q_D. Maka*

$$(E(Q_D), +)$$

adalah grup Abelian dengan elemen identitas $\mathcal{O}$ dan operasi penjumlahan seperti didefinisikan sebelumnya.

Bukti. **1. Tertutup.** Jika $P, Q \in E(Q_D)$, maka $P + Q \in E(Q_D)$. Sesuai dengan penjelasan penjumlahan titik untuk $P \neq Q$, garis yang melalui P dan Q memotong kurva di titik ketiga R. Titik hasil penjumlahan adalah refleksi dari R terhadap sumbu x, yaitu $-R$. Begitu pula untuk $P = Q$, garis yang digunakan adalah garis singgung di P. Titik potong ketiga berada pada kurva dan refleksi terhadap sumbu x menghasilkan titik $P + P$. Dengan demikian, operasi penjumlahan bersifat tertutup pada $E(Q_D)$.

2. Komutatif.

Karena garis melalui P dan Q sama dengan garis melalui Q dan P, maka proses interseksi dan refleksi terhadap sumbu x memberikan $P + Q = Q + P$.

3. Identitas. Untuk setiap $P \in E(Q_D)$, $P+\mathcal{O} = \mathcal{O}+P = P$. Dengan demikian, $\mathcal{O}$ merupakan elemen identitas.

4. Invers. Untuk setiap

$$P = (x, y) \in E(Q_D),$$

terdapat

$$-P = (x, -y) \in E(Q_D),$$

karena

$$(-y)^2 = y^2 = x^3 + ax + b.$$

Selanjutnya,

$$P + (-P) = \mathcal{O}.$$

5. Asosiatif. Pembuktian sifat asosiatif pada operasi penjumlahan titik kurva eliptik secara aljabar memerlukan manipulasi ekspresi rasional yang sangat panjang sehingga sulit dilakukan secara manual. Oleh karena itu, penelitian ini menggunakan Wolfram Mathematica sebagai alat bantu untuk memverifikasi kesetaraan hasil operasi titik secara simbolik. Pendekatan yang digunakan adalah menyederhanakan selisih antara kedua hasil operasi asosiatif menjadi nol setelah diasumsikan bahwa ketiga titik berada pada kurva eliptik [31]. Untuk semua

$$P, Q, R \in E(Q_D),$$

harus berlaku

$$(P + Q) + R = P + (Q + R).$$

Didefinisikan

$$A = (P + Q) + R$$

dan

$$B = P + (Q + R).$$

Prosedur verifikasi dilakukan melalui tahapan berikut:

