

Elementär gruppteori, v.38

Produkter av grupper

Det är ofta fördelaktigt att framställa en komplicerad grupp G som en direkt produkt av enklare grupper $H_1, \dots, H_n$, eller visa att G är isomorf med en dylik produkt, $G \cong H_1 \times H_2 \times \dots \times H_n$. Bekant från analysen är den naturliga produkten $\langle \mathbb{R}^n, + \rangle$ av ordnade n -tupler försedda med addition

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n).$$

Produkter av grupper

Definition. Antag att vi har grupperna $\langle G, * \rangle$ och $\langle H, \diamond \rangle$. Då definieras den direkta produkten $G \times H$ av G och H som mängden av ordnade elementpar (a, b) , där $a \in G$ och $b \in H$, försedd med operationen

$$(a_1, b_1) \cdot (a_2, b_2) = (a_1 * a_2, b_1 \diamond b_2) \in G \times H.$$

Anmärkning. a) Analog definition för n stycken grupper.

b) Om G och H är av ändlig ordning gäller $|G \times H| = |G| |H|$.

Produkter av grupper

Påstående: $G \times H$ är en grupp.

Bevis: Antag att $(a_1, b_1), (a_2, b_2) \in G \times H$. Då erhålls att

$$(a_1, b_1) \cdot (a_2, b_2) = (\underbrace{a_1 * a_2}_{\in G}, \underbrace{b_1 \diamond b_2}_{\in H}) \in G \times H.$$

så $\cdot$ är en operation på $G \times H$.

Produkter av grupper

(i) Nu gäller kalkylerna

$$\begin{aligned}(a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, b_3)) &= (a_1, b_1) \cdot (a_2 * a_3, b_2 \diamond b_3) \\ &= (a_1 * (a_2 * a_3), b_1 \diamond (b_2 \diamond b_3)) \\ &= ((a_1 * a_2) * a_3, (b_1 \diamond b_2) \diamond b_3) \\ &= (a_1 * a_2, b_1 \diamond b_2) \cdot (a_3, b_3) \\ &= ((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3),\end{aligned}$$

så operationen $\cdot$ är associativ.

Produkter av grupper

(ii) Låt e och e' vara neutrala element i G respektive H . För $(a, b) \in G \times H$ gäller

$$(e, e') \cdot (a, b) = (e * a, e' \diamond b) = (a, b),$$

$$(a, b) \cdot (e, e') = (a * e, b \diamond e') = (a, b),$$

och därmed är (e, e') det neutrala elementet i $G \times H$.

(iii) Tag nu $(a, b) \in G \times H$ och betrakta likheterna

$$(a^{-1}, b^{-1}) \cdot (a, b) = (a^{-1} * a, b^{-1} \diamond b) = (e, e'),$$

$$(a, b) \cdot (a^{-1}, b^{-1}) = (a * a^{-1}, b \diamond b^{-1}) = (e, e'),$$

som ger att $(a, b)^{-1} = (a^{-1}, b^{-1})$.

Då har vi visat att $G \times H$ är en grupp. $\square$

Exempel. $Z_6 \cong Z_2 \times Z_3$. (Hemuppgift).

Produkter av grupper

I allmänhet gäller det **inte** att $Z_{mn} \cong Z_m \times Z_n$.

$$(Z_{mn} \cong Z_m \times Z_n \Leftrightarrow \text{sgd}(m, n) = 1)$$

Exempel. Betrakta $Z_2 \times Z_2$ och Kleins fyragrupp. (Se föreläsningssanteckningar).

Struktursatsen för ändliga Abel'ska grupper.

Sats. En ändlig Abel'sk grupp G är alltid isomorf med en ändlig produkt av cykliska grupper,

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \dots \times \mathbb{Z}_{p_n^{r_n}},$$

där $p_1, \dots, p_n$ är (icke nödvändigtvis olika) primtal och $r_1, \dots, r_n$ är positiva heltal.

Produkter av grupper

Ex) Samtliga Abelska grupper av ordning 20.

$$20 = 2 \cdot 2 \cdot 5$$

$$\begin{cases} G_1 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5, \\ G_2 = \mathbb{Z}_4 \times \mathbb{Z}_5. \end{cases}$$

Två Abelska grupper (i isomorfismen)

av ordning 20.

$$\text{Av dem är } G_2 = \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20},$$

så G_2 är cyclisk.

