BAB II !

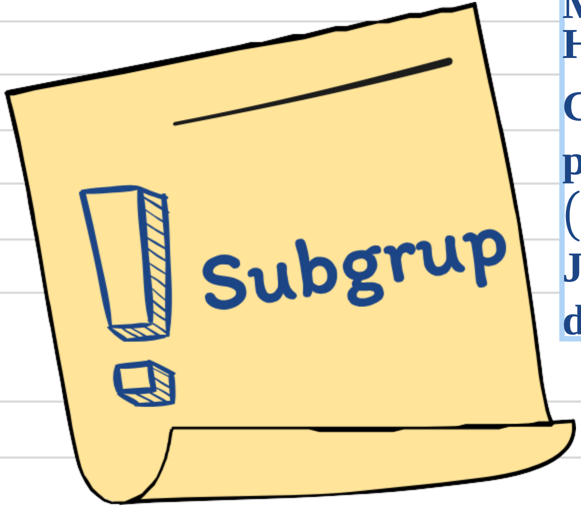
SUBGRUP

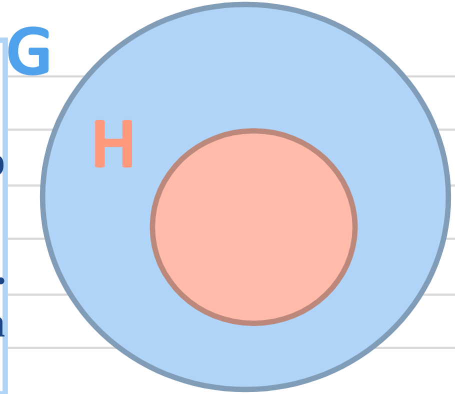
SUBGRUP

2.1 Defenisi dan Contoh

DEFENISI:

Misalkan G suatu grup. Himpunan H dari G adalah subgrup dari G jika H tidak kosong dan H tertutup pada perkalian dan invers $\left(x, y \in H, \textit{berarti } x^{-1} \in H \textit{ dan } xy \in H\right)$. Jika H adalah subgrup dari G, maka dinyatakan $H \leq G$ (*H* subset *G*).





CONTOH

1. Jika G merupakan grup dengan identitas e, maka $H = \{e\}$ merupakan subgroup dari G

Pembahasan:

1. $H \neq \emptyset$
2. $H \leq G$
3. Tertutup : $e * e = e$
4. Asosiatif : $(ee)e = (e)e = e$ dan $e(ee) = e(e) = e$
5. Identitas : H memiliki unsur identitas yaitu e
6. Invers : $e^{-1} = e$

Maka dapat disimpulkan bahwa H merupakan Subgrup dari G karena terpenuhi

CONTOH

2. Diberikan grup $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ terhadap operasi penjumLahan moduLo 6. Buktikan bahwa $S = \{0, 2, 4\}$ merupakan subgroup dari $\mathbb{Z}_6$ dan T$= \{0, 2, 3, 4\}$ bukan subgrup dari $\mathbb{Z}_6$

Pembahasan:

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

+	0	2	3	4
0	0	2	3	4
2	2	4	$\underline{5}$	0
3	3	$\underline{5}$	0	$\underline{1}$
4	4	0	$\underline{1}$	2

PROPOSISI 1.

(Kriteria Subgrup) Suatu subgrup H dari suatu grup G adalah suatu subgrup jika dan hanya jika

1. $H \neq \emptyset$
2. $\forall x, y \in H$ berlaku $xy^{-1} \in H$

Selanjutnya, jika H berhingga, maka cukup untuk memeriksa bahwa H tidak kosong dan tertutup di bawah perkalian.

PROPOSISI 1.

Bukti: Jika H adalah subgrup dari G, maka pasti (1) dan (2) berlaku karena H mengandung identitas G dan invers setiap elemennya dan karena H tertutup di bawah perkalian. Tetap menunjukkan sebaliknya bahwa jika H memenuhi keduanya (1) dan (2), maka $H < G$. Ambil x menjadi elemen apa pun di H. Biarkan $y = x$ dan kriteria (2) untuk menyimpulkan bahwa $1 = xx^{-1} \in H$, sehingga H mengandung identitas G. Kemudian, karena H mengandung 1 dan x, terdapat elemen $1x^{-1}$, yaitu $x^{-1} \in H$ dan H tertutup di bawah mengambil invers. Akhirnya, jika x dan y adalah dua elemen dari H , maka H mengandung x dan y^{-1}, jadi dengan (2), H juga mengandung $x(y^{-1})^{-1} = xy$. Oleh karena itu H juga tertutup dalam perkalian, yang membuktikan H adalah subgrup dari G

CONTOH

1. Tentukan grup (Z, +) , H adaLah himpunan biLangan buLat keLipatan 5. Apakah H subgrup Z?

Pembahasan:

Nyatakan $H = \{5k, k \in Z\}$

1) Tentukan $H \neq \emptyset$

   Tidak kosong karena $5 \in H$

2) Tentukan $H \leq Z$

   $H \leq Z$ karena anggota himpunan H ada di Z

3) Tertutup

   $x, y \in H, x + y \in H$

   Misalkan $x = 5K_1 \in Z$

   $y = 5k_2 \in Z$

   Maka $x + y = 5K_1 + 5k_2$

   $= 5(K_1 + k_2)$

   $x + y = 5.k_3 \in Z$

   Karena $x + y = 5.k_3 \in Z$ adalah tertutup

4) Asosiatif

   $x + y \in H \leq Z$ dan Z merupakan bilangan bulat sehingga syarat ini terpenuhi

5) Identitas

   H himpunan blangan bulat kelipatan 5

   $5 = \{5k, k \in Z\}$ dengan $k = 0$

   $= 5.k = 5.0 = 0$ maka syarat ini terbuki.

