Elementär gruppteori, v.37

Permutationsgrupper

Definition. *Låt M vara en icke-tom mängd. En bijektiv avbildning $f : M \to M$ kallas en permutation av M. Gruppen av permutationer av M, betecknad $\mathrm{Sym}(M)$, definieras av*

$$\mathrm{Sym}(M) = \langle \{f : M \to M, \text{ sådana att } f \text{ är en permutation av } M\}, \circ \rangle,$$

där operationen $\circ$ betecknar funktionssammansättning.

Permutationsgrupper

Påstående: $\mathrm{Sym}(M)$ är en grupp.

Bevis: Om f, g är permutationer så är de bijektiva avbildningar från M till M. Då är även $f \circ g$ en bijektiv avbildning från M till M (Algebra A), vilket ger att $f \circ g$ är en permutation. Därmed är $\mathrm{Sym}(M)$ sluten under operationen $\circ$.

(i) För varje $x \in M$ gäller att

$$\begin{aligned}(f \circ (g \circ h))(x) &= f((g \circ h)(x)) = f(g(h(x))) \\ &= (f \circ g)(h(x)) = ((f \circ g) \circ h)(x)\,.\end{aligned}$$

Då är $f \circ (g \circ h) = (f \circ g) \circ h$ och $\circ$ är associativ.

Permutationsgrupper

(ii) Definiera avbildningen $id : M \to M$ genom $id(x) = x$ för alla $x \in M$. Då är id det neutrala elementet, ty för alla $x \in M$ är

$$f(x) = (f \circ id)(x) = (id \circ f)(x),$$

så $f \circ id = id \circ f = f$ för alla $f \in \mathrm{Sym}(M)$.

Permutationsgrupper

(iii) Om f är en permutation så är f en bijektiv avbildning från M till M. Då är även f^{-1} en bijektiv avbildning från M till M och därmed en permutation. Vidare gäller för alla $x \in M$ att

$$(f \circ f^{-1})(x) = (f^{-1} \circ f)(x) = x = id(x),$$

så $f \circ f^{-1} = f^{-1} \circ f = id$.

Därmed är $\mathrm{Sym}(M)$ en grupp. $\square$

Permutationsgrupper

Definition. *För* $M = \{1, 2, ..., n\}$, $n \geq 1$, *definierar vi*

$$S_n = \mathrm{Sym}(M) = \mathrm{Sym}(\{1, 2, ..., n\}) .$$

S_n *kallas symmetriska gruppen av grad* n.

Observera att elementen i S_n är permutationer, inte talen $1, 2, ..., n$.

Permutationsgrupper

En permutation $f \in S_n$ kan representeras som

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix},$$

varvid det neutrala elementet e och inversen f^{-1} representeras som

$$e = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix} \text{ och } f^{-1} = \begin{pmatrix} f(1) & f(2) & \cdots & f(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Exempel. Om $n \geq 3$ så är S_n **inte en Abelsk grupp.** (Se föreläsningsanteckningar).

* eller:

$$f^{-1} = \begin{pmatrix} 1 & 2 & \cdots & n \\ f^{-1}(1) & f^{-1}(2) & \cdots & f^{-1}(n) \end{pmatrix}$$

Permutationsgrupper

Med stöd av föregående exempel och Sats 14 erhåller vi att om $n \geq 3$ så är S_n **inte en cyklisk grupp.** (Sats 14 : Cyklisk => Abelsk)

Antalet permutationer av $\{1, 2, ..., n\}$ är $n!$, dvs. $|S_n| = n!$ ($|S_1| = 1, |S_2| = 2, |S_3| = 6, |S_4| = 24, ...$).

Permutationsgrupper

Definition. *Om en permutation $g \in S_n$ permuterar de r olika elementen $k_1, k_2, ..., k_r$ cykliskt, vilket betyder att*

$$g(k_1) = k_2, g(k_2) = k_3, ..., g(k_{r-1}) = k_r, g(k_r) = k_1$$

och om de övriga elementen i $\{1, 2, ..., n\}$ lämnas fixa, så kallas g en cykel och betecknas

$$g = (k_1\, k_2 \ldots k_r)\,.$$

Exempel. (Se föreläsningsanteckningar).

Permutationsgrupper

Definition. *Två cykler i S_n kallas disjunkta om de inte innehåller något gemensamt element.*

Exempelvis är (123) och (45) disjunkta, men inte (123) och (35).

Permutationsgrupper

Lemma 15. *Om f och g är disjunkta cykler i S_n, så gäller $f \circ g = g \circ f$.*

Bevis: Tag godtyckligt $k \in \{1, 2, ..., n\}$. Ett av tre fall kan inträffa:

Fall 1: Antag att $f(k) = i \neq k$. Då är $g(k) = k$ och $g(i) = i$, varför

$$(g \circ f)(k) = g(f(k)) = f(k) = f(g(k)) = (f \circ g)(k)\,.$$

Fall 2: Antag att $g(k) = j \neq k$. Analogt med Fall 1.