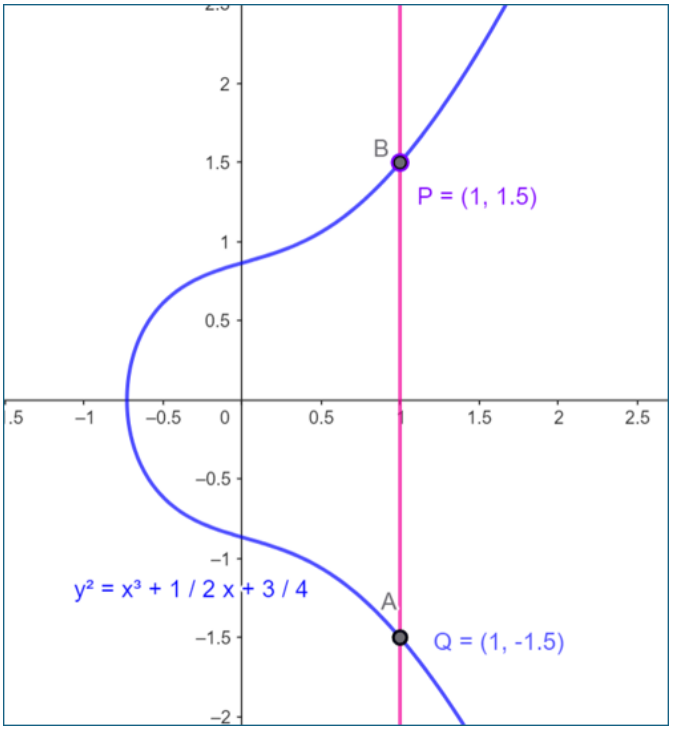
1. Mendefinisikan kurva eliptik

$$E(Q_D) : y^2 = x^3 + ax + b.$$

2. Menentukan tiga titik
$$P = (x_1, y_1), \qquad Q = (x_2, y_2), \qquad R = (x_3, y_3).$$
3. Mengimplementasikan rumus penjumlahan titik berdasarkan hukum grup sehingga diperoleh
$$(P + Q) + R$$
dan
$$P + (Q + R).$$
4. Mengekspresikan selisih kedua hasil tersebut sebagai
$$(x', y') = (P + Q) + R - \big(P + (Q + R)\big).$$
5. Menggunakan fungsi *Expand*, *Factor*, dan *Simplify* pada Mathematica untuk menyederhanakan seluruh ekspresi simbolik.
6. Verifikasi dinyatakan berhasil apabila
$$x' = 0 \qquad \text{dan} \qquad y' = 0,$$
yang menunjukkan bahwa kedua jalur operasi menghasilkan titik akhir yang identik sehingga sifat asosiatif terpenuhi.

Oleh karena itu, $(E(Q_D), +)$ memenuhi kelima aksioma grup Abelian. □

Selanjutnya, kurva eliptik
$$y^2 = x^3 + \frac{1}{2}x + \frac{3}{4}.$$
ditunjukkan pada Gambar 5.



Gambar 5. Kurva $y^2 = x^3 + \frac{1}{2}x + \frac{3}{4}$.

3.4. Analisis Numerik dan Ilustrasi Komputasi Operasi Kurva Eliptik

Terdapat titik $P = \left(1, \frac{3}{2}\right)$ dan $Q = \left(1, -\frac{3}{2}\right)$ pada kurva eliptik

$$y^2 = x^3 + \frac{1}{2}x + \frac{3}{4}.$$

Kasus khusus P dan Q dengan koordinat x yang sama menghasilkan garis yang menghubungkan kedua titik tersebut sejajar dengan sumbu y. Karena $Q = -P$, garis vertikal melalui P dan Q dipandang berpotongan dengan kurva pada titik tak hingga $\mathcal{O}$. Oleh karena itu, $P+Q = \mathcal{O}$.

Hal ini menunjukkan bahwa P dan Q merupakan pasangan titik refleksi terhadap sumbu x. Invers dari suatu titik $P = (x, y)$ adalah $-P = (x, -y)$. Dalam hal ini, $Q = -P$. Dengan menggunakan program Python, diperoleh beberapa titik rasional pada $E(Q_D)$ beserta hasil operasi penjumlahannya.

```
from fractions import Fraction
from math import isqrt


def is_perfect_square(frac):
if frac < 0:
return False
num = frac.numerator
den = frac.denominator
root_num = isqrt(num)
root_den = isqrt(den)
return root_num**2 == num and root_den**2 == den


def rational_sqrt(frac):
if is_perfect_square(frac):
return Fraction(isqrt(frac.numerator),
isqrt(frac.denominator))
return None


def find_unique_rational_points(a, b,
x_limit=20,
denom_limit=20):
points = []
seen = set()


for d in range(1, denom_limit + 1):
for n in range(-x_limit * d,
x_limit * d + 1):


x = Fraction(n, d)
rhs = x**3 + a * x + b
```

```
y = rational_sqrt(rhs)


if (y is not None
and (x, y) not in seen
and (x, -y) not in seen):


# hanya simpan satu dari pasangan
# (x, y) dan (x, -y)
chosen_y = y if y >= 0 else -y
points.append((x, chosen_y))
seen.add((x, chosen_y))


return points


def add_points(P, Q, a):
if P is None:
return Q


if Q is None:
return P


x1, y1 = P
x2, y2 = Q


if x1 == x2 and y1 == -y2:
return None


if P != Q:
m = (y2 - y1) / (x2 - x1)
else:
m = (3 * x1**2 + a) / (2 * y1)


x3 = m**2 - x1 - x2
y3 = m * (x1 - x3) - y1


return (x3, y3)
```

```
# ======== CONTOH KURVA ========
# y^2 = x^3 + (1/2)x + (3/4)


a = Fraction(1, 2)
b = Fraction(3, 4)


# Temukan titik-titik rasional unik
points = find_unique_rational_points(
a, b, x_limit=20, denom_limit=20
)


# Tampilkan hasilnya
print("Titik-titik rasional unik pada kurva:")


for i, (x, y) in enumerate(points):
print(f"{i+1}. ({x}, {y})")


# Penjumlahan dua titik pertama jika memungkinkan
if len(points) >= 2:
P, Q = points[0], points[1]
R = add_points(P, Q, a)


print("\nPenjumlahan titik ke-1 dan ke-2:")
print(f"P = ({P[0]}, {P[1]})")
print(f"Q = ({Q[0]}, {Q[1]})")


if R is None:
print("P + Q = Titik tak hingga")
else:
print(f"P + Q = ({R[0]}, {R[1]})")


else:
print("Belum ditemukan dua titik rasional unik.")
```