6) Invers

   $x = 5K_1 = x^{-1} = -5K_1$

   $= 5(-K_1) \in H$

Jadi, semua syarat telah terpenuhi maka $H \leq Z$

SENTRALISASI DAN NORMALISASI, STABILISATOR DAN KERNEL

2.2 Sentralisasi dan Normalisasi, Stabilisator dan Kernel

DEFENISI 1:

Defenisi 1: $C_G(A) = \{g \in G | gag^{-1} = a, \ \forall\, a \in A, \}$. Subset G ini disebut centralizer A di G. Karena $gag^{-1} = a$, maka jika dan hanyajika $ga = ag$, $C_G(A)$ adalah kumpulan elemen G yang bolak-balik dengan setiap elemen A.

Maka akan ditunjukkan $C_G(A)$ adalah subgrup G. Pertama-tama, $C_G(A) \neq \emptyset$ karena $1 \in C_G(A)$: definisi identitas menentukan bahwa $1a = a1$, untuk semua $a \in G$, (khususnya, untuk semua A) sehingga memenuhi kondisi yang menentukan untuk keanggotaan di $C_G(A)$.

Kedua, asumsikan $x, y \in C_G(A)$, yaitu, untuk semua $a \in A$. $xax^{-1} = a$ dan $yay^{-1} = a$ maka (perhatikan bahwa ini tidak berarti $xy = yx$). Kemudian amati dulu bahwa sejak $yay^{-1} = a$, mengalikan keduanya, untuk sisi pertama di sebelah kiri oleh y^{-1}, maka di sebelah kanan oleh y lalu disederhanakan menghasilkan $a = y^{-1}ay$ yaitu $y^{-1} \in C_G(A)$ sehingga $C_G(A)$ tertutup dengan mengambil invers.

2.2 Sentralisasi dan Normalisasi, Stabilisator dan Kernel

Lanjutan

Sekarang dilihat bahwa.

$$
\begin{aligned}
(xy)a(xy)^{-1} &= (xy)a(y^{-1}x^{-1}) && (\textit{dengan proposisi } 1.1(4) \textit{ diterapkan pada } (xy)^{-1}) \\
&= x(yay^{-1})x^{-1} && (\textit{dengan hukum Asosiatif}) \\
&= xax^{-1} && (\textit{karena } y \in C_G(A)) \\
&= a && (\textit{karena } x \in C_G(A))
\end{aligned}
$$

Jadi $xy \in C_G(A)$ dan $C_G(A)$ ditutup di bawah produk, maka $C_G(A) \leq G$. Dalam kasus khusus ketika $A = \{a\}$ maka akan ditulis $C_G(a)$ bukan $C_G(\{a\})$. Dalam hal ini $a^n \in C_G(a), \forall n \in Z$.

Misalnya, dalam grup abelian $G, C_G(A) = G$, untuk semua subset A.
kita dapat memeriksa dengan inspeksi yaitu $C_{Q8}(i) = \{\pm 1, \pm i\}$.

2.2 Sentralisasi dan Normalisasi, Stabilisator dan Kernel

DEFENISI 2:

Defenisi 2: Didefinisikan $Z(G) = \{g \in G \mid gx = xg, \forall\, x \in G\}$, kumpulan elemen yang bergerak dengan semua elemen G. Subset/Himpunan bagian dari G ini disebut pusat G.

Perhatikan bahwa $Z(G) = C_G(G)$, sehingga argumen di atas membuktikan $Z(G) \leq G$ sebagai kasus khusus. Sebagai latihan, pembaca mungkin ingin membuktikan $Z(G)$ adalah subkelompok secara langsung.

2.2 Sentralisasi dan Normalisasi, Stabilisator dan Kernel

DEFENISI 3:

Defenisi 3 : tentukan $gAg^{-1} = {}^{*}gag^{-1} \,|a \in A+$. Tentukan normalisasi A di G menjadi set $N_G(A) = {}^{*}g \in G|gAg^{-1} = A+$.

Perhatikan bahwa jika $g \in C_G(A)$,maka $gag^{-1} = a \in A, \forall\, a \in A$, jadi $C_G(A) \leq N_G(A)$. Bukti bahwa $N_G(A)$ adalah subkelompok G maka akan mengikuti langkah-langkah yang sama yang menunjukkan bahwa $C_G(A) \leq G$ dengan modifikasi yang sesuai.

Contoh

1. Jika G adalah abelian maka semua elemen G bolak-balik, jadi Z (G) = G. Demikian pula, $C_G(A) = N_G(A) = G\ \forall\ subset\ A$ dari G $sejak\ gag^{-1} = gg^{-1}a = a\ \forall\ g \in G$ dan setiap $a \in A$.

2. Biarkan $G = D_8$ menjadi kelompok dihedral urutan 8 dengan generator biasa r dan s dan biarkan $A = \{1, r, r^2, r^3\}$ menjadi subkelompok rotasi di dihedral 8. Dan menunjukkan bahwa $C_{D8}(A) = A$. Karena semua kekuatan r bolak-balik satu sama lain, $A \leq C_{D8}(A)$. Karena $sr = r^{-1}s \neq rs$, elemen s tidak bolak-balik dengan semua anggota A, $i.e.$, s bukan elemen $C_{D8}A$. Akhirnya, unsur-unsur D_8 yang tidak dalam A adalah semua bentuk sr^i untuk beberapa $i \in \{0,1,2,3\}$. Jika elemen sr^i berada di $C_{D8}(A)$ maka karena $C_{D8}(A)$ adalah subkelompok yang berisi r maka akan memiliki elemen $s = (sr^i)(r^i)$ di $C_{D8}(A)$, a sebuah kontradiksi. Ini menunjukkan $C_{D8}(A) = A$