Undergrupper

Betrakta grupperna $\langle R, + \rangle$ och $\langle Z, + \rangle$ försedda med samma operation (addition). Då $Z \subset R$ är det naturligt att kalla $\langle Z, + \rangle$ en delgrupp av $\langle R, + \rangle$.

Definition. Antag att vi har en grupp $\langle G, * \rangle$. Om $H \subseteq G$ och $\langle H, * \rangle$ är en grupp, så kallas $\langle H, * \rangle$ en undergrupp (delgrupp) till gruppen $\langle G, * \rangle$.

Undergrupper

Anmärkning. a) $\langle G, * \rangle$ och $\langle \{e\}, * \rangle$ kallas de triviala undergrupperna till $\langle G, * \rangle$.

b) Om e och e' är de neutrala elementen i $\langle G, * \rangle$ respektive $\langle H, * \rangle$, så gäller $e' * e' = e' = e' * e$, vilket enligt Sats 12 (i) medför att $e' = e$. Vi har därmed samma neutrala element i båda grupperna.

Undergrupper

Sats 17. Givet en grupp $\langle G, * \rangle$ och $H \subseteq G$. Då är $\langle H, * \rangle$ en undergrupp till $\langle G, * \rangle$ om och endast om både 1) och 2) gäller:

- 1) $H \neq \emptyset$;
- 2) $a, b \in H \Rightarrow a * b^{-1} \in H$, där b^{-1} är inversen till b i G .

Bevis: (Hemuppgift).

Speciellt för ändliga grupper gäller:

Undergrupper

Sats 18. Givet en ändlig grupp $\langle G, * \rangle$ och $H \subseteq G$. Då är $\langle H, * \rangle$ en undergrupp till $\langle G, * \rangle$ om $H \neq \emptyset$ och $a, b \in H \Rightarrow a * b \in H$.

För beviset behövs ett hjälpresultat:

Lemma 19. Låt a vara ett element i den ändliga gruppen $\langle G, * \rangle$. Då finns det ett minsta positivt heltal n med $a^n = e$. Vidare gäller det att gruppelmenten $a = a^1, a^2, a^3, \dots, a^{n-1}, a^n = e$ är olika.

Undergrupper

Bevis: Klart om $a = e$. Antag att $a \neq e$ och betrakta i G elementföljden $a, a^2, a^3, \dots$. Då G är ändlig måste följden ha element som upprepar sig. Välj en sådan upprepning:

$$a^p = a^q$$

med $p > q$. Multiplikation av båda leden med a^{-q} ger:

$$a^{p-q} = e,$$

där $p-q > 0$. Alltså $a^m = e$ för $m = p-q > 0$. Låt n vara det minsta positiva heltal med denna egenskap. (Ett sådant tal existerar). Nu är alla element $a, a^2, \dots, a^n$ olika, ty om $a^i = a^j$ för $1 \leq j < i \leq n$ så gäller det att $a^{i-j} = e$ med $1 \leq i-j < n$, vilket strider mot definitionen av n . $\square$

Undergrupper

Bevis av Sats 18: Tag $a \in H$. Upprepad användning av antagandet $a, b \in H \Rightarrow a * b \in H$ ger att

$$a^k \in H \text{ för alla } k \geq 1. \quad (*)$$

Om $H = \{e\}$, så är H en undergrupp av G . Om $H \neq \{e\}$, så väljer vi $a \in H$ sådant att $a \neq e$. Då G är en ändlig grupp ger Lemma 19 att det finns ett $k_0 > 1$ med

$$a^{k_0} = e.$$

Undergrupper

att det finns ett $k_0 > 1$ med

$$a^{k_0} = e.$$

Multiplicera med a^{-1} och erhåll: $a^{k_0-1} = a^{-1}$. Emedan $k_0 - 1 \geq 1$ ger nu (*) att

$$a \in H \Rightarrow a^{-1} = a^{k_0-1} \in H.$$

Tag nu $a, c \in H$. Då gäller det att $a, c^{-1} \in H$ och vidare att $a * c^{-1} \in H$, (med stöd av antagandet $a, b \in H \Rightarrow a * b \in H$). Men då ger Sats 17 att $\langle H, * \rangle$ är en undergrupp till $\langle G, * \rangle$. $\square$

Symmetri

Allmänt uttryckt är symmetrin av ett objekt en omordning av objektet så att alla dess väsentliga grunddrag bevaras. Hos månghörningar betyder detta att hörn omplaceras till hörn och sidor till sidor.

