
PERMUTATIONER

Definition. En **permutation** av en mängd S är en bijektiv funktion $\sigma : S \to S$. Mängden av alla permutationer bildar en grupp $Sym(S)$ under sammansättningen (se exempel 4 (c)). Om $S = \{1, 2, \ldots, n\}$ betecknar man $Sym(S)$ med S_n. För att beskriva elementen i S_n använder man tabellbeteckningen:

Om $\sigma(1) = a_1$, $\sigma(2) = a_2, \ldots, \sigma(n) = a_n$ kommer vi att skriva

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ a_1 & a_2 & \ldots & a_n \end{pmatrix}$$

Antalet ellement i S_n är $n!$

Permutationer kan presenteras mera kompakt. Låt $p_1, p_2, \ldots, p_k \in \{1, 2, \ldots, n\}$ och låt $(p_1, p_2, \ldots, p_k)$ beteckna funktionen $\sigma(p_1) = p_2$, $\sigma(p_2) = p_3, \ldots, \sigma(p_k) = p_1$ och $\sigma(i) = i$, då $i \neq p_1, \ldots, p_k$. T.ex. $(1, 2, 3)$ är beteckningen på $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.

$(p_1, p_2, \ldots, p_k)$ kallas för en **cykel av längd** k.

Om $f = (p_1, p_2, \ldots, p_k)$ och $g = (p'_1, p'_2, \ldots, p'_k)$, där alla tal p_1, $p_2, \ldots, p_k$, p'_1, $p'_2, \ldots, p'_k$ är olika då säger man att f och g är disjunkta cykler.

För två disjunkta cykler ρ, $\sigma \in S_n$ gäller att $\rho\sigma = \sigma\rho$. Visa!

Varje permutation kan skrivas som en produkt av disjunkta cykler. Här följer ett enkelt recept: Man väljer ett tal p_1 som inte avbildas på sig självt. Därefter tar man bilden p_2 av p_1, bilden p_3 av p_2 osv tills man får p_1 igen. Då har man en cykel. Nu tar vi ett tal som inte ingår i första cykel och gör på samma sätt. T.ex. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} = (1, 4, 6)(2, 3)(5) = (1, 4, 6)(2, 3)$. Man brukar utelämna cykler av längd 1.

En cykel (a, b) av längd 2 kallas för **transposition**. En transposition byter alltså plats på två element och låter övriga vara.

Påstående. Varje permutation i S_n, $n \geq 2$, kan skrivas som en produkt av transpositioner.

Bevis. Övning 6.9 i kursboken.

En permutation i S_n, $n \geq 2$ kan skrivas som en produkt av antingen ett jämnt eller udda antal transpositioner.

En permutation i S_n kallas **jämn** eller **udda**, beroende på om den kan skrivas som ett jämnt eller udda antal transpositioner.

Exempel. Permutationen

$$\rho = (1, 7, 5, 2, 3)(6, 4) = (1, 3)(1, 2)(1, 5)(1, 7)(6, 4)$$

är udda.

Sats 7.2 Mängden av alla jämna permutationer bildar en grupp m a p sammansättningen och kallas för den alternerade gruppen för n element. Betecknas A_n.

Definition. En grupp $(G, *)$ kallas abelsk om

$$a * b = b * a \text{ då } a, b \in G$$

Sats 6.3. S_n är inte abelsk då $n \geq 3$.

DELGRUPPER

En **delgrupp** till en grupp G är en delmängd $H \subseteq G$ så att H bildar en grupp under samma operation som G. Om $H \neq G$ är H en äkta delgrupp. Om $H = \{e\}$ är H en trivial delgrupp.

Lemma. Låt G vara en grupp med operation $*$ och låt H vara en delgrupp till G. Då följande gäller:

(a) om f är det neutrala elementet i H och e är det neutrala elementet i G, så är $f = e$;

(b) om $a \in H$ så är inversen till a i H lika med inversen till a i G.

Bevis. (a) Eftersom f är det neutrala elementet i H, är $f * f = f$. Multiplicera likheten från höger med inversen f^{-1} till f i G. Tack vare associativiteten får vi

$$\begin{aligned} f^{-1} * (f * f) &= f^{-1} * f, \\ (f^{-1} * f) * f &= e, \\ e * f &= e, \\ f &= e. \end{aligned}$$

(b) Låt $a \in G$. Låt a^{-1} vara inversen till a i G och låt c vara inversen till a i H. Då är $a * c = c * a = f$ och därmed $a * c = c * a = e$, ty $e = f$ enligt (a). Detta innebär att c är inversen till a i G, dvs $c = a^{-1}$.

Sats 7.1. Låt G vara en grupp. En delmängd $H \subseteq G$ bildar en delgrupp om och endast om

(i) H är icke-tom;

(ii) $a * b \in H$ för alla $a, b \in H$;

(iii) $a^{-1} \in H$ för alla $a \in H$.

Bevis. $\Rightarrow$ Låt H vara en delgrupp till G. (i) gäller ty H har minst ett neutralt element; (ii) gäller, ty $*$ är en operation på H; (iii) gäller, ty om $a \in H$ så har a en invers a' i H och enligt lemma ovan a' är lika med inversen a^{-1} till a i G vilket ger $a^{-1} \in H$.

$\Leftarrow$ Låt H vara en delmängd till G som uppfyller (i), (ii) och (iii). (ii) betyder att $*$ är en operation på H. Associativiteten följer från att $*$ är associativ på hela G. Gruppens neutrala elementet e ligger i H eftersom om $a \in H$ (sådant element existerar enligt (i)) så är $a^{-1} \in H$ enligt (iii) och $e = a * a^{-1} \in H$ enligt (ii). Detta ger att e är ett neutralt element i H. Varje element $a \in H$ har en invers i H, nämligen a^{-1}, som ligger iH enligt (iii). Alltså är H en grupp m a p $*$.

Exempel 1. $U = \{z \in \mathbb{C} \mid |z| = 1\}$ är en delgrupp i $\mathbb{C} \setminus \{0\} = \mathbb{C}^*$ under multiplikation. (Visa!)

Exempel 2. Alla $(n \times n)$-matriser med reella element och med determinant lika med 1 är en delgrupp (betecknas $SL_n(\mathbb{R})$) till gruppen $GL_n(R)$ av alla $(n \times n)$-matriser med reella element och med determinant $\neq 0$ under matrismultiplikation. Vi har

$$A, B \in SL_n(\mathbb{R}) \Rightarrow \det A = 1 = \det B \Rightarrow \det(AB) = \det A \det B = 1 \Rightarrow AB \in SL_n(\mathbb{R})$$

vilket visar slutheten. Om $A \in SL_n(\mathbb{R})$ och A^{-1} är inversen till A så gäller $AA^{-1} = E$ (E är enhetsmatrisen), $1 = \det E =$

$\det AA^{-1} = \det A \det A^{-1}$ vilket ger nu $\det A^{-1} = 1$ så att $A^{-1} \in SL_n(\mathbb{R})$.

Exempel 3. De jämna permutationerna i S_n bildar en delgrupp - den **alternerande gruppen** (Sats 7.2).