Contoh

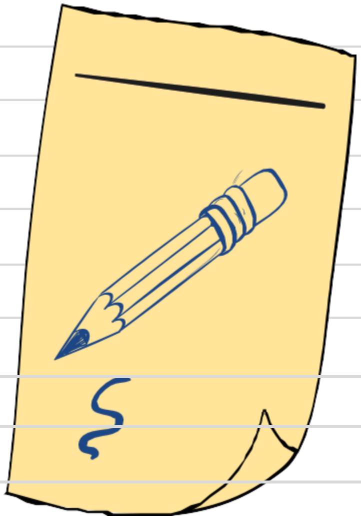
3. Seperti pada contoh sebelumnya biarkan $G = D_8$ dan biarkan $A = *1, r, r^2, r^3)$. Dan akan menunjukkan bahwa $N_{D8}, (A) = D_8$. Karena, secara umum, pemusatan subset terkandung dalam malizer $A \leq N_{D8}, (A)$. Selanjutnya menghitung bahwa$sAs^{-1} = \{ s1s^{-1}, sr^2s^{-1}, sr^3s^{-1} \} = \{1, r^3, r^2, r\}$ jadi itu $s \in N_{D8}(A)$. (Perhatikan bahwa set sAs^{-1} sama dengan set A meskipun elemen dalam, dua set ini muncul dalam urutan yang berbeda – ini karena s berada dalam normalisasi A tetapi tidak dalam pemusatan A.) Sekarang baik r dan s milik subkelompok $N_8, (A)$ dan karenanya $s^i r^j \in N_{D8}$ A (untuk semua bilangan bulat i dan j, yaitu, setiap elemen D_8 ada di $N_{D8}, (A)$ (ingat bahwa r dan s menghasilkan D_8). Karena $D_8 \leq N_{D8}, (A)$ kita memiliki $N_{D8}, (A) = D_8$ (penahanan terbalik yang jelas dari definisi normalisasi).

4. Tunjukan bahwa pusat D_8 adalah subkelompok $\{1, r^2\}$. Pertama amati bahwa pusat dari setiap kelompok G terkandung dalam Cc (A) untuksetiap subset A dari G. Jadi dengan Contoh 2 di atas $Z(D_8) \leq C_{D8}(A) = A$, di mana $A = \{1, r, r^2, r^3\}$ Penyelesaian di Contoh 2 menunjukkan bahwa r dan r^3 serupa tidak dalam $Z(D_8)$, sehingga $Z(D_8) \leq 1, r^2$.{Untuk} menunjukkan reverse inclusion mencatat bahwa r bolak-balik dengan r^2 dan menghitung bahwa itu s juga bolak-balik dengan r^2. Karena r dan s menghasilkan D_8, setiap elemen D_8bolak-balik dengan r^2 (dan 1), maka $*1, r^2 + \leq Z(D_8)$ dan kesetaraan berlaku.

Contoh

5. Biarkan $G = S_3$ dan memberikan A menjadi subkelompok $\{1, (12)\}$. Akan menjelaskan mengapa $C_{S_3}(A) = N_{S_3}(A) = A$. Seseorang dapat menghitung secara langsung bahwa $C_{S_3}(A) = A$, menggunakan ide-ide dalam Contoh 2 di atas untuk meminimalkan perhitungan. Atau, karena elemen bolak-balik dengan kekuatannya, $A \le C_{S_3}(A)$. Dengan Teorema Lagrange (Latihan 19 di Bagian 1.7) urutan subkelompok $C_{S_3}(A)$ dari S_3 membagi $|S_3| = 6$. Juga oleh Teorema Lagrange diterapkan pada subkelompok A dari kelompok $C_{S_3}(A)$ bahwa kita memiliki $2 \mid |C_{S_3}(A)|$. Satu-satunya kemungkinan adalah: $|C_{S_3}(A)| = 2$ atau 6. Jika yang terakhir terjadi, $C_{S_3}(A) = S_3$, $i.e.$, $A \le Z(S_3)$; ini adalah kontradiksi karena (1 2) tidak bolak-balik dengan (123). Jadi $|C_{S_3}(A)| = 2$ dan jadi $A = C_{S_3}(A)$.

Catatan berikutnya bahwa $N_{S_3}(A) = A$ karena $\sigma \in N_{S_3}(A)$ jika dan hanya jika $\{\sigma 1 \sigma^{-1}, \sigma(12)\sigma^{-1}\} = \{1, (12)\}$. Karena $\sigma 1 \sigma^{-1} = 1$, kesetaraan set ini terjadi jika dan hanya jika $\sigma(12)\sigma^{-1} = (12)$ juga maka, jika dan hanya jika $\sigma \in C_{S_3}(A)$. Pusat S_3 adalah identitas karena $Z(S_3) \le C_{S_3}(A) = A$ dan $(12) \notin Z(S_3)$.