Symmetrin hos regelbundna månghörningar och polyedrar kan med fördel studeras med hjälp av permutationsgrupper.

Symmetri

Låt oss betrakta en regelbunden n -hörning M för vilken vi numrerar hörnen moturs med talen $1, 2, \dots, n$ och antar att $n \geq 3$. Symmetrierna hos M ges då av rotationer moturs samt speglingar i symmetriaxlar.

Exempel. Fallet $n = 3$ (Se föreläsningsanteckningar).

Symmetri

Definiera nu permutationerna $R, S_p \in S_n$ genom

$$R = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix},$$
$$S_p = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}.$$

Då gäller

$$R^{k+1} \circ S_p = R \circ (R^k \circ S_p) = \dots = S_p \circ R^{-k} \quad (*)$$
$$R^k \circ S_p = S_p \circ R^{-k},$$

för $k = 0, 1, \dots, n-1$. (~~Se föreläsningsanteckningar~~). (Hemuppgift)

Symmetri

Alla "tänkbara placeringar av M " fås genom att upprepa R och S_p , (S_p vänder på M , R roterar på M). Definiera nu

$$H = \{R^l, R^k \circ S_p : l = 0, \dots, n-1, k = 0, \dots, n-1\}.$$

Påstående: $\langle H, \circ \rangle$ är en grupp.

Bevis: Vi betraktar fyra fall och utnyttjar formel (*) ovan.

1) Betrakta $R^{l_1} \circ R^{l_2}$. Om $l_1 + l_2 \leq n-1$ gäller det att $R^{l_1} \circ R^{l_2} = R^{l_1+l_2} \in H$. Om $l_1 + l_2 \geq n$ har vi $R^{l_1} \circ R^{l_2} = R^{n+(l_1+l_2-n)} = e \circ R^{l_1+l_2-n} \in H$.

- 2) Betrakta $(R^k \circ S_p) \circ R^l$. Vi antar att $k - l \geq 0$ och tillämpar
 (*): $(R^k \circ S_p) \circ R^l = (S_p \circ R^{-k}) \circ R^l = S_p \circ R^{l-k} = R^{k-l} \circ S_p \in H$.
 Om vi antar att $k - l < 0$ erhålls $(R^k \circ S_p) \circ R^l = (S_p \circ R^{-k}) \circ R^l = S_p \circ R^{n+(l-k-n)} = S_p \circ e \circ R^{l-k-n} = R^{n+k-l} \circ S_p \in H$.
 3) $R^l \circ (R^k \circ S_p) = (R^l \circ R^k) \circ S_p = R^{l+k} \circ S_p \in H$.

$$4) \quad (R^{k_1} \circ S_p) \circ (R^{k_2} \circ S_p) \stackrel{4.1}{=} R^{k_1} \circ S_p \circ (S_p \circ R^{-k_2}) = R^{k_1} \circ R^{-k_2}.$$

Om $k_1 - k_2 \geq 0$ så är det sista ledet lika med $R^{k_1-k_2} \in H$. Om

$k_1 - k_2 < 0$ så får vi efter sammansättning med $e = R^n$ att det sista
ledet är lika med $R^{n+(k_1-k_2)} \in H$.

Vi har alltså visat att $a, b \in H \Rightarrow a \circ b \in H$ och då ger Sats 18 att
 H är en undergrupp till S_n . $\square$

Symmetri

Alla symmetrier av M bildar då gruppen $D_n = \langle H, \sigma \rangle$ som kallas diedergruppen. Denna grupp av permutationer är en undergrupp till S_n .

Ordningen för diedergruppen är $|D_n| = 2n$, ty vi har $2n$ olika permutationer, n rotationer R^k och n stycken sammansättningar av speglingen S_p med rotationen R^k , dvs $R^k \circ S_p$.

