6. Grupy a jejich podgrupy

Grupa $G = G(\cdot, {}^{-1}, \mathbf{1})$ je algebra taková, že $\cdot$ je asociativní binární operace, $\mathbf{1}$ je neutrální prvek a pro každý prvek $a \in G$ je a^{-1} prvek inverzní.

Z 2.16 plyne, že v každé grupě G jsou pro všechna $a, b \in G$ splněny identity $(a^{-1})^{-1} = a$ a $(ab)^{-1} = b^{-1}a^{-1}$.

Jestliže v monoidu $S(\cdot, \mathbf{1})$ jsou všechny prvky invertibilní, tak lze definovat na S unární operaci ${}^{-1}$ tak, že pro $a \in S$ je a^{-1} jeho (jednoznačně určený) inverzní prvek. Algebra $S(\cdot, {}^{-1}, \mathbf{1})$ je pak grupa. Rozdíl mezi grupami a monoidy, které jsou tvořeny výhradně invertibilními prvky, je tedy pouze formální, a spočívá v tom, zda přiřazení inverzního prvku je nebo není výslovně uvedeno v seznamu operací příslušné algebry.

Důsledek 2.17 může proto být formulován také tak, že invertibilní prvky libovolného monoidu tvoří grupu. Například invertibilní prvky monoidu $\mathbb{Z}(\cdot, 1)$ jsou 1 a -1, zatímco invertibilní prvky monoidů $\mathbb{Q}(\cdot, 1)$, $\mathbb{R}(\cdot, 1)$ a $\mathbb{C}(\cdot, 1)$ jsou všechna nenulová čísla příslušného číselného oboru. Tyto grupy jsou komutativní, příkladem nekomutativní grupy pro nás bude symetrická grupa S_Ω (binární operací je skládání permutací, unární operací inverzní permutace a nulární operací identická permutace).

Všimněte si, že existenci inverzních prvků v monoidu $S(\cdot, 1)$ lze také formulovat tak, že rovnice $a \cdot x = 1$ a $y \cdot a = 1$ jsou řešitelné pro každé $a \in S$ (viz 2.15). Ovšem pak jsou řešitelné i všechny rovnice tvaru $a \cdot x = b$ a $y \cdot a = b$, neboť lze položit $x = a^{-1}b$ a $y = ba^{-1}$.

Jestliže $G = G(\cdot, {}^{-1}, \mathbf{1})$ je grupa, tak z $ac = bc$ plyne $a = acc^{-1} = bcc^{-1} = b$ a z $ca = cb$ podobně plyne $a = b$. Znamená to, že $G(\cdot, \mathbf{1})$ je monoid s krácením. Rovnice $ax = b$ a $ya = b$ proto mají v grupách vždy právě jedno řešení.

6.1 Lemma. *Buď $G = G(\cdot, {}^{-1}, \mathbf{1})$ a $H = H(\cdot, {}^{-1}, \mathbf{1})$ dvě grupy a $f : G \to H$ zobrazení slučitelné s $\cdot$. Potom je f homomorfismus grup.*

Důkaz. Z $\mathbf{1}_G \cdot \mathbf{1}_G = \mathbf{1}_G$ plyne $f(\mathbf{1}_G) \cdot f(\mathbf{1}_G) = f(\mathbf{1}_G) = f(\mathbf{1}_G) \cdot \mathbf{1}_H$, takže $f(\mathbf{1}_G) = \mathbf{1}_H$. Z $aa^{-1} = \mathbf{1}_G$ plyne $f(a)f(a^{-1}) = f(\mathbf{1}_G) = \mathbf{1}_H$, takže $f(a^{-1}) = (f(a))^{-1}$. $\square$

V grupě $G = G(\cdot, {}^{-1}, \mathbf{1})$ definujeme i záporné mocniny. Je-li $a \in G$, $n \in \mathbb{N}$, tak $a^{-n} = (a^{-1})^n$. Podle 2.16 je zobrazení $a \mapsto a^{-1}$ bijekcí G.