Stabilisator dan Kernel Tindakan Grup

Fakta bahwa normaLisasi A di G, pemusatan A di G, dan pusat G adaLah semua subkeLompok dapat disimpuLkan sebagai kasus khusus hasiL pada tindakan keLompok, menunjukka nbahwa struktur G tercermin oLeh set di mana ia bertindak, sebagai berikut: jika G adaLah keLompok yang bertindak pada set S dan s adaLah beberapa eLemen tetap dari S, stabiLizer s di G adaLah set $G_S = \{g \in G \mid g.s = s\}$

(Lihat Latihan 4 di Bagian 1.7). dapat dituunjukkan secara singkat bahwa $G_s \leq G$: pertama $I \in G$, dengan aksioma (2) dari suatu tindakan. Juga, jika $y \in G_s$

$s = 1 \cdot s = (y^{-1} y).s$

$= y^{-1}.(y.s)$ (menuruttindakandariaksioma (1))

$= y^{-1}.s$ (karena $y \in G_s$)

jadi $y^{-1} \in G$ juga akhirnya jika $x, y \in G_s$ maka

$(xy).s = x.(y.s)$ (menuruttindakandariaksioma (1))

$= x.s$ $(karena\ y \in G_s)$

$= s$ $(karena\ x \in G_s)$

Ini membuktikan G_s adaLah subkeLompok dari G. Argumen serupa (tetapi Lebih mudah) membuktikan bahwa inti dari suatu tindakan adaLah subkeLompok, di mana inti dari aksi G pada S didefinisikan sebagai

$$\{g \in G \mid g.s = s, \forall\, s \in S\}$$

Contoh

1. KeLompok $G = D_8$ bertindak pada set A dari empat simpuL kuadrat {Lih. Contoh 4 di Bagian 1.7). StabiLizer dari setiap simpuL a adaLah subkeLompok {1,t} dari D_8 di mana t adalah refLeksi tentang garis simetri meLewati simpuL a dan pusat kuadrat. Inti dari tindakan ini adaLah subkeLompok identitas karena hanya simetri identitas yang memperbaiki setiap simpuL.
2. Grup G = D_8 juga bertindak pada set A yang eLemennya adaLah dua pasangan simpuL situs yang tidak berurutan {daLam peLabeLan Figure 2 di Bagian 1.2, A = { {1, 3}, {2, 4} }). Inti dari aksi D_8 pada set A ini adaLah subkeLompok $*1, s, r^2, sr^2+$ dan untuk kedua eLemen $a \in A$ stabiLizer a dalam D_8 sama dengan inti aksi

$$g: B \to gBg^{-1} \text{ dimana } gBg^{-1} = \{gbg^{-1} \mid b \in B\}$$

$$g: a \to gag^{-1}$$

(lihat Latihan 16 di Bagian 1.7). Di bawah tindakan ini, mudah untuk memeriksa bahwa $N_G(A)$ adalah penstabilizer A di G (i,e, $N_G(A) = G_S$ di mana $S = A \in P(G)$), jadi $N_G(A)$ adalah subkelompok G. Selanjutnya biarkan kelompok $N_G A$ bertindak pada set $S = A$ dengan konjugasi, yaitu, untuk semua $g \in N_G A$ dan $a \in A$ ( )

Perhatikan bahwa ini memetakan A ke A dengan definisi $N_G(A)$ dan memberikan tindakan pada A. Di sini mudah untuk memeriksa bahwa $C_G(A)$ adalah kernel(inti) dari tindakan ini, maka $C_G(A) \le N_G(A)$; dengan transitivitas hubungan " $\le$," $C_G(A) \le G$. Akhirnya, Z (G) adalah kernel dari G yang bekerja pada S = G dengan konjugasi. jadi $Z(G) \le G$.

GRUP SIKLIK
SUBGRUP SIKLIK

2.3 Grup Siklik dan Subgrup Siklik

DEFENISI:

Grup H adaLah sikLik jika H dapat dihasiLkan oLeh satu eLemen yaitu ada beberapa eLemen $x \in H$ sedemikian sehingga $H = \{x^n \mid n \in \mathbb{Z}\}$(dimana operasinya adaLah perkaLian)

DaLam notasi aditif H adaLah sikLik jika $H = \{nx \mid n \in \mathbb{Z}\}$ DaLam kedua kasus, kita akan menuLis $H = \langle x \rangle$ dan mengatakan H dihasiLkan oLeh x (x adaLah generator H). Sebuah grup sikLik dapat menghasiLkan Lebih dari satu generator. MisaLnya, jika $H = \langle x \rangle$ kemudian $H = \langle x^{-1} \rangle$ karena $(x^{-1})^n = x^{-n}$ dan karena n meLewati semua biLangan buLat, begitu juga $-n$ sehingga,

$$\{x^n \mid n \in \mathbb{Z}\} = \{(x^{-1})^n \mid n \in \mathbb{Z}\}$$

Akan ditunjukkan bagaimana menentukan semua generator untuk grup sikLik tertentu H. Satu yang harus diingat bahwa eLemen $\langle x \rangle$ adaLah pangkat dari x (atau keLipatan x, daLam grup dituLis aditif) dan bukan biLangan buLat. BeLum tentu benar bahwa semua pangkat x berbeda. Menurut hukum/sifat eksponen (Latihan 19 daLam bagian 1.1) grup sikLik adaLah abeLian.

Contoh

1. Diberikan $G = D_{2n} = \langle r, s \mid r^n = s^2 = 1, rs = sr^{-1} \rangle$, $n \geq 3$ dan diberikan H adalah subgrup dari semua rotasi dari n-gon. Jadi $H = \langle r \rangle$ dan elemen-elemen berbeda dari H adalah $1, r, r^2, \dots, r^{n-1}$ (semua ini adalah pangkat yang berbeda dari r). Secara khusus $|H| = n$ dan generator, r , dari H berorde n. pangkat dari r siklus (maju dan mundur) dengan periode n, yaitu,

$$r^n = 1, r^{n+1} = r, r^{n+2} = r^2, \dots$$
$$r^{-1} = r^{n-1}, r^{-2} = r^{n-2}, \dots$$

Secara umum, untuk menulis pangkat apapun dari r, katakanlah r^t, dalam bentuk r^k, untuk beberapa k antara 0 dan $n-1$ gunakan algoritma pembagian untuk menulis,

$$t = nq + k, dimana\ 0 \leq k < n$$

Maka,

$$r^t = r^{nq+k} = (r^n)^q r^k = 1^q r^k = r^k$$

Sebagai contoh, pada D_8, $r^4 = 1$ jadi $r^{105} = r^{4(26)+1} = r$ dan $r^{-42} = r^{-4(11)+2} = r^2$. Perhatikan bahwa D_{2n} sendiri bukan grup siklik karena non abelian.