Fall 3: Antag att $f(k) = k$ och $g(k) = k$. Då är

$$(g \circ f)(k) = g(f(k)) = g(k) = k = f(k) = f(g(k)) = (f \circ g)(k)\,.$$

Därmed är $f \circ g = g \circ f$ för disjunkta cykler i S_n. $\square$

Permutationsgrupper

Låt oss nu fortsätta med vårt tidigare exempel. Emedan cyklerna är disjunkta är ordningsföljden irrelevant och vi får

$$
\begin{aligned}
(143) \circ (25) &= (25) \circ (143) \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 3 & 2 \end{pmatrix} = f \, .
\end{aligned}
$$

Exempel. (Se föreläsningsanteckningar).

Permutationsgrupper

Sats. *Varje $f \in S_n$ är antingen en cykel eller produkten av disjunkta cykler i S_n.*

Observera att en permutation som är en cykel kan framställas med flera olika cykelbeteckningar, exempelvis för $f = (1423)$ i S_4 gäller det att

$$f = (4231) = (2314) = (3142) = (1423)\,.$$

Neutrala elementet i S_n kan skrivas som

$$e = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix} = (1)(2)...(n) = (1) = (2) = ... = (n)\,.$$

Vi avslutar detta avsnitt med ett antal exempel (se föreläsningsanteckningar).

Permutationsgrupper

Ex] Kortpacke med 13 spadrkort + Joker med bildsidan nedåt i ordningen:

A, 2, ..., 10, kn, D, K, J.

Utför perfekta omblandningar: dela högen i två delar med sju kort var och blandar korten turvis om varandra så att A alltid är underst och J alltid överst.

Hur många omblandningar krävs för att återställa den ursprungliga ordningen?

Isomorfa grupper

När är två grupper väsentligen lika? Denna fråga kan besvaras med hjälp av begreppet isomorfi för grupper. Först skall vi dock införa begreppet homomorfi för algebraiska strukturer:

Definition. *Antag att* $\langle G, * \rangle$ *och* $\langle H, \diamond \rangle$ *är algebraiska strukturer och att* $f : G \to H$. *Då kallas* f *en homomorfi om det för alla* $a, b \in G$ *gäller att*

$$f(a * b) = f(a) \diamond f(b) .$$

Isomorfi

Homomorfivillkoret betyder att varje likhet $z = x * y$ i G medför likheten $f(z) = f(x) \diamond f(y)$ i H.

Exempelvis är avbildningen $f : Z\backslash\{0\} \to Z_+$ given av $f(x) = x^2$ en homomorfi mellan de algebraiska strukturerna $\langle Z\backslash\{0\}, \cdot\rangle$ och $\langle Z_+, \cdot\rangle$, ty $f(x\,y) = (x\,y)^2 = x^2y^2 = f(x)\,f(y)$.

Isomorfi

Definition. *Två grupper* $\langle G, * \rangle$ *och* $\langle H, \diamond \rangle$ *är isomorfa, vilket betecknas* $\langle G, * \rangle \cong \langle H, \diamond \rangle$, *om det finns en bijektion* $\varphi : G \to H$ *sådan att för alla* $a, b \in G$ *gäller att*

$$\varphi(a * b) = \varphi(a) \diamond \varphi(b) .$$

Då säger vi att φ *är en isomorfism.*

$\left(a * b = \varphi^{-1}(\varphi(a) \diamond \varphi(b)) \right)$

Exempel. Z_2 och S_2 är isomorfa. (Se föreläsningsanteckningar).

Isomorfi

Det gäller att $|S_3| = |Z_6| = 6$. Är grupperna isomorfa? Vi har tidigare noterat att Z_6 är Abelsk men inte S_3. Med stöd av följande lemma kan vi ge ett nekande svar på frågan.

Lemma 16. *Om gruppen $\langle G, * \rangle$ är Abelsk och $\langle G, * \rangle \cong \langle H, \diamond \rangle$, så är även $\langle H, \diamond \rangle$ en Abelsk grupp.*

Bevis: Låt $\varphi : G \to H$ vara en isomorfism. Tag godtyckliga $x, y \in H$. Då finns det element $a, b \in G$ sådana att $\varphi(a) = x$ och $\varphi(b) = y$. Vidare gäller det att

$$x \diamond y = \varphi(a) \diamond \varphi(b) = \varphi(a * b) = \varphi(b * a) = \varphi(b) \diamond \varphi(a) = y \diamond x\,,$$

så $\langle H, \diamond \rangle$ är en Abelsk grupp. $\square$