6.2 Lemma. *Pro $a \in G$, $n \in \mathbb{Z}$ je $a^{-n} = (a^n)^{-1}$.*

Důkaz. Pro $n = 0$ zřejmé. Je-li $n = -m < 0$, je třeba ukázat $a^m = (a^{-m})^{-1}$, čemuž je ekvivalentní $(a^m)^{-1} = a^{-m}$. Stačí tedy ověřit, že $a^{-n} = (a^n)^{-1}$ platí pro $n > 0$. Postupujme indukcí, pro $n = 1$ je to zřejmé. Máme $a^{-n-1} = (a^{-1})^{n+1} = (a^{-1})^n \cdot a^{-1} = a^{-n} \cdot a^{-1} = (a^n)^{-1}a^{-1} = (aa^n)^{-1} = (a^{n+1})^{-1}$. $\square$

6.3 Lemma. *Pro $a \in G$, $n, m \in \mathbb{Z}$ je $a^n a^m = a^{n+m}$.*

Důkaz. Je-li $n = 0$ nebo $m = 0$, je vztah zřejmý. Je-li $n > 0$, $m > 0$, použij 5.1. Je-li $n < 0$, $m < 0$, je $a^n a^m = (a^{-n})^{-1}(a^{-m})^{-1} = ((a^{-m})(a^{-n}))^{-1} = (a^{-m-n})^{-1} = a^{n+m}$. Je-li $n > 0 > m$ a $n \geq -m$, tak $a^n a^m = a^{n+m}a^{-m}a^m = a^{n+m}$. Je-li $n > 0 > m$ a $-m > n$, tak $a^n a^m = a^n a^{-n} a^{m+n} = a^{m+n}$. Konečně, je-li $n < 0 < m$, je $a^n a^m = a^n a^{-n} a^{m+n} = a^{n+m}$. $\square$

6.4 Lemma. *Pro $a \in G$, $n, m \in \mathbb{Z}$ je $(a^n)^m = a^{nm}$.*

Důkaz. Je-li $n = 0$ nebo $m = 0$, je vztah zřejmý. Pro $n > 0$, $m > 0$ lze použít 5.1. Je-li $m > 0 > n$, je $(a^n)^m = ((a^{-n})^{-1})^m = ((a^{-n})^m)^{-1} = (a^{-nm})^{-1} = a^{nm}$. Je-li $m < 0$, je $(a^n)^m = ((a^n)^{-m})^{-1} = (a^{-nm})^{-1} = a^{nm}$. $\square$

Každá podgrupa generovaná jednoprvkovou množinou se nazývá *cyklická*.

6.5 Důsledek. *Buď G grupa a $a \in G$ její prvek. Pak $\{a^i;\ i \in \mathbb{Z}\}$ je cyklická podgrupa generovaná a.*

Důkaz. Množina $A = \{a^i;\ i \in \mathbb{Z}\}$ musí zjevně ležet v každé podgrupě, jež obsahuje a. Podle 6.2 a 6.3 je A uzavřena na $\cdot$ i $^{-1}$. $\square$

Řádem podgrupy grupy G se míní její mohutnost. Řád G se obvykle značí $|G|$. *Řád prvku* $a \in G$ je řád cyklické podgrupy generované a.

Buď H podgrupa grupy G. Definujme relaci $\mathrm{rmod}\, H$ tak, že prvky a, b jsou v této relaci (což zapisujeme $a \equiv b \,\mathrm{rmod}\, H$) právě když $ab^{-1} \in H$.

Podobně pišme $a \equiv b \,\mathrm{lmod}\, H$ právě když $a^{-1}b \in H$.

6.6 Lemma. *Relace* $\mathrm{rmod}\, H$ a $\mathrm{lmod}\, H$ *jsou ekvivalence.*

Důkaz. $a \equiv a \,\mathrm{rmod}\, H$, neboť $aa^{-1} = \mathbf{1} \in H$. Je-li $ab^{-1} \in H$, je $(ab^{-1})^{-1} = ba^{-1} \in H$, takže relace $\mathrm{rmod}\, H$ je symetrická. Ať $a \equiv b \,\mathrm{rmod}\, H$ a $b \equiv c \,\mathrm{rmod}\, H$. Pak $ac^{-1} = ab^{-1}bc^{-1} \in H$. $\square$

Jsou-li A, B dvě podmnožiny G, tak $A \cdot B = AB$ označuje množinu $\{cd;\ c \in A, d \in B\}$. Pro $a, b \in G$ místo $\{a\}B$, $A\{b\}$ píšeme prostě aB, Ab.