2. Diberikan $H = \mathbb{Z}$ dengan operasi $+$. Dengan demikian $H = \langle 1 \rangle$ (dimana 1 adalah bilangan bulat 1 dan identitas dari H adalah 0) dan setiap elemen di H dapat ditulis secara unik dalam bentuk $n \cdot 1$, untuk suatu $n \in \mathbb{Z}$. Berbeda dengan contoh sebelumnya, kelipatan dari generator semuanya berbeda dan kita perlu mengambil keduanya positif, kelipatan negatif dan nol dari generator untuk memperoleh semua elemen dari H. Dalam contohini $|H|$ dan order dari generator 1 keduanya ∞. Perhatikan juga bahwa $H = \langle -1 \rangle$ karena setiap bilangan bulat x dapat ditulis sebagai $(-x)(-1)$.

Contoh

3. Diberikan $(G, \times)$. Jika diketahui $G = \{1, -1, i, -i\}$, dengan $i = \sqrt{-1}$, maka selidiki apakah G merupakan grup siklik dengan generator i atau $-i$.

Pembahasan:

G disebut grup siklik jika ada $a \in G$ sedemikian sehingga $G = \{a^n | n \in \mathbb{Z}\}$. Elemen a pada G ini disebut generator dari grup siklik tersebut.

Ambil $i \in G$, sehingga

$$i^2 = \sqrt{-1} \times \sqrt{-1} = -1$$

$$i^3 = i^2 \times i = -1 \times \sqrt{-1} = -1 \times i = -i$$

$$i^4 = i^2 \times i^2 = -1 \times -1 = 1$$

Jadi $G = \{1, -1, i, -i\}$ adalah grup siklik dengan generator i dan $|i| = 4$

Ambil $-i \in G$, sehingga

$$(-i)^2 = (-i) \times (-i) = i^2 = -1$$

$$(-i)^3 = (-i)^2 \times -i = -1 \times -i = i$$

$$(-i)^4 = (-i)^2 \times (-i)^2 = -1 \times -1 = 1$$

Jadi $G = \{1, -1, i, -i\}$ adalah grup siklik dengan generator $-i$ dan $|-i| = 4$

4. Tunjukkan bahwa $(\mathbb{R}, +)$ Bukan merupakan grup siklik

Pembahasan:

kita harus menunjukkan bahwa tidak ada $a \in \mathbb{R}$ yang menjadi generator pada himpunan bilangan real.

Pembuktiannya menggunakan kontradiksi.

Andaikan $a \in \mathbb{R}$ merupakan generator dari $\mathbb{R}$. Perhatikan bahwa:

$0y = 0$, (identitas penjumlahan di $\mathbb{R}$)

$1y = y$, $2y = y + y$, $3y = y + y + y$, dan seterusnya

Disisi lain

$-1y = -y$, $-2y = (-y) + (-y)$, $3y = (-y) + (-y) + (-y)$, dan seterusnya.

Dengan demikian, diperoleh

$$\{na | n \in \mathbb{Z}\} = \{\dots, -3y, -2y, -y, 0, y, 2y, 3y, \dots\}$$

Karena $a \in \mathbb{R}$, maka terdapat $z = \frac{a}{2} \in \mathbb{R}$, padahal z tidak dapat dinyatakan sebagai kelipatan a. jadi pengandaian salah (a bukan generator dari $\mathbb{R}$) sehingga $(\mathbb{R}, +)$ bukan merupakan grup siklik

Proposisi 2.

Proposisi 2. Jika $H = \langle x \rangle$ maka $|H| = |x|$ (dimana jika satu sisi persamaan ini tidak terbatas, begitu juga yang lainnya) lebih spesifik

1. Jika $|H| = n < \infty$ maka $x^n = 1$ dan $1, x, x^2, \dots, x^{n-1}$ adalah semua elemen-elemen yang berbeda dari H, dan
2. Jika $|H| = \infty$ maka $x^n \neq 1$ untuk semua $n \neq 0$ dan $x^a \neq x^b$ untuk semua $a \neq b$ di $\mathbb{Z}$

Bukti:

Diberikan $|x| = n$ dan pertama pertimbangan untuk kasus $n < \infty$. Elemen $1, x, x^2, \dots, x^{n-1}$ adalah berbeda karena jika $x^a = x^b$, dengan mengatakan$0 \leq a < b < n$, maka $x^{b-a} = x^0 = 1$, bertentangan dengan n adalah pangkat positif terkecil dari x yang memberikan identitas. Dengan demikian Hmemiliki paling sedikit n elemen dan tinggal menunjukkan bahwa ini adalah semuanya.

Seperti pada contoh 1, jika x^t adalah pangkat dari x, dengan menggunakan algoritma pembagian dapat ditulis $t = nq + k$ dimana $0 \leq k < n$, jadi

$$x^t = x^{nq+k} = (x)^{nq}x^k = (x^n)^q x^k = 1^q x^k = x^k \in \{1, x, x^2, \dots, x^{n-1}\}$$

seperti yang kita inginkan

Misalkan selanjutnya $|x| = \infty$ jadi tidak ada pangkat positif dari x yang merupakan identitasnya. Jika $x^a = x^b$, untuk suatu a dan b dengan mengatakan $a < b$, maka $x^{b-a} = 1$, adalah kontrakdiksi. Pemangkatan berbeda dari x adalah elemen berbeda dari H jadi $|H| = \infty$. Hal ini melengkapi bukti proposisi.

