Teori Grup dan Peranannya dalam Perkembangan Penelitian Terkini

Indah Emilia Wijayanti

Departemen Matematika Universitas Gadjah Mada
Yogyakarta Indonesia
Seri Webinar FMIPA UT
14 Oktober 2023

Outline

Pengertian Grup dan Grup Faktor

Proses Abstraksi

Definisi

Diberikan himpunan tak kosong G. Didefinisikan suatu operasi biner $*$ pada G. Himpunan G disebut **grup** terhadap operasi $*$ jika memenuhi sifat:

1. $(\forall a, b, c \in G)\ (a * b) * c = a * (b * c)$ (aksioma asosiatif)
2. $(\exists e_G \in G)(\forall a \in G)\ e_G * a = a = a * e_G$ (aksioma eks. el. identitas)
3. $(\forall a \in G)(\exists b \in G)\ a * b = e_G = b * a$. (aksioma eks. el. invers untuk setiap elemen di G)

Contoh-contoh

1. Himpunan semua bilangan real tak nol $\mathbb{R}^*$ terhadap perkalian:

$$\cdot : \mathbb{R}^* \times \mathbb{R}^* \to \mathbb{R}^*, \quad \cdot(r, s) = rs.$$

   merupakan grup multiplikatif yang komutatif.
2. Demikian juga $\mathbb{Q}^*$ dan $\mathbb{C}^*$.
3. Grup Dihedral D_3.

Perumuman

Apakah bisa dibentuk grup dihedral yang melibatkan segi-n beraturan ?

Himpunan Bilangan Bulat Modulo n

- Bilangan bulat positif n.
- Himpunan bilangan bulat modulo n adalah $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$,
- Didefinisikan operasi penjumlahan modulo n, yaitu untuk setiap $x, y \in \mathbb{Z}_n$,

$$x + y = kn + r, \quad 0 \leq r < n,$$

  jadi didefinisikan $(x + y) \mod n = r$.
- $(\mathbb{Z}_n, +)$ membentuk grup (aditif) komutatif.

Beberapa Notasi

Diberikan grup G, subgrup-subgrup H, K di G dan $g \in G$.

- $HK = \{hk \mid h \in H, k \in K\}$.
- Apakah HK subgrup G?
- $gH = \{gh \mid h \in H\}$ disebut koset kiri H.
- $Hg = \{hg \mid h \in H\}$ disebut koset kanan H.
- Apakah gH dan Hg merupakan subgrup G ?
- Apakah $gH = Hg$?

Kesamaan Dua Koset

Diberikan koset-koset gH dan kH.

$$gH = kH \Leftrightarrow k^{-1}g \in H$$

Pembentukan Grup Faktor

Diberikan grup G dan subgrup H di dalam G.

- Untuk setiap $g \in G$ dibentuk gH.
- Dibentuk himpunan $G/H = \{gH \mid g \in G\}$.
- Didefinisikan operasi berikut:

$$g_1H * g_2H = (g_1g_2)H,$$

untuk setiap g_1H dan g_2H di G/H.

Pertanyaan

Apakah $(G/H, *)$ merupakan grup ?

Operasi Yang Terdefinisi dengan Baik

Operasi $*$ Sebagai Fungsi

Akan dibuktikan $*$ merupakan fungsi, dengan

$$\begin{aligned} * : G/H \times G/H &\to G/H, \\ (g_1H, g_2H) &\mapsto g_1H * g_2H = (g_1g_2)H. \end{aligned}$$

- Ambil g_1H, g_2H, k_1H dan k_2H di G/H dengan syarat

$$g_1H = k_1H, g_2H = k_2H,$$

  artinya $k_1^{-1}g_1 \in H$ dan $k_2^{-1}g_2 \in H$.
- Lebih lanjut, terdapat $h_1, h_2 \in H$ sehingga $k_1^{-1}g_1 = h_1$ dan $k_2^{-1}g_2 = h_2$.
- Akan dibuktikan apakah $g_1H * g_2H = k_1H * k_2H$.

Operasi Yang Terdefinisi dengan Baik (2)

- Perhatikan $g_1H * g_2H = k_1H * k_2H$ artinya sbb:

$$\begin{aligned} g_1H * g_2H &= k_1H * k_2H \\ (g_1g_2)H &= (k_1k_2)H \\ (k_1k_2)^{-1}(g_1g_2) &\in H \\ k_2^{-1}k_1^{-1}g_1g_2 &\in H. \end{aligned}$$

- Apakah pernyataan tersebut terbukti?

Pertanyaan

Apa syarat agar $k_2^{-1}k_1^{-1}g_1g_2 \in H$?

Pengertian Subgrup Normal

Definisi

Diketahui H adalah subgrup dari grup G. Subgrup G disebut subgrup normal jika untuk setiap $g \in G$ berlaku $gH = Hg$.

Teorema (Syarat Perlu dan Cukup dari Subgrup Normal)

Diketahui H adalah subgrup dari grup G. Subgrup H merupakan subgrup normal jika dan hanya jika untuk setiap $g \in G$ berlaku $gHg^{-1} \subseteq H$.

Contoh

- Perhatikan subgrup $12\mathbb{Z}$ di dalam grup $(\mathbb{Z}, +)$.
- Jelas $12\mathbb{Z}$ adalah subgrup normal, sebab $\mathbb{Z}$ adalah grup komutatif.
- Grup faktor yang terbentuk adalah

$$\mathbb{Z}/12\mathbb{Z} = \{0 + 12\mathbb{Z}, 1 + 12\mathbb{Z}, \ldots, 11 + 12\mathbb{Z}\}.$$

- Secara umum untuk setiap bilangan asli n, jika diambil subgrup $n\mathbb{Z}$ di dalam grup maka grup faktor yang terbentuk adalah

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

Homomorfisma Grup

Pengertian

Definisi

Diberikan sebarang dua grup $(G, *_G)$ dan $(G', *_{G'})$. Fungsi $f : G \to G'$ disebut homomorfisma grup jika memenuhi

$$f(g_1 *_G g_2) = f(g_1) *_{G'} f(g_2)$$

untuk setiap $g_1, g_2 \in G$

- Dapat diinterpretasikan bahwa homomorfisma grup adalah suatu fungsi yang mengawetkan operasi, yakni peta hasil operasi sama dengan hasil operasi dari masing-masing petanya.

Beberapa Contoh Homomorfisma Grup (1)

- Fungsi eksponensial $f : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ dengan $f(x) = e^x, \forall x \in \mathbb{R}$.
- Secara umum, jika $a \in \mathbb{R}^+$ maka fungsi $f(x) = a^x, \forall x \in \mathbb{R}$ juga merupakan homomorfisma dari $f : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$.
- Jika $a \in \mathbb{R}^+$ maka fungsi $f(x) =^a log x, \forall x \in \mathbb{R}^+$ juga merupakan homomorfisma dari $f : (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$.

Contoh Homomorfisma Grup (2)

- Diketahui A adalah matriks berukuran 2×3 dengan komponen-komponen di $\mathbb{R}$ dinotasikan $A \in M_{2\times 3}(\mathbb{R})$.
- Dari matriks A tersebut dapat dibentuk fungsi berikut:

$$\begin{aligned} T_A : \mathbb{R}^3 &\longrightarrow \mathbb{R}^2 \\ v &\mapsto T_A(v) = Av;\ \forall v \in \mathbb{R}^3 \end{aligned}$$

- Telah diketahui bahwa $\mathbb{R}^3$ merupakan grup terhadap penjumlahan $+_{\mathbb{R}^3}$ dan $\mathbb{R}^2$ grup terhadap penjumlahan $+_{\mathbb{R}^2}$.
- Mengingat $A(v+w) = Av + Aw$, T_A merupakan fungsi dan bersifat

$$T_A(v+w) = T_A(v) + T_A(w).$$

- Dapat disimpulkan bahwa T_A merupakan homomorfisma grup dari grup $(\mathbb{R}^3, +_{\mathbb{R}^3})$ ke grup $(\mathbb{R}^2, +_{\mathbb{R}^2})$.

Contoh-contoh lain

- Sifat derivatif: derivatif jumlah dua fungsi = jumlah masing-masing derivatif nya.
- Sifat integral tertentu: integral tertentu jumlah dua fungsi = jumlah masing-masing integral tertentu nya.
- Sifat limit: limit jumlah dua fungsi = jumlah masing-masing limit nya.
- Untuk matriks tertentu A berukuran $n \times m$ atas $\mathbb{R}$ berlaku sifat untuk setiap matriks B_1 dan B_2 berukuran $m \times p$ atas $\mathbb{R}$ berlaku sifat

$$A(B_1 + B_2) = AB_1 + AB_2.$$

Apakah dapat diberikan contoh homomorfisma grup dari sifat-sifat tersebut?

Teorema Utama Homomorfisma

Jika $f : G \to G'$ adalah homomorfisma grup, dan H adalah subgrup normal di G dengan $H \subseteq \mathrm{Ker}(f)$,maka dapat dibentuk isomorfisma

$$f' : G/H \to Im(f)$$

dengan definisi:

$$f'(gH) = f(g)$$

untuk setiap $gH \in G/H$.

Kejadian-kejadian khusus :

- Jika $H = \mathrm{Ker}(f)$.
- Jika f adalah epimorfisma.
- Jika $H = \mathrm{Ker}(f)$ dan f adalah epimorfisma.

Contoh

- Perhatikan subgrup $12\mathbb{Z}$ di dalam grup $(\mathbb{Z}, +)$.
- Jelas $12\mathbb{Z}$ adalah subgrup normal, sebab $\mathbb{Z}$ adalah grup komutatif.
- Grup faktor yang terbentuk adalah

$$\mathbb{Z}/12\mathbb{Z} = \{0 + 12\mathbb{Z}, 1 + 12\mathbb{Z}, \ldots, 11 + 12\mathbb{Z}\}.$$

- Secara umum untuk setiap bilangan asli n, jika diambil subgrup $n\mathbb{Z}$ di dalam grup maka grup faktor yang terbentuk adalah

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}.$$

Contoh

- Mudah dipahami bahwa $GL_2(\mathbb{R}) = \{A \in M_{2\times 2}(\mathbb{R}) | \det(A) \neq 0\}$ merupakan grup terhadap operasi perkalian matriks;
- $\mathcal{H} = \{B \in M_{2\times 2}(\mathbb{R}) | \det(B) = 1\}$ merupakan subgrup dari $GL_2(\mathbb{R})$.
- Akan dibuktikan $\mathcal{H}$ merupakan subgrup normal.

  Diambil sebarang $A \in GL_2(\mathbb{R})$. Akan dibuktikan $A\mathcal{H}A^{-1} \subseteq \mathcal{H}$. Diambil sebarang $B \in \mathcal{H}$, berarti $\det(B) = 1$. Akan ditunjukkan $ABA^{-1} \in \mathcal{H}$. Mudah dipahami

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(A)\frac{1}{\det(A)} = 1.$$

  Jadi, $ABA^{-1} \in \mathcal{H}$. Berdasarkan "Syarat Perlu dan Cukup" subgrup normal, berakibat $\mathcal{H}$ merupakan subgrup normal.

Terapan Grup di Kriptografi

Latar Belakang

Definisi

Kurva eliptik E didefinisikan sebagai himpunan titik solusi terhadap persamaan dengan bentuk $Y^2 = X^3 + aX + b$.

- Pada himpunan titik solusi tersebut didefinisikan operasi yang membentuk himpunan titik tersebut menjadi sebuah grup abelian.
- Untuk setiap dua titik P dan Q pada kurva E, jika dibuat garis yang menghubungkan kedua titik ini, akan didapatkan titik ketiga pada kurva E, yaitu titik R. Selanjutnya cerminkan titik R terhadap sumbu-x, hasilnya dinamakan R'.
- Operasi antara P dan Q selanjutnya dinotasikan dengan $+$, yaitu $P + Q = R'$.

Contoh : Operasi titik P dan Q pada kurva $E : Y^2 = X^3 + 1$

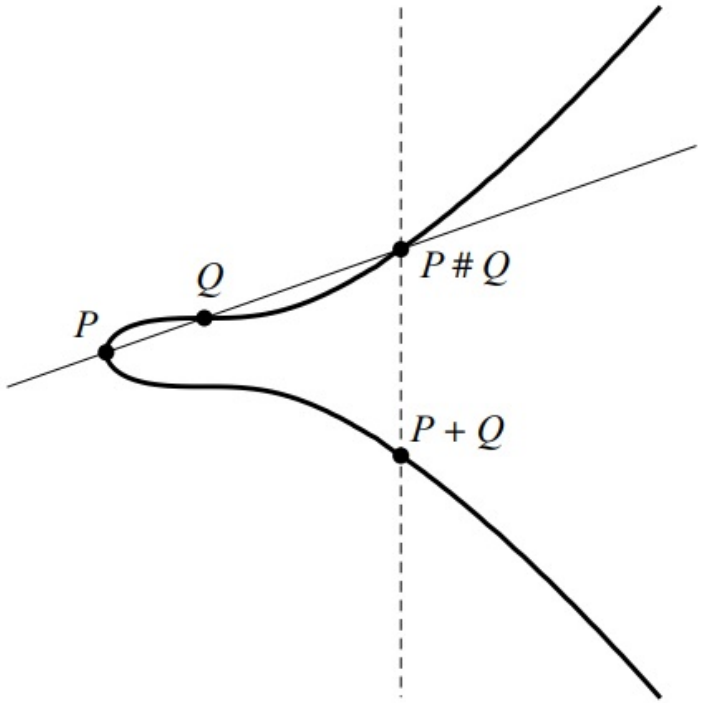

Figure: Operasi dua titik pada kurva $E : Y^2 = X^3 + 1$

Contoh : Operasi titik $P = Q$ pada kurva $E : Y^2 = X^3 - 3x + 1$

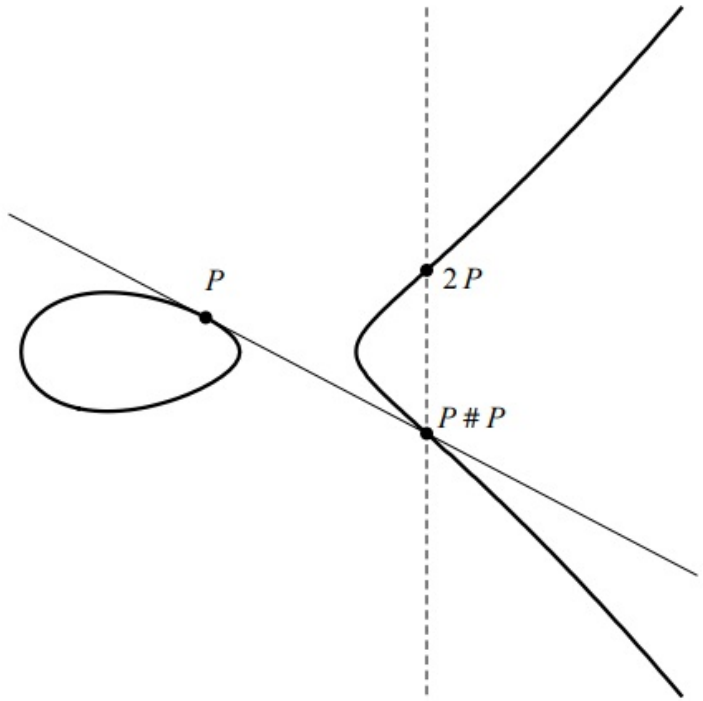

Figure: Operasi titik P dengan dirinya sendiri pada kurva $E : Y^2 = X^3 - 3X + 1$

Kurva Eliptik Sebagai Grup Komutatif

- Diberikan kurva eliptik E $Y^2 = X^3 + aX + b$ digabung dengan titik $\mathcal{O}$ yang memenuhi $4a^3 + 27b^2 \neq 0$.
- Misalkan P_1 dan P_2 adalah titik di E.
  1. Jika $P_1 = \mathcal{O}$, maka $P_1 + P_2 = P_2$.
  2. Jika $P_2 = \mathcal{O}$, maka $P_1 + P_2 = P_1$.
- Misalkan $P_1 = (x_1, y_1)$ dan $P_2 = (x_2, y_2)$
  1. Jika $x_1 = x_2$ dan $y_1 = -y_2$, maka $P_1 + P_2 = \mathcal{O}$.
  2. Selain itu, misalkan:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{jika } P_1 \neq P_2 \\ \\ \frac{3x_1^2 + A}{2y_1} & \text{jika } P_1 = P_2 \end{cases}$$

Maka $P_1 + P_2 = (x_3, y_3)$, dengan:

$$x_3 = \lambda^2 - x_1 - x_2 \quad \text{dan} \quad y_3 = \lambda(x_1 - x_3) - y_1$$

Kurva Eliptik atas Lapangan Hingga

Kurva eliptik atas lapangan hingga F_q adalah persamaan dalam bentuk:

$E : Y^2 = X^3 + aX + b$ dengan $a, b \in F_q$ yang memenuhi $4a^3 + 27b^2 \neq 0$

dan titik-titik E memiliki koordinat di F_q yang dinotasikan oleh:

$$E(F_q) = \{(x, y) : x, y \in F_q \text{ memenuhi } y^2 = x^2 + ax + b\} \cup \{\mathcal{O}\}$$

Contoh

- Diketahui persamaan kurva eliptik $E : Y^2 = X^3 + 3X + 8$ atas F_{13} dan dinotasikan $E(F_{13})$.
- Akan dihitung anggotanya dengan cara memeriksa semua kemungkinan nilai $x = 0, 1, 2, \cdots, 12$ yang berbentuk *square modulo* 13, jika masing-masing nilai x tersebut disubstitusi ke dalam persamaan $x^3 + 3x + 8$.
- Misalnya $x = 1$ menghasilkan nilai 12 dan

$$5^2 \equiv 12 \mod 13 \text{ dan } 8^2 \equiv 12 \mod 13$$

sehingga akan menghasilkan dua titik $(1, 5)$ dan $(1, 8)$ pada $E(F_q)$.

- $E(F_q)$ terdiri dari 9 titik, yaitu

$$\{\mathcal{O}, (1, 5), (1, 8), (2, 3), (2, 10), (9, 6), (9, 7), (12, 2), (12, 11)\})$$

Contoh Menjumlahkan Dua Titik di $E(F_q)$

- Perhatikan $P = (9, 7)$ dan $Q = (1, 8)$ dengan $P, Q \in (F_{13})$.
- Mencari nilai λ, yaitu:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{8-7}{1-9} \mod 13 = \frac{1}{-8 \mod 13} = \frac{1}{5} \mod 13 = 1 \cdot 8$$

- Mencari nilai x_3, yaitu:

$$x_3 = (\lambda^2 - x_1 - x_2) \mod 13 = (8^2 - 9 - 1) \mod 13 = 54 \mod 13 =$$

- Mencari nilai y_3, yaitu:

$$y_3 = (\lambda(x_1 - x_3) - y_1) \mod 13 = (8(9-2) - 7) \mod 13 = 10$$

sehingga $P + Q = (9, 7) + (1, 8) = (2, 10)$ yang juga merupakan anggota $E(F_{13})$.

Sifat

Teorema

Let $E(F_q)$ be an elliptic curve, where $q = p^n$ for some prime number p. Then there exist positive integers n_1 and n_2 such that $(E(F_q), +)$ is isomorphic to $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$. Furthermore, $n_2 | n_1$.

Ucapan Terima Kasih

Terima kasih ditujukan kepada:

- Rektor Universitas Terbuka dan jajarannya.
- Dekan dan jajaran pengurus Fakultas Sains dan Teknologi Universitas Terbuka.
- Pengurus Indonesian Mathematical Society (IndoMS).
- Annisa Dini Handayani, Rafifa Rafida, Rintang Utami, Rifky Manuel Satyana.

References I

- Adkins, W.A., Weintraub, S.H., Algebra an Approach via Module Theory, Graduate Text in Mathematics, Springer Verlag, New York, 1992.
- Stinson, D.R., Paterson, M.B., Cryptography : Theory and Practice Fourth Edition, Taylor and Francis Group, Boca Raton, 2019.
- Sutherland, A., Elliptic Curve (Lecture Notes), Massachussets Institute of Technology, 2017.
- https://ocw.mit.edu/courses/18-783-elliptic-curves-spring-2021/pages/lecture-notes-and-worksheets/