6.7 Lemma. *Buď $a \in G$. Pak $[a]_{\mathrm{rmod}\, H} = Ha$ a $[a]_{\mathrm{lmod}\, H} = aH$. Přitom platí, že* $\mathrm{card}[a]_{\mathrm{rmod}\, H} = |H| = \mathrm{card}[a]_{\mathrm{lmod}\, H}$.

Důkaz. Ať $b \equiv a \,\mathrm{rmod}\, H$. Pak $b = ba^{-1}a \in Ha$. Naopak $ha \equiv a \,\mathrm{rmod}\, H$ pro každé $h \in H$, neboť $haa^{-1} = h \in H$. Je tedy $[a]_{\mathrm{rmod}\, H} = Ha$. Zobrazení $h \mapsto ha$ je bijekce H na Ha, takže $\mathrm{card}(Ha) = \mathrm{card}(H) = |H|$. $\square$

6.8 Lemma. $\mathrm{card}(G/\,\mathrm{rmod}\, H) \cdot |H| = |G| = \mathrm{card}(G/\,\mathrm{lmod}\, H) \cdot |H|$.

Důkaz. Uvažme zobrazení $aH \mapsto Ha^{-1}$ množiny $\{aH;\ a \in G\} = G/\mathrm{lmod}\, H$ na množinu $\{Ha;\ a \in G\} = G/\,\mathrm{rmod}\, H$. Jde o korektně definované zobrazení, neboť Ha^{-1} je rovno $(aH)^{-1}$. Protože toto zobrazení je bijektivní, musí mít uvažované množiny stejnou mohutnost. $\square$

Z 6.8 plyne, že $\mathrm{card}(G/\,\mathrm{rmod}\, H) = \mathrm{card}(G/\,\mathrm{lmod}\, H)$. Tuto mohutnost nazýváme *index* podgrupy H v grupě G a značíme $|G : H|$. (Je třeba si uvědomit, že $G/\,\mathrm{rmod}\, H$ zde označuje pouze množinu rozkladových tříd ekvivalence $\mathrm{rmod}\, H$, nikoliv algebru – $\mathrm{rmod}\, H$ totiž nemusí být vždy kongruence.)

Vztah uvedený v 6.8 je znám jako Lagrangeova věta:

Věta. (Lagrangeova) *Buď G grupa a H její podgrupa. Pak $|G| = |H| \cdot |G : H|$.*

6.9 Důsledek. *Buď G konečná grupa a H její podgrupa. Pak $|H|$ dělí $|G|$.*

Množiny Ha se nazývají *pravé rozkladové třídy* H v G. Množiny aH se nazývají *levé rozkladové třídy* H v G. O podgrupě N grupy G řekneme, že je *normální*, jestliže $a^{-1}ha \in N$ pro každé $h \in N$ a $a \in G$.

6.10 Tvrzení. *Buď G grupa a N její podgrupa. Následující podmínky jsou ekvivalentní.*

(i) *N je normální podgrupa G,*
(ii) *$aN = Na$ pro každé $a \in G$,*
(iii) *$\mathrm{rmod}\, N$ je kongruence G.*

Přitom ke každé kongruenci ρ grupy G existuje právě jedna normální podgrupa H grupy G taková, že $\rho = \mathrm{rmod}\, H$.

Dříve než přistoupíme k důkazu 6.10, zmíníme, že podle 6.7 lze 6.10(ii) vyjádřit také jako rovnost ekvivalencí $\mathrm{rmod}\, N$ a $\mathrm{lmod}\, N$. V takovém případě je zvykem psát pouze $\mathrm{mod} N$ – přitom vztah $a \equiv b \mod N$ se čte 'a je kongruentní s b modulo N'.

Důkaz. Buď N podgrupa G. (i) $\Rightarrow$ (ii) Buď $a \in G$ a $h \in N$. Pak $ah = aha^{-1}a \in Na$, a naopak $ha = aa^{-1}ha \in aN$.
(ii) $\Rightarrow$ (iii) Buď $a, b, c, d \in G$ a ať $a \equiv c\, \mathrm{rmod}\, N$ a $b \equiv d\, \mathrm{rmod}\, N$. Pak $ac^{-1} \in N$, $bd^{-1} \in N$, takže $(ab)(cd)^{-1} = abd^{-1}c^{-1} = hac^{-1}$, kde $h \in N$ je dáno vztahem $a(bd^{-1}) = ha$. Tudíž $(ab)(cd)^{-1} \in N$ a $\mathrm{rmod}\, N$ je slučitelná s binární operací $\cdot$. Protože platí $a \equiv c\, \mathrm{lmod}\, N$, je $a^{-1}c = a^{-1}(c^{-1})^{-1} \in N$, takže $a^{-1} \equiv c^{-1}\, \mathrm{rmod}\, N$ a $\mathrm{rmod}\, N$ je slučitelné také s unární operací ${}^{-1}$.
(iii) $\Rightarrow$ (i) Buď $h \in N$, $a \in G$ a ať $\mathrm{rmod}\, N$ je kongruence. Pak $ha \equiv a\, \mathrm{rmod}\, H$, takže $a^{-1}ha \equiv a^{-1}a\, \mathrm{rmod}\, H$. Protože $a^{-1}a = \mathbf{1}_G$, tak nutně $a^{-1}ha \in H$.

Buď nyní ρ kongruence a položme $H = [\mathbf{1}]_\rho$. Z $\mathbf{1} \cdot \mathbf{1} = \mathbf{1}$ a $\mathbf{1}^{-1} = \mathbf{1}$ plyne, že H je podgrupa G. Ať $a, b \in G$ jsou takové, že $ab^{-1} \in H$. Pak $ab^{-1}\rho\mathbf{1}$, a tedy $a\rho b$. Naopak z $a\rho b$ plyne $ab^{-1}\rho\mathbf{1}$, čili $ab^{-1} \in H$. Dokázali jsme, že ρ je rovno $\mathrm{rmod}\, H$. Podle (i–iii) je H normální podgrupa G. $\square$

6.11 Důsledek. *Každá podgrupa indexu 2 je normální.*

Důkaz. Z $|G : H| = 2$ plyne, že G má dvě pravé a dvě levé rozkladové třídy. Protože H je jak levá, tak pravá rozkladová třída, musí být druhá rozkladová třída v obou případech rovna $G \backslash H$. Z 6.10(ii) tudíž dostáváme, že H je normální podgrupa G. $\square$

Je-li $(N_i;\ i \in I)$ neprázdná soustava normálních podgrup grupy G, tak $\cap(N_i;\ i \in I)$ je zjevně opět normální podgrupa. Normální podgrupy tedy tvoří uzávěrový systém nad G. Podle 4.2 můžeme proto hovořit o svazu normálních podgrup.

Podle 6.10 má každá kongruence ρ grupy G tvar $\mathrm{mod} H$, kde H je normální podrupa grupy G. Podgrupa H je přitom rovna té rozkladové třídě $\mathrm{mod} H$, jež obsahuje prvek $\mathbf{1}$. Proto pro dvě různé normální podgrupy H a K jsou kongruence $\mathrm{mod}\, H$ a $\mathrm{mod}\, K$ různé. Zobrazení $H \mapsto \mathrm{mod}\, H$ je tedy bijektivní zobrazení svazu normálních podgrup grupy G na svaz kongruencí grupy G. Jelikož $K \subseteq H$ zjevně platí právě když je $\mathrm{mod}\, K \subseteq \mathrm{mod}\, H$, dostáváme z 4.4, že zobrazení $H \mapsto \mathrm{mod}\, H$ je izomorfismus svazů.

Je-li $f : G \to H$ homomorfismus grup, tak jádro zobrazení f je kongruence grupy G. To znamená, že existuje právě jedna normální podgrupa N grupy G, pro kterou je $\ker f$ rovno $\mathrm{mod}\, N$. Podgrupa N se shoduje s tou rozkladovou třídou ekvivalence $\ker f$, která obsahuje neutrální prvek $\mathbf{1}_G$, takže $N = \{a \in G;\ f(a) = \mathbf{1}_H\}$. Podgrupě N se říká *jádro homomorfismu f* a značí se $\mathrm{Ker}\, f$.

6.12 Tvrzení. *Buď $f : G \to H$ homomorfismus grup. Pak* $\operatorname{Ker} f$ *je normální podgrupa* G, $|G| = |\operatorname{Ker} f| \cdot |\operatorname{Im} f|$ a $|\operatorname{Im} f| = |G : \operatorname{Ker} f|$.

Důkaz. Protože řád podgrupy $\operatorname{Im} f$ grupy H je roven počtu tříd ekvivalence $\ker f$, a protože $\ker f$ má $|G : \operatorname{Ker} f|$ tříd, dostáváme uvedené vztahy přímo z Lagrangeovy věty. □

Je-li N normální podgrupa grupy G, tak můžeme zkonstruovat kvocientní grupu $G/\bmod N$. Jejími prvky jsou všechny rozkladové třídy N v G. Místo $G/\bmod N$ se většinou píše pouze G/N.

Ve zbytku této kapitoly se budeme především věnovat symetrickým grupám. Tomu, kdo absolvoval standardní kurs lineární algebry, bude značná část uvedené látky pravděpodobně známa.

Je-li f permutace množiny Ω, tak definujeme relaci ρ_f na Ω tak, že $(a,b) \in \rho_f$ právě když $f^m(a) = b$ pro nějaké $m \in \mathbb{Z}$. Relace ρ_f je zjevně reflexivní, symetrická a tranzitivní, takže to je ekvivalence na Ω. Rozkladovým třídám ρ_f říkáme *orbity tranzitivity.* (Uvážíme-li na Ω graf s hranami $\{a, f(a)\}$, tak orbity tranzitivity se shodují s tranzitivními komponentami tohoto grafu.)

Je-li $\Gamma \subseteq \Omega$ orbita tranzitivity permutace f a a je prvek Γ, tak každý prvek Γ musí být možné vyjádřit jako $f^m(a)$, takže Γ je rovno $\{f^m(a);\, m \in \mathbb{Z}\}$.

Ať pro nějaká celá čísla $s > r$ platí $f^s(a) = f^r(a)$. Pak je $f^{s-r}(a) = a$ a $s-r > 0$. Ať $k > 0$ je nejmenší takové, že $f^k(a) = a$. Potom pro $0 \le i < j < k$ je $f^i(a) \neq f^j(a)$ a Γ obsahuje právě prvky $\{a, f(a), \dots, f^{k-1}(a)\}$.

Uvedených vlastností lze použít v případě, kdy množina Ω je konečná, k *cyklickému zápisu* permutace f:

Ať $\Gamma_1, \dots, \Gamma_r$ jsou orbity tranzitivity permutace f, ať $\{a_1, \dots, a_r\}$ je nějaká transversála tohoto rozkladu a ať k_i, $1 \le i \le r$, udává počet prvků orbity Γ_i. Pro $1 \le i \le r$ a $1 \le j \le k_i$ položme $a_{ij} = f^j(a_i)$. Pak permutaci f zapisujeme ve tvaru

$$(a_{11}\ \dots\ a_{1k_1})(a_{21}\ \dots\ a_{2k_2})\ \dots\ (a_{r1}\ \dots a_{rk_r}).$$

Přitom prvek a_i se zřejmě shoduje s a_{ik_i}. Platí $\Gamma_i = \{a_{ij};\ 1 \le j \le k_i\}$, takže každý prvek Ω se v cyklickém zápisu vyskytuje právě jednou. Zápisu lze rozumět tak, že každý prvek, za kterým nenásleduje pravá závorka, se zobrazí do prvku od něj vpravo, a prvek, za kterým následuje pravá závorka, se zobrazí za nejbližší předcházející levou závorku.

Uvažme například permutaci h množiny $\{1,2,3,4,5,6\}$, která je zadaná vztahy $h(1) = 2$, $h(2) = 5$, $h(3) = 6$, $h(4) = 4$, $h(5) = 1$ a $h(6) = 3$. Její cyklický zápis bude $(1\,2\,5)(3\,6)(4)$. Přesný tvar zápisu ovšem záleží na volbě pořadí orbit a na výběru transversály. Při jiném pořadí orbit bude i jiné pořadí částí v závorkách, a při jiné volbě reprezentanta orbity budou prvky uvnitř odpovídajících závorek cyklicky posunuty. Výše uvedenou permutaci je tudíž možno zapsat například také $(2\,5\,1)(4)(6\,3)$. Jednobodové orbity se často ze zápisu vynechávají, a pak se hovoří o *zkráceném cyklickém zápisu.* Jedním z možných zkrácených zápisů permutace h je $(3\,6)(2\,5\,1)$.

Pro každou orbitu tranzitivity Γ_i permutace f definujeme permutaci $f_i \in S_\Omega$ tak, že $f_i(a) = f(a)$ pro $a \in \Gamma_i$ a $f_i(a) = a$ pro $a \notin \Gamma_i$. Je zřejmé, že f je rovno

$f_1 \circ f_2 \circ \cdots \circ f_r$ a že permutace f_i vzájemně komutují (tj. pro $1 \le i \le j \le r$ je $f_i \circ f_j = f_j \circ f_i$). Všimněte si, že f_i je identita právě když má orbita Γ_i jediný bod. Zápisu $f = f_1 \circ \cdots \circ f_r$ se říká *úplná dekompozice* permutace f. Protože orbity f jsou jednoznačně určeny, je úplná dekompozice definována až na pořadí také jednoznačně.

Zkrácený cyklický zápis permutace f_i je $(a_{i1} \dots a_{ik})$. Například výše definovaná permutace $h \in S_6$ má úplnou dekompozici $h_1 \circ h_2 \circ h_3$, kde h_1 má zkrácený cyklický zápis $(1\,2\,5)$, h_2 má zkrácený cyklický zápis $(3\,6)$ a h_3 je identita.

Permutace $f \in S_\Omega$ se zkráceným cyklickým zápisem $(a\,b)$ se nazývají *transpozice*.

6.13 Lemma. *Ať $f \in S_\Omega$ má zkrácený cyklický zápis $(c_1 \dots c_k)$, kde $k \ge 2$. Transpozici $(c_i\, c_{i+1})$, $1 \le i < k$, označme t_i. Potom platí $f = t_1 \circ \cdots \circ t_{k-1}$.*

Důkaz. Pro $1 \le i < k$ je, jak lze snadno ověřit indukcí, $t_i \circ t_{k-1}(c_k)$ rovno c_i. Proto $t_1 \circ \cdots \circ t_{k-1}$ zobrazí c_k na c_1.

Transpozice $t_{i+1}, \dots, t_{k-1}$ prvkem c_i nepohnou, takže $t_i \circ \cdots \circ t_{k-1}(c_i)$ je rovno c_{i+1}. Protože transpozice $t_1, \dots, t_{i-1}$ prvkem c_{i+1} nehýbají, tak vskutku platí $t_1 \circ \cdots \circ t_{k_1}(c_i) = c_{i+1}$. □

Každou složku cyklické dekompozice permutace $f \in S_\Omega$ lze tedy vyjádřit jako složení transpozic. Proto platí:

6.14 Důsledek. *Buď Ω konečná množina. Transpozice na množině Ω generují S_Ω.*

V následujícím lemmatu jsou permutace reprezentovány svými zkrácenými cyklickými zápisy. Obě rovnosti lze bezprostředně ověřit.

6.15 Lemma. *Buď $r \ge 0$ a $s \ge 0$ celá čísla. Pak*

(*) $$(a\,b) \circ (a\,c_1 \dots c_r\,b\,d_1 \dots d_s) = (a\,c_1 \dots c_r)(b\,d_1 \dots d_s)$$

a

(**) $$(a\,b) \circ (a\,c_1 \dots c_r)(b\,d_1 \dots d_s) = (a\,c_1 \dots c_r\,b\,d_1 \dots d_s)$$

Je-li Ω konečná množina o n prvcích, tak S_Ω je izomorfní symetrické grupě S_n. Proto se při vyšetřování permutací konečných množin lze omezit na permutace z S_n.

Znaménko $\operatorname{sgn}(f)$ permutace $f \in S_n$ definujeme jako $(-1)^{n-k}$, kde k je počet orbit tranzitivity permutace f. Permutacím se znaménkem 1 se říká *sudé*, ostatním permutacím se říká *liché*. Protože identická permutace má n orbit a transpozice $n-1$ orbit, vidíme, že identita je permutace sudá a transpozice jsou permutace liché.

6.16 Lemma. *Buď $t \in S_n$ transpozice. Pak pro každou permutaci $f \in S_n$ platí*

$$\operatorname{sgn}(t \circ f) = -\operatorname{sgn}(f).$$

Důkaz. Ať $(a\,b)$ je zkrácený cyklický zápis transpozice t. Jsou-li a a b v téže orbitě tranzitivity permutace f, tak $t \circ f$ má podle (*) o jednu orbitu více než f. Naopak, leží-li a a b v různých orbitách f, počet orbit podle (**) o jednu klesne. □

6.17 Důsledek. *Buď $t_1, \ldots, t_k \in S_n$ transpozice. Pak* $\operatorname{sgn}(t_1 \circ \cdots \circ t_k) = (-1)^k$.

6.18 Důsledek. sgn *je homomorfismus S_n na $\{-1, 1\}$.*

Důkaz. Buď f a g dvě permutace z S_n. Podle 6.14 lze každou z nich zapsat jako součin transpozic, například ať $f = t_1 \circ \cdots \circ t_r$ a $g = t_1' \circ \cdots \circ t_s'$. Podle 6.17 je $\operatorname{sgn}(g \circ f) = (-1)^{s+r} = (-1)^s(-1)^r = \operatorname{sgn}(g) \cdot \operatorname{sgn}(f)$. $\square$

Jádro homomorfismu sgn jsou právě všechny sudé permutace. Podgrupě sudých permutací se říká *alternující grupa* a značívá se A_n. Je to normální podgrupa S_n, což plyne například z toho, že je jádrem homomorfismu. Podle 6.12 má A_n v S_n index 2, takže 6.11 nám nabízí jiný důkaz normality A_n v S_n. Grupa S_n má řád $n!$ a grupa A_n má řád $\frac{n!}{2}$.

O dvou prvcích a, b grupy G řekneme, že jsou *konjugovány* v grupě G, jestliže existuje $g \in G$ takové, že $g^{-1}ag = b$. Protože $g^{-1}ag = b$ je ekvivalentní $gbg^{-1} = a$, je relace 'být konjugován' symetrická. Každý prvek je konjugován sám se sebou, neboť $a^{-1}aa = a$. S $\mathbf{1}$ není konjugován žádný jiný prvek, jelikož $g^{-1}\mathbf{1}g = \mathbf{1}$ pro každé $g \in G$. Z $g^{-1}ag = b$ a $h^{-1}bh = c$ plyne $(gh)^{-1}a(gh) = c$, čímž je ověřena tranzitivita, a vidíme, že relace 'být konjugován' je ekvivalencí.

V obecném případě může být odpověď na otázku, zda dva prvky grupy jsou konjugovány, velmi obtížná. Lineární algebra má tolik významných aplikací právě proto, že tento problém je v grupě regulárních matic nad komplexními čísly dobře algoritmicky zpracován. (Součin dvou regulárních matic je opět regulární matice, jednotková matice je regulární a matice inverzní je rovněž regulární. Proto regulární matice tvoří vzhledem k běžnému násobení matic grupu, a to nad libovolným tělesem, nejen nad komplexními nebo reálnými čísly.) V lineární algebře se ovšem spíše než o konjugaci matic hovoří o jejich podobnosti. To je ovšem jen jiný název pro tentýž pojem, neboť o maticích A a B říkáme, že jsou podobné, jestliže existuje regulární matice C taková, že $A = CBC^{-1}$.

Ukážeme, že v případě symetrických grup lze konjugaci dvou permutací snadno poznat. Ať permutace $f \in S_n$ má orbity r orbit o $k_1, k_2 \ldots, k_r$ prvích. Můžeme předpokládat, že platí $k_1 \geq k_2 \geq \ldots k_r$. Posloupnosti $(k_1, k_2, \ldots, k_r)$ se říká *typ* permutace.

6.19 Tvrzení. *Dvě permutace $f, g \in S_n$ jsou konjugovány právě když mají stejný typ.*

Důkaz. Má-li permutace f cyklický zápis $(a_{11} \ \ldots \ a_{1k_1}) \ldots (a_{r1} \ \ldots \ a_{rk_r})$, tak permutace hfh^{-1} má cyklický rozklad $(h(a_{11}) \ \ldots \ h(a_{1k_1})) \ldots (h(a_{r1}) \ \ldots \ h(a_{rk_r}))$, takže permutace vzájemně konjugované vskutku mají tentýž typ. Naopak, jestliže f a g mají stejný typ $(k_1, \ldots, k_r)$, tak pro vhodná a_{ij} a b_{ij} lze f zapsat ve tvaru $(a_{11} \ \ldots \ a_{1k_1}) \ldots (a_{r1} \ \ldots \ a_{rk_r})$ a g lze zapsat ve tvaru $(b_{11} \ \ldots \ b_{1k_1}) \ldots (b_{r1} \ \ldots \ b_{rk_r})$. Označme h zobrazení $a_{ij} \mapsto b_{ij}$. Pak h je permutace z S_n a platí $g = hfh^{-1}$. $\square$

Všimněte si, že podgrupa N grupy G je normální právě tehdy, když s každým prvkem $a \in N$ jsou v N obsaženy i všechny prvky s ním konjugované. Pokud najdeme takovou podgrupu S_n, která obsahuje kromě identické permutace pouze všechny prvky nějakého typu, bude to jistě normální podgrupa grupy S_n.

6.20 Tvrzení. $\{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1)(2)(3)(4)\}$ *je normální podgrupa* S_4.

Důkaz. Uvedený seznam permutací obsahuje všechny permutace z S_4, které jsou typu $(2,2)$. Podle předchozího tedy stačí ukázat, že tyto permutace skutečně tvoří podgrupu S_4. Položme $\Omega = \{1,2,3,4\}$ a ať $(a\ b)(c\ d)$ a $(i\ j)(k\ l)$ jsou permutace Ω. Jsou-li shodné, vznikne jejich složením id_Ω. Jsou-li různé, lze předpokládat $a = i$, $c = k$. Pak nutně $b = l$ a $d = j$, přičemž $(a\ d)(c\ b) \circ (a\ b)(c\ d) = (a\ c)(b\ d)$. $\square$

Grupě permutací $\{(1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3), (1)(2)(3)(4)\}$ se říká *Kleinova grupa.* Tato grupa je z hlediska grup permutací dosti výjimečná, neboť lze ukázat, že pro $n \neq 4$ a $n \geq 3$ nemá S_n kromě A_n žádnou jinou vlastní normální podgrupu. (Podgrupa H grupy G se nazývá *vlastní*, je-li různá od G a od $\{\mathbf{1}_G\}$.)

Jsou-li f a g dva automorfismy nějaké algebry $A = \Omega(\alpha_1, \ldots, \alpha_k)$, tak $f \circ g$ i f^{-1} jsou podle 2.9 rovněž automorfismy této algebry. Množina $\mathrm{Aut}(A)$ všech automorfismů algebry A je tudíž podmonoid monoidu $\mathrm{End}(A)$ a současně podgrupa grupy S_Ω. Leží-li dva prvky $a, b \in A$ v téže orbitě nějakého automorfismu $f \in \mathrm{Aut}(A)$, tak jsou ze strukturálního hlediska ekvivalentní. Z tohoto prostého faktu vychází řada úvah jak v matematice samotné, tak i v jejích aplikacích. Přitom grupu automorfismů má smysl vyšetřovat i u jiných objektů než u algeber — například má smysl mluvit o grupě automorfismů nějakého grafu, automatu nebo formálního jazyka.