Perhatikan bahwa bukti proposisi memberikan metode untuk mereduksi pangkat sembarang dari generator dalam grup siklik berhingga menjadi pangkat “sisa terkecil”.

Proposisi 3

Diberikan G adalah sembarang grup, dengan $x \in G$ dan diberikan $m, n \in \mathbb{Z}$. Jika $x^n = 1$ dan $x^m = 1$, maka $x^d = 1$, dimana $d = (m, n)$. Khususnya, jika $x^m = 1$ untuk suatu $m \in \mathbb{Z}$, maka $|x|$ membagi m.

BUKTI

Berdasarkan Algoritma Euclid (Dapat dilihat pada Bagian 0.2 (6)) terdapat bilangan bulat r dan s sedemikian sehingga $d = mr + ns$, dimana d adalah FPB dari m dan n. Dengan demikian

$$\boldsymbol{x^d = x^{mr+ns} = (x^m)^r (x^n)^s = 1^r 1^s = 1}$$

Ini membuktikan pernyataan pertama.

Jika $x^m = 1$, diberikan $n = |x|$. Jika $m = 0$, tentu $n|m$, jadi kita asumsi $m \neq 0$. Karena beberapa pangkat bukan nol dari x adalah identitasnya, $n < \infty$. Diberikan $d = (m, n)$ jadi dengan hasil sebelumnya $x^d = 1$. Karena $0 < d \leq n$ dan n adalah pangkat positif terkecil dari x yang menghasilkan identitas, kita mempunyai $d = n$ yaitu $n|m$, seperti yang ditegaskan

TEOREMA 4

Teorema 4. Setiap dua grup siklik dengan order yang sama adalah isomorfik. Terlebih khusus.

Jika $n \in \mathbb{Z}^+$ dan $\langle x \rangle$ dan $\langle y \rangle$ keduanya adalah grup siklik beroder n, maka bayangan/peta/hasil

$$\varphi : \langle x \rangle \to \langle y \rangle$$
$$x^k \mapsto y^k$$

Jadi, terdefenisi dengan jelas dan merupakan isomorfisma

Jika $\langle x \rangle$adalah grup siklik tak hingga, maka bayangan/peta/hasil

$$\varphi : \mathbb{Z} \to \langle x \rangle$$
$$k \mapsto x^k$$

Jadi, terdefenisi dengan jelas dan merupakan isomorfisme

Bukti Teorema 4.

Misalkan $\langle x\rangle$ dan $\langle y\rangle$ adalah dua grup siklik yang berorde n. Diberikan $\varphi\colon \langle x\rangle \to \langle y\rangle$ dengan definisi $\varphi(x^k) = y^k$, pertama-tama kita harus membuktikan bahwa φ terdefenisi dengan jelas, yaitu
Jika $x^r = x^s$, maka $\varphi(x^r) = \varphi(x^s)$.
Karena $x^{r-s} = 1$. Proposisi 3 menunjukkan $n|r - s$.
Ditulis $r = tn + s$ jadi

$$\begin{aligned}\varphi(x^r) &= \varphi(x^{tn+s}) \\ &= y^{tn+s} \\ &= (y^n)^t y^s\end{aligned}$$

$\varphi(x^r) = y^s = \varphi(x^s)$.
Ini membuktikan bahwa φ terdefenisi dengan jelas.
Sesuai dengan sifat eksponen bahwa $\varphi(x^a x^b) = \varphi(x^a)\varphi(x^b)$ (Cek Kebenaran)
$\varphi(x^a) = y^a$ dan $\varphi(x^b) = y^b$

$$\varphi(x^a x^b) = \varphi(x^{a+b})$$
$$\varphi(x^a x^b) = y^{a+b}$$
$$\varphi(x^a x^b) = y^a y^b$$
$$\varphi(x^a x^b) = \varphi(x^a)\varphi(x^b)$$

Jadi φ adalah homomorfisma karena eleman y^k dari $y\langle\ \rangle$ adalah bayangan dari x^k yang dipasangkan φ, maka banyangan ini surjektif . Karena kedua grup memiliki orde berhingga yang sama, maka setiap surjeksi dari satu ke yang lain adalah bijeksi, jadi φ adalah isomorfisma (sebagai alternatif, φ memiliki invers dua sisi yang jelas).

Jika $\langle x\rangle$ adalah grup siklik tak hingga, misalkan $\varphi\colon \mathbb{Z} \to \langle x\rangle$ didefenisikan oleh $\varphi(k) = x^k$. Perhatikan bahwa bayangan/peta sudah terdefenisi yang jelas,karena tidak ada ambiguitas dalam representasi eleman dalam domain. Karena (dengan proposisi 2) $x^a \neq x^b$ untuk semua $a, b \in \mathbb{Z}$ yang berbeda, φ adalah injektif.

Menurut defenisi grup siklik φ adalah surjektif. Seperti di atas sifat eksponen memastikan bahwa φ adalah homomorfisma, maka φ adalah isomrofisma, hal ini melengkapi bukti.

Seperti yang telah disebutkan sebelumnya, grup siklik tertenu mungkin memiliki lebih dari satu generator. Dua proposisi berikutnya, menentukan secara tepat pangkat x yang manayang menghasilkan grup x . ⟨ ⟩

Proposisi 5

Diberikan G adalah grup, misalkan $x \in G$ dan misalkan $a \in \mathbb{Z} - *0+$.