Pada dasarnya, menentukan titik-titik rasional pada kurva eliptik dapat menjadi sangat sulit. Namun, dalam artikel ini disajikan contoh enkripsi ketika melibatkan bilangan rasional sehingga dapat digunakan untuk mengeksplorasi ECC dan mengembangkan pemahaman mengenai konsep ECC lebih lanjut.

Contoh 1. Rama dan Shinta ingin saling bertukar pesan rahasia "LOVE" menggunakan kriptografi kurva eliptik berbasis struktur aljabar pada daerah integral $D = \mathbb{Z}$ dan lapangan hasil baginya, $Q_D = \mathbb{Q}$. Mereka menggunakan kurva eliptik $y^2 = x^3 + \frac{1}{2}x + \frac{3}{4}$ sebagai sistem dasar. Rama dan Shinta sepakat menggunakan titik generator $P = \left(1, \frac{3}{2}\right)$. Shinta sebagai penerima memilih kunci privat $d = 2$, kemudian menghitung kunci publik sebagai hasil *point doubling* dari titik P, yaitu $Q = 2P$.

Langkah Enskripsi. Rama ingin mengirimkan pesan teks "LOVE" kepada Shinta. Mengingat diperlukan pemetaan satu-satu, Rama memetakan setiap huruf ke suatu titik M pada kurva. Titik-titik yang digunakan untuk huruf "LOVE" beserta pasangan enkripsinya disajikan pada Tabel 1.

Tabel 1. Pemetaan huruf dan pasangan enkripsi.

Huruf	Titik M pada E	k	$C_1 = kP$	$C_2 = M + kQ$
L	$M_1 = \left(1, \frac{3}{2}\right)$	5	$\left(\frac{31115574109}{8106301225}, \frac{11233394994413829}{145970661585750}\right)$	$\left(-\frac{2320182575087899908534\ldots}{150828976681780342882829\ldots}, -\frac{589621018772939988838\ldots}{593799760550554453932\ldots}\right)$
O	$M_2 = 2P = \left(-\frac{23}{36}, \frac{89}{216}\right)$	2	$\left(-\frac{23}{36}, \frac{89}{216}\right)$	$\left(\frac{31115574109}{8106301225}, \frac{11233394994413829}{145970661585750}\right)$
V	$M_3 = 3P = \left(\frac{277}{3481}, -\frac{365157}{410758}\right)$	3	$\left(\frac{277}{3481}, -\frac{365157}{410758}\right)$	$\left(\frac{6452689}{1140624}, -\frac{16552413863}{1218186432}\right)$
E	$M_4 = 4P = \left(\frac{6452689}{1140624}, -\frac{16552413863}{1218186432}\right)$	1	$\left(1, \frac{3}{2}\right)$	$\left(\frac{277}{3481}, -\frac{365157}{410758}\right)$

Dengan menggunakan ElGamal [32], Rama mengirim pasangan

$$(C_1, C_2)$$

kepada Shinta untuk setiap huruf, dengan $C_1 = kP$ dan $C_2 = M + kQ$. Di sini, k diambil dari himpunan bilangan bulat karena jika menggunakan bilangan pecahan, interpretasi "setengah titik", misalnya $\frac{1}{2}P$, tidak dapat dilakukan secara langsung melalui mekanisme perkalian skalar standar.

Dalam kriptografi standar seperti ECDSA atau ECDH, operasi biasanya dilakukan pada lapangan hingga atau bilangan modulo [33]. Artinya, sistem tersebut bekerja pada ruang bilangan yang terbatas, sedangkan artikel ini menyajikan analisis pada struktur lapangan hasil bagi Q_D yang tak hingga.

Tabel 1 menyajikan pemetaan beberapa karakter menjadi titik-titik pada kurva eliptik yang didefinisikan di atas lapangan hasil bagi Q_D, beserta proses pembentukan pasangan *ciphertext* menggunakan mekanisme dasar *Elliptic Curve Cryptography* (ECC). Setiap karakter direpresentasikan sebagai titik M pada kurva eliptik, kemudian dipilih suatu bilangan k untuk menghasilkan pasangan enkripsi (C_1, C_2) dengan $C_1 = kP$ dan $C_2 = M + kQ$.

Hasil tersebut menunjukkan bahwa seluruh operasi penjumlahan titik dan perkalian skalar dapat dilakukan secara konsisten menggunakan aritmetika pada lapangan hasil bagi sehingga struktur grup Abelian pada kurva eliptik tetap dipertahankan.

Berbeda dengan implementasi ECC pada lapangan hingga GF(p) atau GF(2^m) [34, 35], operasi yang dilakukan pada lapangan hasil bagi menghasilkan koordinat berupa bilangan rasional dengan pembilang dan penyebut yang dapat berkembang menjadi sangat besar. Kondisi ini tampak pada nilai-nilai C_1 dan C_2 pada Tabel 1 yang memiliki representasi pecahan dengan digit yang panjang.

Meskipun representasi tersebut meningkatkan kompleksitas komputasi, seluruh operasi dilakukan secara eksak (*exact arithmetic*) tanpa kehilangan informasi akibat reduksi modulo. Dengan demikian, setiap tahapan operasi titik pada kurva eliptik dapat diamati dan diverifikasi secara simbolik sesuai dengan teori aljabar yang mendasarinya.

Tabel 1 menunjukkan bahwa konstruksi lapangan hasil bagi yang dibangun dari daerah integral mampu mendukung seluruh operasi dasar pada kurva eliptik, mulai dari representasi titik, perkalian skalar, hingga pembentukan pasangan *ciphertext*. Dengan kata lain, penelitian ini menunjukkan bahwa struktur lapangan hasil bagi menyediakan kerangka matematis yang konsisten bagi operasi-operasi kurva eliptik sebagaimana yang digunakan dalam ECC.

Kriptografi pada kurva eliptik dengan koefisien pecahan lebih cocok untuk eksplorasi teoretis karena pertumbuhan ukuran pembilang dan penyebut menyebabkan komputasi pecahan menjadi lebih lambat dibandingkan dengan lapangan hingga yang digunakan untuk implementasi kriptografi praktis dan efisien. Oleh karena itu, $E(Q_D)$ tidak digunakan secara langsung dalam implementasi kriptografi modern.

Hasil pembuktian teoretis dan validasi komputasi menunjukkan bahwa konstruksi lapangan hasil bagi Q_D mampu mendukung seluruh operasi aljabar pada kurva eliptik secara konsisten. Namun demikian, implementasi praktis ECC saat ini hampir seluruhnya menggunakan lapangan hingga (*finite field*) karena alasan efisiensi komputasi dan standar keamanan.

Oleh karena itu, perlu dilakukan analisis perbandingan antara karakteristik Q_D dan $\mathbb{F}_p$ untuk menunjukkan posisi penelitian ini dalam konteks pengembangan ECC modern. Perbandingan tersebut disajikan pada Tabel 2.

Tabel 2. Perbandingan *Quotient Field* dan *Finite Field*.

Aspek	*Quotient Field* Q_D	*Finite Field* $\mathbb{F}_p$	Implikasi terhadap Penelitian
Asal konstruksi	Dibentuk dari daerah integral melalui konstruksi *quotient field*.	Dibentuk sebagai lapangan hingga dengan operasi modulo bilangan prima p.	Menunjukkan dua pendekatan pembentukan lapangan yang berbeda.
Domain koordinat	Bilangan rasional, $(x, y) \in Q_D^2$.	Bilangan modulo, $(x, y) \in \mathbb{F}_p^2$.	Penelitian menggunakan koordinat rasional sebagai dasar analisis simbolik.
Operasi aritmetika	Menggunakan operasi pecahan secara eksak (*exact rational arithmetic*).	Menggunakan operasi modulo sehingga hasil selalu direduksi terhadap p.	Seluruh proses perhitungan dapat diamati tanpa kehilangan informasi akibat reduksi modulo.
Point addition dan *point doubling*	Menghasilkan koordinat rasional yang dapat ditelusuri pada setiap tahap perhitungan.	Menghasilkan koordinat modulo yang langsung direduksi.	Memudahkan analisis matematis dan verifikasi sifat grup.
Struktur grup	Membentuk grup Abelian pada $E(Q_D)$.	Membentuk grup Abelian pada $E(\mathbb{F}_p)$.	Struktur grup tetap dipenuhi pada kedua domain.
Validasi kurva	Diskriminan digunakan untuk memastikan kurva tidak singular sebelum operasi titik dilakukan.	Diskriminan juga digunakan untuk memastikan kurva valid sebelum implementasi ECC.	Konsep validasi kurva berlaku pada kedua jenis lapangan.
Verifikasi komputasi	Dapat diverifikasi menggunakan komputasi simbolik, seperti Mathematica dan Python.	Umumnya diverifikasi melalui implementasi modular dan pengujian algoritma ECC.	Pendekatan simbolik memudahkan analisis teoretis.
Kompleksitas komputasi	Ukuran pembilang dan penyebut pecahan terus bertambah sehingga komputasi menjadi lebih lambat.	Kompleksitas lebih efisien karena seluruh operasi berada pada lapangan hingga.	Menjelaskan keterbatasan Q_D untuk implementasi praktis.
Aplikasi utama	Analisis matematis, pembelajaran, dan *symbolic computation*.	Implementasi praktis ECC, ECDH, ECDSA, TLS, IoT, dan *blockchain*.	Menunjukkan bahwa kedua lapangan memiliki tujuan penggunaan yang saling melengkapi.

4. Kesimpulan

Penelitian ini menunjukkan bahwa konstruksi lapangan hasil bagi (*quotient field*) dari suatu daerah integral menyediakan fondasi aljabar yang konsisten untuk mendefinisikan dan meng-

analisis kurva eliptik. Melalui *embedding* kanonik $D \hookrightarrow Q_D$, lapangan Q_D dapat digunakan sebagai domain koordinat bagi kurva eliptik $E(Q_D)$. Validasi menggunakan diskriminan memastikan bahwa kurva yang digunakan bersifat nonsingular, sehingga operasi *point addition*, *point doubling*, dan perkalian skalar dapat didefinisikan dengan baik.

Analisis struktur aljabar menunjukkan bahwa himpunan titik $E(Q_D)$ bersama titik tak hingga $\mathcal{O}$ dan operasi penjumlahan membentuk grup Abelian. Konsistensi operasi tersebut juga didukung melalui verifikasi komputasi simbolik dan ilustrasi numerik menggunakan Mathematica dan Python. Hasil komputasi memperlihatkan bahwa operasi pada $E(Q_D)$ dapat dilakukan secara eksak menggunakan aritmetika rasional. Namun, pertumbuhan ukuran pembilang dan penyebut pada operasi berulang menyebabkan kompleksitas komputasi meningkat secara signifikan, sehingga Q_D lebih sesuai digunakan untuk analisis teoretis dan simbolik daripada untuk implementasi kriptografi praktis.

Kontribusi utama penelitian ini adalah penyusunan kerangka konseptual yang menghubungkan konstruksi *quotient field*, *embedding* daerah integral, pembentukan dan validasi kurva eliptik, struktur grup Abelian, serta verifikasi komputasi sebagai dasar matematis untuk memahami mekanisme ECC. Kerangka ini memperjelas hubungan antara konsep-konsep dalam Aljabar Abstrak dan operasi dasar pada kurva eliptik, sekaligus menegaskan perbedaan peran antara Q_D sebagai domain untuk eksplorasi matematis dan *finite field* sebagai domain yang lebih sesuai untuk implementasi ECC modern.

Kontribusi Penulis. **Miftah Sigit Rahmawati**: Konseptualisasi, metodologi, investigasi, penulisan. **Muhammad Fadli Hasa**: perangkat lunak, validasi, analisis formal, visualisasi.

Ucapan Terima Kasih. Para penulis mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dalam penelitian ini dan dalam penyusunan manuskrip.

Pembiayaan. Penelitian ini tidak menerima pendanaan eksternal.

Konflik Kepentingan. Tidak ada konflik kepentingan yang terkait dengan artikel ini.

Ketersediaan Data. Tidak tersedia.

Referensi

[1] S. Gajbhiye, S. Karmakar, and M. Sharma, "Study of finite field over elliptic curve: Arithmetic means," *International Journal of Computer Applications*, vol. 47, no. 17, pp. 32–38, 2012, doi:10.5120/7283-0411.
[2] M. A. Mohamed, "A survey on elliptic curve cryptography," *Applied Mathematical Sciences*, vol. 8, no. 153–156, pp. 7665–7691, 2014, doi:10.12988/ams.2014.49752.
[3] B. N. Koblitz, "Elliptic curve cryptosystems," vol. 4, no. 177, pp. 203–209, 1987.
[4] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996.
[5] D. Hankerson, S. Vanstone, and A. Menezes, *Guide to Elliptic Curve Cryptography*, 1st ed., ser. Springer Professional Computing. Springer New York, NY, 2004, doi:10.1007/b97644.
[6] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed. Chapman & Hall/CRC, 2014.
[7] National Institute of Standards and Technology, "Recommendation for discrete logarithm-based cryptography: Elliptic curve domain parameters," https://csrc.nist.gov/pubs/sp/800/186/final, 2023.
[8] T. W. Hungerford, *Algebra*, 1st ed., ser. Graduate Texts in Mathematics. Springer New York, NY, 1974, doi:10.1007/978-1-4612-6101-8.
[9] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed. John Wiley & Sons, July 2003.
[10] S. Kim and S. Kim, "Algebraic structure in elliptic curves," vol. 13, no. 3, pp. 143–152, 2019.
[11] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., ser. Graduate Texts in Mathematics. Springer, 2009, vol. 106, doi:10.1007/978-0-387-09494-6.

[12] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*, 2nd ed., ser. Discrete Mathematics and Its Applications. Chapman & Hall/CRC, April 2008.
[13] D. Maimut and A. C. Matei, "Speeding-up elliptic curve cryptography algorithms," *Mathematics*, vol. 10, no. 19, p. 3676, 2022, doi:10.3390/math10193676.
[14] A. M. Awaludin *et al.*, "High-speed and unified ECC processor for generic weierstrass curves over GF(p)," IACR ePrint Archive, 2022.
[15] C. Heuberger *et al.*, "Some notes on a formal algebraic structure of cryptology," *Theoretical Computer Science*, vol. 11, no. 1, pp. 1–24, 2021, doi:10.3390/math9182183.
[16] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, 1st ed., ser. Addison-Wesley Series in Mathematics. Addison-Wesley, February 1994.
[17] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, ser. Graduate Texts in Mathematics. Springer, 1995, vol. 150, doi:10.1007/978-1-4612-5350-1.
[18] P. Longa, "Accelerating the scalar multiplication on elliptic curve cryptosystems over prime fields," Master's thesis, University of Ottawa, June 2007.
[19] H. Angdinata and X. Xu, "An elementary formal proof of the group law on weierstrass elliptic curves in any characteristic," *arXiv*, 2023, doi:10.48550/arXiv.2302.10640.
[20] L. De Feo, "Mathematics of isogeny based cryptography," *arXiv preprint arXiv:1711.04062*, 2017, doi:10.48550/arXiv.1711.04062.
[21] D. J. Unger, "Yield criteria representable by elliptic curves and weierstrass form," *Procedia Structural Integrity*, vol. 35, no. C, pp. 2–9, 2021, doi:10.1016/j.prostr.2021.12.041.
[22] R. Wituła and D. Słota, "Cardano's formula, square roots, chebyshev polynomials and radicals," *Journal of Mathematical Analysis and Applications*, vol. 363, no. 2, pp. 639–647, 2010, doi:10.1016/j.jmaa.2009.09.056.
[23] D. K. Angdinata and J. Xu, "An elementary formal proof of the group law on weierstrass elliptic curves in any characteristic," in *Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany*, 2023, doi:10.4230/LIPIcs.ITP.2023.6.
[24] S. Lang, *Algebra*, 3rd ed. Springer, 2002, doi:10.1007/978-1-4613-0041-0.
[25] N. Koblitz, "Good and bad uses of elliptic curves in cryptography," *Moscow Mathematical Journal*, vol. 2, no. 4, pp. 693–715, 2002, doi:10.17323/1609-4514-2002-2-4-693-715.
[26] I. Heckenberger, E. Meir, and L. Vendramin, "Finite-dimensional nichols algebras of simple yetter–drinfeld modules (over groups) of prime dimension," *Advances in Mathematics*, vol. 444, pp. 1–24, 2024, doi:10.1016/j.aim.2024.109637.
[27] M. c. Kang, "Bezout's theorem and ideals of terminal forms," *Expositiones Mathematicae*, vol. 28, no. 3, pp. 265–268, 2010, doi:10.1016/j.exmath.2009.09.003.
[28] D. Vidakovic, D. Parezanovic, J. Kaljevic, and G. Ivanjica, "Addition and doubling of points 1," vol. 3, no. July, pp. 25–30, 2013.
[29] Y. Hao *et al.*, "Lightweight architecture for elliptic curve scalar multiplication over prime field," *Electronics*, vol. 11, no. 14, pp. 1–24, 2022, doi:10.3390/electronics11142234.
[30] A. Pakapongpun and S. Srisuk, "On the problem of tangency of ellipse curve," *Asian Journal of Applied Sciences*, vol. 6, no. 6, pp. 542–546, 2018, doi:10.24203/ajas.v6i6.5534.
[31] K. Fujii and H. Oike, "An algebraic proof of the associative law of elliptic curves," *Advances in Pure Mathematics*, vol. 7, no. 12, pp. 649–659, 2017, doi:10.4236/apm.2017.712040.
[32] M. R. Khan *et al.*, "Analysis of elliptic curve cryptography & RSA," *Journal of ICT Standardization*, vol. 11, no. 4, pp. 355–378, 2023, doi:10.13052/jicts2245-800X.1142.
[33] D. Kamboj and S. Sharma, "Study of efficient scalar multiplication over elliptic curve," in *Current Topics on Mathematics and Computer Science*, 2021, vol. 11, pp. 20–29, doi:10.9734/bpi/ctmcs/v11/4235f.
[34] A. Kak, "Lecture 7: Finite fields (part 4): Finite fields of the form GF(2^n), theoretical underpinnings of modern cryptography," pp. 1–40, 2013, lecture Notes on Computer and Network Security.
[35] S. Bajracharya, C. Shu, K. Gaj, and T. El-Ghazawi, "Implementation of elliptic curve cryptosystems over GF(2^n) in optimal normal basis on a reconfigurable computer," in *Lecture Notes in Computer Science*, vol. 3203, 2004, pp. 1001–1005, doi:10.1007/978-3-540-30117-2_115.