Vi observerar att D_n är en äkta (icke-trivial) undergrupp av S_n då $n \geq 4$, ty då är $2n = |D_n| < |S_n| = n!$. Vidare noterar vi att D_n "byggs upp" av R och S_p , dvs. D_n genereras av $\{R, S_p\}$.

Notera även att D_n är en icke-Abelsk grupp

Generering av grupper

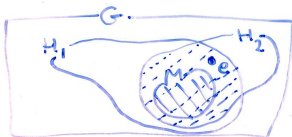
Generering av grupper

Låt $\langle G, * \rangle$ vara en grupp och tag en icke-tom delmängd M av G . Tag snittet av alla undergrupper H till G som innehåller M . Beteckna detta snitt med $\langle M \rangle$, alltså

$$\langle M \rangle = \bigcap_{\substack{M \subseteq H \\ H \text{ delgr. av } G}} H.$$

Påstående. $\langle \langle M \rangle, * \rangle$ är en undergrupp till G .

Bevis: Vi har att $e \in \langle M \rangle \neq \emptyset$, ty $e \in H$ för varje undergrupp H av G



44

$$\langle M \rangle = \dots$$

Generering av grupper

Tag $a, b \in \langle M \rangle$. Detta medför att $a, b \in H$ för alla undergrupper H sådana att $M \subseteq H$. Då gäller det att $a, b^{-1} \in H$ för alla undergrupper H sådana att $M \subseteq H$. Av detta följer att $a * b^{-1}$ tillhör alla undergrupper H sådana att $M \subseteq H$. Därmed gäller det att $a * b^{-1} \in \langle M \rangle$. Då ger Sats 17 att $\langle \langle M \rangle, * \rangle$ är en undergrupp till G .
 $\square$

Anmärkning. $\langle M \rangle$ är den minsta undergruppen till G som innehåller M .

Generering av grupper

Definition. Givet en grupp $\langle G, * \rangle$ och en icke-tom delmängd M av G . Då kallas $\langle M \rangle$ undergruppen till G genererad av M och M kallas generator för undergruppen $\langle M \rangle$.

Generering av grupper

Sats 20. Elementen i $\langle M \rangle$ är de element i G som kan skrivas som $a_1 \cdot a_2 \cdot \dots \cdot a_k$, där $a_i \in M$ eller $a_i^{-1} \in M$, för $k = 1, 2, \dots$.

Bevis: Definiera

$$H = \{a_1 \cdot a_2 \cdot \dots \cdot a_k : a_i \in M \text{ eller } a_i^{-1} \in M, k = 1, 2, \dots\}.$$

Klart att $M \subseteq H$ och att $H \neq \emptyset$. Tag $a = a_1 \cdot a_2 \cdot \dots \cdot a_k \in H$ och $b = b_1 \cdot b_2 \cdot \dots \cdot b_l \in H$. Då är $a^{-1} = a_k^{-1} \cdot a_{k-1}^{-1} \cdot \dots \cdot a_2^{-1} \cdot a_1^{-1} \in H$. Därmed gäller det att $ba^{-1} = b_1 \cdot b_2 \cdot \dots \cdot b_l \cdot a_k^{-1} \cdot a_{k-1}^{-1} \cdot \dots \cdot a_1^{-1} \in H$. Sats 17 ger då att H är en undergrupp till G . Vidare gäller att $\langle M \rangle \subseteq H \subseteq G$. Definitionen på H ger att $H \subseteq \langle M \rangle$, ty $a_1 \cdot a_2 \cdot \dots \cdot a_k$ tillhör varje undergrupp som M är delmängd av, och därmed även snittet $\langle M \rangle$. Alltså gäller det att $H = \langle M \rangle$. $\square$

Generering av grupper

Exempel. $Z \times Z = \langle \{(1, 0), (0, 1)\} \rangle$ då operationen är addition. (Se föreläsningsanteckningar).

Anmärkning. Om G är en cyklisk grupp så finns det ett element $a \in G$ sådant att $G = \{a^k : k \in Z\}$. Med andra ord gäller $G = \langle a \rangle$, dvs. den undergrupp som genereras av a är hela G , a är därmed generator för G .