1. Jika $|x| = \infty$, maka $|x^a| = \infty$,
2. Jika $|x| = n < \infty$, maka $|x^a| = \frac{n}{(n,a)}$
3. Secara khusus, jika $|x| = n < \infty$ dan a adalah bilangan bulat positif yang membagi n, maka $|x^a| = \frac{n}{a}$

Bukti: (1) Dengan menggunakan kontradiksi asumsi bahwa $|x| = \infty$ tapi $|x^a| = m < \infty$. Dengan menggunakan defenisi order

$$1 = (x^a)^m = x^{am}$$

Jadi

$$x^{-am} = (x^{am})^{-1} = 1^{-1} = 1$$

Sekarang salah satu dari am atau $-am$ adalah positif (karena a atau m adalah 0 sehingga beberapa pangkat positif dari x adalah identitasnya. Ini kontradiksi dengan hipotesis $x = \infty$, jadi asumsi $x^a < \infty$, pasti salah, yaitu (1) berlaku.

Proposisi 5

Bukti (2):

Di bawah notasi dari (2) diberikan

$y = x^a$, $(n, a) = d$ dan ditulis $n = db$, $a = dc$,

Untuk $b, c \in \mathbb{Z}$ dengan $b > 0$. Karena d adalah pembagi persekutuan terbesar dari n dan a, bilangan bulan b dan c relatif prima:

$$(b, c) = 1$$

Untuk menetapkan (2) kita harus menunjukkan $|y| = b$. Catatn pertama yaitu

$$y^b = x^{ab} = x^{dcb} = (x^{db})^c = (x^n)^c = 1^c = 1$$

Jadi, dengan proposisi 3 diterapkan pada $\langle y \rangle$, kita melihat bahwa $|y|$ membagi b. Misalkan $k = |y|$. Maka

$$x^{ak} = y^k = 1$$

Jadi dengan proposisi 3 diterapkan pada $\langle x \rangle$, $n|ak$, yaitu, $db|dck$. Jadi $b|ck$. Karena b dan c tidak memiliki faktor yang sama, b harus membagi k. Karena b dan k adalah bilangan bulat positif yang saling membagi, $b = k$, yang membuktikan

Bukti (3).

Ini adalah kasus khusus dari (2) yang diambil untuk referensi di masa mendatang

Proposisi 6.

Diberikan $H = \langle x \rangle$.

1. Asumsi $|x| = \infty$. Maka $H = \langle x^a \rangle$ jika dan hanya jika $a = \pm 1$.
2. Asumsi $|x| = n < \infty$. Maka Maka $H = \langle x^a \rangle$ jika dan hanya jika $(a, n) = 1$. Secara khusus, jumlah generator dari H adalah $\varphi(n)$ (dimana φ adalah fungsi φ euler)

Bukti 1:
Jika $|x| = \infty$ dan berdasarkan proposisi 5 maka terdapat $H = \langle x^a \rangle$ dengan $|x^a| = \infty$. Karena $|x| = \infty$ dan $|x^a| = \infty$ maka $|x| = |x^a| = \infty$. Berdasarkan proposisi 2, $x^n \neq 1$ dan sesuai defenisi, $x^n = x^{-n}$ maka berakibat $x^{-n} \neq 1$ sehingga dapat ditulis,

$$x^n = x^{-n} \neq 1$$

$$(x^1)^n = (x^{-1})^n \neq 1$$

Yang berarti bahwa bentuk $(x^a)^n = (x^1)^n = (x^{-1})^n \neq 1$ sedemikian sehingga $a = \pm 1$.
Sehingga terbukti.

Bukti 2:
Jika $|x| = n < \infty$, proposisi 2 mengatakan x menghasilkan subgrup dari H dari order $|x^a|$. Subgrup ini sama dengan H jika dan hanya jika $|x^a| = |x|$. dengan proposisi 5,

$$|x^a| = |x| \text{ jika dan hanya jika } \frac{n}{(a,n)} = n,$$ yaitu jika dan hanya jika $(a, n) = 1$.
Karena $\varphi(n)$ adalah defenisi, jumlah dari $a \in \{1, 2, \dots, n\}$ sedemikian sehingga $(a, n) = 1$, ini adalah jumlah generator dari H..

Contoh.
Proposisi 6 menjelaskan dengan tepat kelas residu mana yang $\overline{a}$ mod n menghasilkan $\mathbb{Z}/n\mathbb{Z}$: anggap $\overline{a}$ menghasilkan $\mathbb{Z}/n\mathbb{Z}$ jika dan hanya jika $(a, n) = 1$. Misalnya 1, 5, 7 dan 11 adalah generator $\mathbb{Z}/12\mathbb{Z}$ dan $\varphi(12) = 4$.

TEOREMA 7

Diberikan $H = \langle x \rangle$ merupakan grup siklik.

1. Setiap subgrup H adalah siklik. Lebih tepatnya, jika $K \leq H$, maka $K = \{1\}$ atau $K = \langle x^d \rangle$, dimana d adalah bilangan bulat positif terkecil sehingga $x^d \in K$.
2. Jika $|H| = \infty$, maka untuk sembarang bilangan bulat tak negatif yang berbeda a dan b, $x^a \neq x^b$. Selanjutnya untuk setiap bilangan bulat m, $\langle x^m \rangle = \langle x^{|m|} \rangle$, dimana $|m|$ menyatakan nilai mutlak m, sehingga subgrup nontrivial dari H berkorespondensi secara bijektif dengan bilangan bulat $1, 2, 3, \ldots$
3. Jika $|H| = n < \infty$, maka untuk setiap bilangan bulat positif a yang membagi n terdapat subgrup unik dari H orde a. Subgrup ini adalah grup siklik $\langle x^d \rangle$, dimana $d = \frac{n}{a}$. Selanjutnya untuk setiap bilangan bulat m, $\langle x^m \rangle = \langle x^{(n,m)} \rangle$, sehingga subgrup dari H berkorespodensi secara bijektif dengan pembagi positif dari n.

Bukti (1)

Diberikan $K \leq H$. Jika $K = 1$, proposisi benar untuk subgrup ini, jadi kita asumsikan $K \neq *1+$. Jadi ada beberapa $a \neq 0$ sedemikian sehingga $x^a \in K$. Jika $a < 0$ maka karena K adalah grup $x^{-a} = (x^a)^{-1} \in K$. Oleh karena itu K selalu terdapat beberapa pangkat positif dari x. Misalkan

$$P = \{b | b \in \mathbb{Z}^+ dan\, x^b \in K\}$$

Dengan persamaan di atas, P adalah himpunan tak kosong dari bilangan bulat positif. Dengan prinsip penataan sumur (bagian 0.2) P memiliki elemen minimun, sebut saja d. Karena K adalah subgrup dan $x^d \in K$, $\langle x^d \rangle \leq K$. Karena K adalah subgrup dari H, setiap elemen dari K berbentuk x^auntuk suatu bilangan bulat a. Dengan Algoritma Pembagian, kita dapat menulis

$$a = qd + r, 0 \leq r < d.$$

Maka $x^r = x^{(a-qd)} = x^a (x^a)^{-q}$ adalah elemen dari K karena kedua x^a dan x^b adalah elemen dari K. Dengan minimalitas dari d mengikuti, maka $r = 0$, yaitu $a = qd$ dan $x^a = (x^d)^\wedge q \in \langle x^d \rangle$. Ini memberikan penahanan terbalik $K \leq \langle x^d \rangle$ yang membuktikan (1).

Bukti (2)

Asumsikan $|H| = \infty$ dan misalkan terdapat $a, b \in \mathbb{Z}^+ + \{0\}$, msks berdasarkan proposisi 2, $x^a \neq x^b$ sehingga $a \neq b$ yang berakibat $\langle x^a \rangle \neq \langle x^b \rangle$

Selanjutnya jika terdapat m$\in \mathbb{Z}$ maka terdapat $\langle x^m \rangle$. Sesuai dengan sifat nilai mutlak yaitu $|m| = m$ sedemikian hingga $\langle x^m \rangle = \langle x^{|m|} \rangle$

Misalkan $m = \{1,2,3, \dots\}$ maka terdapat $\langle x^m \rangle = \langle x^{|m|} \rangle$ yang merupakan subgrup nontrivial dari H yang berkorespodensi secara bijektif dengan bilangan bulat 1,2,3, ...

Bukti (3)

Asumsikan $H = n < \infty$ dan $a|n$. Misalkan $d = \frac{n}{a}$ dan terapkan proposisi 5(3) untuk memperoleh bahwa $\langle x^d \rangle$ adalah subgrup dari orde a, yang menunjukkan adanya subgrup dari orde a. Untuk menunjukkan keunikan, misalkan K adalah sembarang subgrup dari H orde a. Pada bagian (1) kita memiliki,

$$K = \langle x^b \rangle$$

Dimana b adalah bilangan bulat positif terkecil sehingga $x^b \in K$. Dengan proposisi 5,

$$\frac{n}{d} = a = |K| = |x^b| = \frac{n}{(n,b)},$$

Jadi $d = (n, b)$. Secara khusus, $d|b$. Karena b adalah kelipatan dari d, $x^b \in \langle x^d \rangle$, maka

$$K = \langle x^b \rangle \leq \langle x^d \rangle$$

Karena $|\langle x^d \rangle| = a = |K|$, kita mempunyai $K = \langle x^d \rangle$.

Pernyataan terakhir dari (3) mengikuti dari pengamatan bahwa $\langle x^m \rangle$ adalah subgrup dari $\langle x^{(n,m)} \rangle$ dan, ini mengikuti dari proposisi 5(2) dan proposisi (2) bahwa mereka memiliki urutan yang sama. Karena (n, m) pasti merupakan pembagi dari n, ini menunjukkan bahwa setiap subgrup H muncul dari pembagi dari n, hal ini melengkapi pembuktian.

Contoh

1. Kita dapat menggunakan proposisi 6 dan teorema 7 untuk mendaftar semua subgrup $\mathbb{Z}/n\mathbb{Z}$ untuk n tertentu. Misalnya untuk contoh, subgrup dari $\mathbb{Z}/12\mathbb{Z}$ adalah

a) $\mathbb{Z}/12\mathbb{Z} = \langle 1\rangle = \langle 5\rangle = \langle 7\rangle = \langle\overline{11}\rangle$ (order 12)
b) $\langle 2\rangle = \langle\overline{10}\rangle$ (order 6)
c) $\langle 3\rangle = \langle 9\rangle$ (order 4)
d) $\langle 4\rangle = \langle 8\rangle$ (order 3)
e) $\langle 6\rangle$ (order 2)
f) $\langle 0\rangle$ (order 1)

Inklusi di antara mereka diberikan oleh,
$\langle a\rangle \leq \langle b\rangle$ jika dan hanya jika $(b,12)|(a,12)$, $1 \leq a, b \leq 12$

2. Kita juga dapat menggabungkan hasil dari bagian ini dengan yang sebelumnya. Sebagai contoh, kita dapat memperoleh subgrup dari grup G dengan membentuk $C_G(\langle x\rangle)$ dan $N_G(\langle x\rangle)$, untuk setiap $x \in G$.
Kita dapat memeriksa bahwa elemen g di G bergerak dengan x jika dan hanya jika g bergerak dengan semua pangkat x, maka

$$C_G(\langle x\rangle) = C_G(x)$$

Sebagaimana dicatat dalam latihan 6, bagian 2, $\langle x\rangle \leq N_G(\langle x\rangle)$ tetapi kesetaraan tidak berlaku. Misalnya, jika $G = Q_8$ dan $x = i$,
$C_G(i) = \{\pm 1, \pm i\} = \langle i\rangle$ dan $N_G(\langle i\rangle) = Q_8$

Terima Kasih

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik.