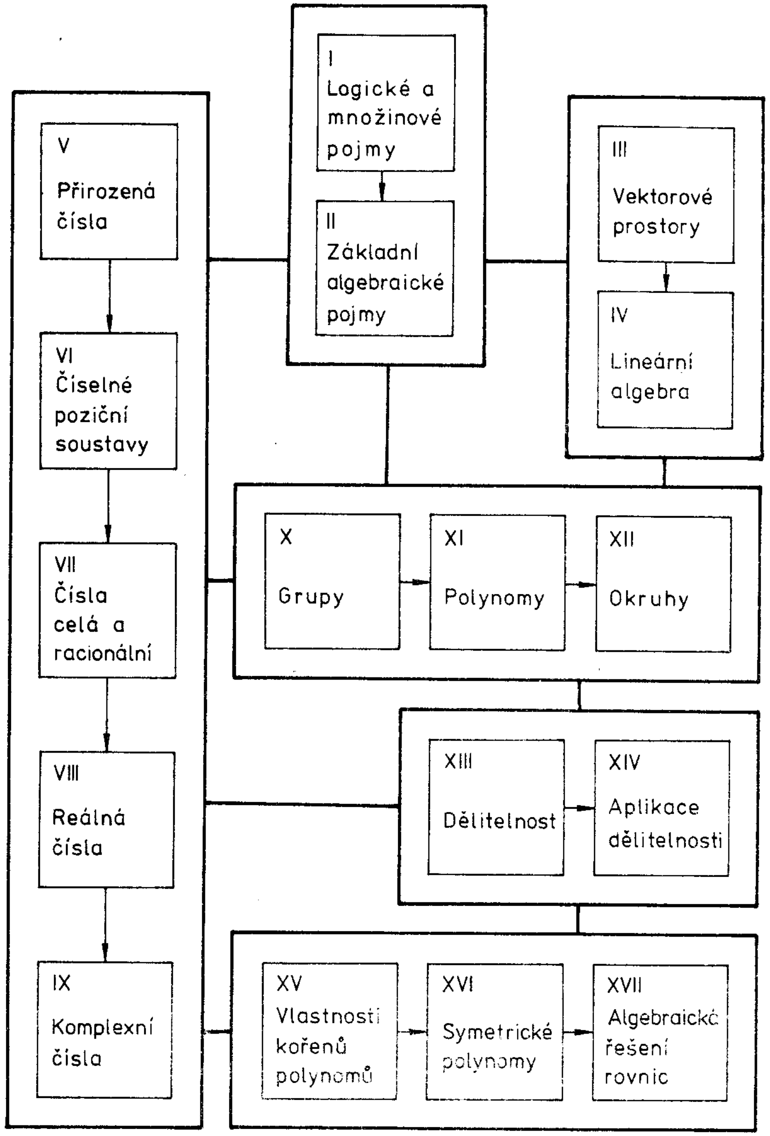


KAPITOLA X

GRUPY

§ 1. Základní vlastnosti grup

S algebraickou strukturou zvanou grupa se čtenář seznámil již v prvním ročníku studia a poznal přitom řadu konkrétních příkladů grup. Grupami jsou některé obory čísel (ať již s operací sčítání či násobení), dále víme, že každý vektorový prostor tvoří vzhledem k operaci sčítání vektorů grupu, rovněž množiny zobrazení některých typů s operací skládání zobrazení jsou často grupy atd.

Pojem grupy se stal jedním ze základních pojmů moderní algebry, nalezl uplatnění v řadě různých i nematematických vědních disciplín. To si vynutilo vznik celé rozsáhlé partie matematiky — teorie grup. Jedním z průkopníků této teorie byl i sovětský matematik O. J. Šmidt*), který již v roce 1916 vydal svou „Abstraktní teorii grup“, jež byla ve světovém měřítku první ucelenou učebnicí této teorie.

V této kapitole si nejprve připomeneme definici pojmu grupy, která byla vyslovena v kapitole II, § 4. Přitom budeme užívat multiplikativní zápis i příslušnou terminologii (viz kapitola II, § 3).

Definice. *Struktura s jednou binární operací* $(G, \cdot)$ *se nazývá* grupa, *právě když platí*

1. $(\forall x, y, z \in G)\ (xy)z = x(yz)$,
2. $(\exists x \in G)\ (\forall y \in G)\ (xy = y \wedge yx = y)$

(takový prvek existuje jediný, nazývá se jednotkový prvek a značí se 1, eventuelně též e),

3. $(\forall x \in G)\ (\exists y \in G)\ (xy = 1 \wedge yx = 1)$

(v kapitole II jsme ukázali, že pro každé x existuje právě jeden prvek $y \in G$ uvedených vlastností, nazývá se inverzní prvek k x a značí se x^{-1}).

Je-li struktura $(G, \cdot)$ *navíc komutativní, nazývá se* komutativní *neboli* Abelova*) grupa.

Další příklady grup nalezne čtenář na konci tohoto paragrafu. Nyní, abychom si

*) O. J. Šmidt (1891—1956). Významný sovětský algebraik, zakladatel moskevské algebraické školy, znám též jako polární badatel a kosmolog.

*) Niels Henrik Abel (1802—1829), norský matematik.

procvičili práci s podmínkami uvedenými v definici grupy, odvodíme větu, která bývá důležitá při zjišťování, zda je daná struktura grupou.

Věta 1. *Nechť* $(G, \cdot)$ *je neprázdná asociativní struktura. Pak* $(G, \cdot)$ *je grupa, právě když* G *je struktura s dělením, tj. když platí*

$$(1) \qquad (\forall x, y \in G)\,(\exists z, z' \in G)\,(xz = y \wedge z'x = y).$$

Důkaz. 1. Jestliže $(G, \cdot)$ je grupa, je dokonce strukturou s jednoznačným dělením — viz kapitola II, § 4, věta 1b.

2. Nechť tedy $(G, \cdot)$ je asociativní struktura s dělením a $G \neq \emptyset$. Pak existuje $a \in G$ a z podmínky dělení plyne existence prvku $e \in G$ tak, že $e \,.\, a = a$. Dokážeme, že e je jednotkovým prvkem v G. Buď tedy $b \in G$ a nechť y je takový prvek v G, že $a \,.\, y = b$ (existence prvku y plyne z předpokladů věty). Pak rovnost $ea = a$ implikuje $(ea) \,.\, y = a \,.\, y$ a podle asociativního zákona a zavedení y dostáváme $e \,.\, b = b$. Rovněž snadno nahlédneme, že platí $b \,.\, e = b$. Označíme $\bar{e}$ takový prvek z G, pro nějž $a \,.\, \bar{e} = a$ (ve struktuře s dělením musí existovat); analogicky předchozímu ukážeme, že $b \,.\, \bar{e} = b$. Avšak $e \,.\, \bar{e} = e$ (poněvadž pro každé $b \in G$ je $b \,.\, \bar{e} = b$) a $e \,.\, \bar{e} = \bar{e}$, tudíž $e = \bar{e}$. Tedy $(G, \cdot)$ je struktura s jednotkovým prvkem.

Buď dále $x \in G$. Pak existují $y_1, y_2 \in G$ tak, že $x \,.\, y_1 = e$ a $y_2 \,.\, x = e$ — tj. prvky inverzní k x. Abychom ukázali, že $y_1 = y_2$, stačí vyšetřit výraz $y_2 \,.\, x \,.\, y_1$. Platí $(y_2 \,.\, x) \,.\, y_1 = e \,.\, y_1 = y_1$ a zároveň $y_2(xy_1) = y_2 \,.\, e = y_2$. Díky předpokladu o asociativnosti operace „·“ je proto $y_1 = y_2$, a tedy $(G, \cdot)$ je grupou.

V následujícím příkladě si ukážeme užití právě dokázané věty.

Příklad 1. Vezměme množinu M všech matic typu $(2, 2)$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

pro něž a, b, c, d jsou čísla celá a determinant

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad - bc = 1.$$

Definujme v M operaci násobení matic obvyklým způsobem (viz též kapitola II, § 4, příklad 21 anebo obecně kapitola IV, § 3):

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Protože pro determinant výsledné matice platí

$$(aa' + bc')\,(cb' + dd') - (ab' + bd')\,(ca' + dc') =$$
$$= bc(b'c' - a'd') + ad(a'd' - b'c') = (ad - bc)\,(a'd' - b'c'),$$

je součin libovolných matic z M rovněž prvkem množiny M, takže $(M, \cdot)$ je struktura. Víme již, že násobení matic (typu $(2, 2)$) je asociativní, a snadno se přesvědčíme, že pro libovolná celá čísla a, b, c, d, e, f, g, h platí

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} de - bg & df - bh \\ ag - ce & ah - cf \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix}$$

a dále

$$\begin{pmatrix} de - cf & af - be \\ dg - ch & ah - bg \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} e & f \\ g & h \end{pmatrix},$$

což znamená, že $(M, \cdot)$ je struktura s dělením. Tedy podle věty 1 je $(M, \cdot)$ grupa.

Větu 1 lze tedy s výhodou využít při ověřování, zda daná struktura je grupa; namísto hledání jednotkového prvku a ověřování podmínky existence prvků inverzních stačí vyšetřit pouze vlastnost dělení. Rovněž v případě, že struktura je zadána Cayleyho tabulkou, se „ověřovací procedura“ zřejmě zjednoduší.

Mnoho informací o struktuře grupy lze získat vyšetřováním jejích podgrup. S pojmem podgrupy se čtenář seznámil a procvičil si ho dostatečně již v § 4 kapitoly II. Zopakujeme proto jen definici podgrupy a připomeneme jednu nutnou a postačující podmínku pro to, aby podmnožina dané grupy byla její podgrupou.

Definice. *Struktura* $(H, \circ)$ *je* <u>*podgrupou*</u> *grupy* $(G, \cdot)$, *právě když*

1. $H \subseteq G$;
2. *operace „∘“ je zúžením (restrikcí) operace „·“ na množinu* H, *tj.* $(\forall x, y \in H)\,(x \circ y = x \,.\, y)$;
3. $(H, \circ)$ *je grupa.*

Poznamenejme, že je obvyklé operaci v dané grupě i v její podgrupě označovat týmž symbolem, což vlastně umožňuje podmínka 2 z definice podgrupy. Obdobně ve formulacích typu „podmnožina H grupy G je její podgrupou“ automaticky bereme operaci v H jako restrikci operace grupy G (na množinu H). Tak je nutno chápat i následující větu (viz též věta 3 z § 4, kap. II).

Věta 2. *Buď* $(G, \cdot)$ *grupa. Podmnožina* H *množiny* G *je podgrupou v* G, *právě když*

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

Užití věty 2 si ukážeme v následujícím příkladě.

Příklad 2. Symetrická grupa n prvků označovaná S_n je grupa všech permutací množiny $\{1, 2, \ldots, n\}$ s operací skládání permutací (viz kapitola II, § 4, příklad 4). Připomeňme si definici této operace (budeme užívat multiplikativní zápis). Jsou-li

$$A=\begin{pmatrix}1 & 2 & \dots & n\\ i_1 & i_2 & \dots & i_n\end{pmatrix}, \qquad B=\begin{pmatrix}1 & 2 & \dots & n\\ j_1 & j_2 & \dots & j_n\end{pmatrix}$$

libovolné permutace z S_n, je

$$(2) \qquad A\,.\,B=\begin{pmatrix}1 & 2 & \dots & n\\ j_{i_1} & j_{i_2} & \dots & j_{i_n}\end{pmatrix}.$$

Permutaci

$$\begin{pmatrix}1 & 2 & \dots & n\\ i_1 & i_2 & \dots & i_n\end{pmatrix}\in S_n$$

nazveme sudou, právě když v pořadí $(i_1, i_2, \dots, i_n)$ je sudý počet inverzí neboli když

$$\mathrm{Sg}\,(i_1, i_2, \dots, i_n)=1$$

(viz kapitola IV, § 2).

Označme A_n množinu všech sudých permutací z S_n. Ukážeme, že A_n je podgrupa v S_n (nazývá se alternující grupa n prvků). Užijeme větu 2.

Protože identická permutace

$$E=\begin{pmatrix}1 & 2 & \dots & n\\ 1 & 2 & \dots & n\end{pmatrix}$$

je zřejmě sudá, je $A_n \neq \emptyset$.

K ověření podmínky 2 z věty 2 užijeme následující větu.

Lemma 1. *Nechť A, B jsou libovolné permutace z S_n, pak součet počtu inverzí permutací A a B je buď roven počtu inverzí permutace AB, anebo je o sudé číslo větší.*

Tedy zapsáno formulí

$$(3) \qquad (\forall A, B\in S_n)\,(\exists k\in \mathbf{N})\,I(A)+I(B)=I(AB)+2k.$$

Důkaz se přenechává čtenáři (viz cvičení 1).

Jsou-li tedy A, B libovolné permutace z A_n, jsou čísla $I(A)$ a $I(B)$ sudá, takže pro počet inverzí složené permutace platí podle (3)

$$I(AB)=I(A)+I(B)-2k.$$

Tedy $I(AB)$ je číslo sudé a $AB\in A_n$.

Je-li A^{-1} inverzní permutace k permutaci $A\in A_n$, je $AA^{-1}=E$, a protože pro identickou permutaci E platí $I(E)=0$, je opět podle (3)

$$I(A)+I(A^{-1})=2k,$$

takže A^{-1} je sudá permutace, a tedy $A^{-1}\in A_n$.

Podle věty 2 je tedy alternující grupa A_n podgrupou symetrické grupy S_n.

Zaveďme ještě jeden termín, který je v matematické literatuře obvyklý. Je-li $(G, \cdot)$ konečná grupa (tj. je-li její nosič G konečná množina), nazývá se počet prvků množiny G řád grupy $(G, \cdot)$. Je-li množina G, a tedy i grupa $(G, \cdot)$ nekonečná, budeme též říkat, že grupa $(G, \cdot)$ je nekonečného řádu.

Je ihned zřejmé (neboť každý izomorfismus je prosté zobrazení), že libovolné dvě izomorfní grupy mají týž řád.

Příklad 3. Jak již víme (viz kapitola IV, § 2), je počet různých pořadí $(i_1, i_2, \dots, i_n)$ z n prvků roven číslu $n!$. Protože každému takovému pořadí odpovídá právě jedna permutace

$$\begin{pmatrix}1 & 2 & \dots & n\\ i_1 & i_2 & \dots & i_n\end{pmatrix}$$

symetrické grupy S_n, je řád této grupy $n!$.

Protože právě polovina ze všech permutací z S_n $(n>1)$ je sudých, je řád alternující grupy A_n roven číslu $n!/2$.

Symetrické grupy hrají v teorii konečných grup velmi důležitou roli, jak ukazuje následující věta.

Věta 3. *Každá konečná grupa řádu n je izomorfní s jistou podgrupou symetrické grupy S_n (neboli lze ji izomorfně vnořit do S_n).*

Důkaz. Mějme dánu grupu $(G, \cdot)$ řádu n. Její prvky označme $a_1, a_2, \dots, a_n$. Pro každé $x\in G$ označme F_x zobrazení G do G, které každému prvku $a\in G$ přiřazuje prvek ax, tj.

$$(4) \qquad (\forall a\in G)\,F_x(a)=ax.$$

Takové zobrazení nazveme projekce grupy G (určená prvkem x). Protože v G lze krátit libovolným prvkem, je každá projekce F_x prosté zobrazení, a protože G je struktura s dělením, je F_x zobrazení G na G. Tedy pro každé $x\in G$ je projekce F_x vlastně permutace množiny G, kterou díky označení prvků z G můžeme zapsat též takto:

$$F_x=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ a_1x & a_2x & \dots & a_nx\end{pmatrix}=\begin{pmatrix}a_1 & a_2 & \dots & a_n\\ a_{i_1} & a_{i_2} & \dots & a_{i_n}\end{pmatrix},$$

kde pro $k=1, 2, \dots, n$ je $a_{i_k}=a_kx$, takže

(a) každá projekce grupy G definuje jisté pořadí $(i_1, i_2, \dots, i_n)$ čísel $1, 2, \dots, n$.

Jsou-li x a y různé prvky grupy G, je

$$F_x(\underline{1}) = x \neq F_y(\underline{1}) = y,$$

kde symbol $\underline{1}$ označuje jednotkový prvek grupy G. Odtud ihned plyne, že

(b) různé prvky grupy G určují různé projekce grupy G (a tedy i pořadí definovaná těmito projekcemi jsou různá).

Díky asociativnosti grupy $(G, \cdot)$ snadno ukážeme, že

(c) složení $F_x . F_y$ projekcí F_x a F_y grupy G je opět projekce grupy G, přičemž platí

$$(5) \qquad (\forall x, y \in G) F_x . F_y = F_{xy}.$$

K tomuto účelu zvolíme libovolné prvky $x, y, a \in G$ a postupně ukážeme

$$(F_x . F_y)(a) = F_y(F_x(a)) = F_y(ax) = (ax)y = a(xy) = F_{xy}(a).$$

Protože a je libovolný prvek grupy G, dostáváme odtud ihned platnost formule (5) a vlastně celého tvrzení (c).

Definujeme nyní zobrazení φ, jež každému prvku $x \in G$ přiřadí permutaci

$$\varphi(x) = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix},$$

kde $(i_1, i_2, \dots, i_n)$ je pořadí definované projekcí F_x podle (a).

Z (b) ihned plyne, že φ je prosté zobrazení množiny G do symetrické grupy S_n (všech permutací množiny $\{1, 2, \dots, n\}$).

K důkazu věty 3 tedy stačí ověřit, že φ má vlastnost izomorfismu. Nechť x, y jsou libovolné prvky z G a nechť

$$\varphi(x) = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \qquad \varphi(y) = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix},$$

takže pro odpovídající projekce F_x a F_y platí

$$F_x(a_r) = a_{i_r}, \quad F_y(a_r) = a_{j_r}, \quad r = 1, 2, \dots, n.$$

Podle (5) je (pro $r = 1, 2, \dots, n$)

$$F_{xy}(a_r) = (F_x . F_y)(a_r) = F_y(F_x(a_r)) = F_y(a_{i_r}) = a_{j_{i_r}},$$

takže

$$\varphi(xy) = \begin{pmatrix} 1 & 2 & \dots & n \\ j_{i_1} & j_{i_2} & \dots & j_{i_n} \end{pmatrix}.$$

To však je permutace složená z permutací $\varphi(x)$ a $\varphi(y)$, takže skutečně

$$\varphi(xy) = \varphi(x) . \varphi(y),$$

čímž je věta 3 dokázána.

Poznamenejme, že když zobecníme pojem permutace tak, že jí budeme rozumět prosté zobrazení jakékoliv (i nekonečné) množiny na sebe, můžeme právě dokázanou větu vyslovit v obecnějším tvaru.

Věta 3'. *Libovolná grupa $(G, \cdot)$ je izomorfní s jistou podgrupou grupy všech permutací množiny G.*

Protože důkaz této věty je zcela analogický důkazu věty 3, přenecháváme jej čtenáři.

Výsledků odvozených v důkazu předcházející věty 3 využijeme k nalezení podmínky, jež je užitečná při vyšetřování asociativnosti některých struktur.

Věta 4. *Nechť $(G, \cdot)$ je struktura s krácením, s dělením a s jednotkovým prvkem. Pak $(G, \cdot)$ je asociativní, právě když skládání zobrazení je operací v množině všech projekcí F_x struktury $(G, \cdot)$.*

Důkaz. Nechť struktura G splňuje předpoklady věty.

a) Nechť dále je $(G, \cdot)$ asociativní. Pak je grupou a podle bodu (c) v důkazu věty 3 (či — v případě nekonečné množiny G — analogicky podle věty 3') je skládání zobrazení operací v množině všech projekcí v G.

b) Nechť operace skládání zobrazení je operací v množině všech projekcí v G. Pak k libovolným prvkům $x, y \in G$ musí existovat $z \in G$ takové, že

$$F_x . F_y = F_z,$$

neboli

$$(\forall a \in G)(F_x . F_y)(a) = F_z(a).$$

Tedy speciálně pro z rovné jednotkovému prvku $\underline{1}$ struktury G obdržíme

$$(F_x . F_y)(\underline{1}) = F_z(\underline{1})$$

a podle definice projekce a definice skládání zobrazení

$$(F_x . F_y)(a) = F_y(F_x(a))$$

dostáváme

$$F_y(F_x(\underline{1})) = F_z(\underline{1}) \Rightarrow (\underline{1}x)y = \underline{1}z \Rightarrow xy = z.$$

Pro projekce struktury G tedy platí (5).

Zvolme nyní libovolné prvky $x, y, z \in G$, pak

$$x(yz) = F_{yz}(x) = (F_y . F_z)(x) = F_z(F_y(x)) = (xy)z,$$

takže struktura $(G, \cdot)$ je asociativní.

Pokud jde o užití věty 4, poznamenejme, že například v případě konečných struktur $(G, \cdot)$, jejichž operace je zadána multiplikativní tabulkou, snadno ověříme vlastnosti struktury G, které věta předpokládá, zatímco ověření asociativnosti obvykle bývá obtížné. Větu lze užít i v negativním případě, jak vidíme v následujícím příkladu.

Příklad 4. Nechť $M=\{a, b, c, d, f, g\}$ a nechť operace struktury $(M, \cdot)$ je dána tabulkou 1.

$\cdot$	a	b	c	d	f	g
a	a	b	c	d	f	g
b	b	c	a	f	g	d
c	c	a	b	g	d	f
d	d	f	g	c	b	a
f	f	g	d	b	a	c
g	g	d	f	a	c	b

Tab. 1

Snadno ověříme, že prvek a je neutrálním prvkem struktury $(M, \cdot)$ i že tato struktura je s krácením a s dělením (neboť v každém řádku i sloupci multiplikativní tabulky se každý prvek vyskytuje právě jednou), dokonce vidíme, že je též komutativní i s inverzními prvky (neboť v každém sloupci i řádku tabulky se vyskytuje neutrální prvek, a to symetricky vzhledem k diagonále tabulky). Struktura $(M, \cdot)$ však není asociativní, neboť například složení projekcí F_f a F_d není projekce.

$$F_f=\begin{pmatrix} a & b & c & d & f & g \\ f & g & d & b & a & c \end{pmatrix}, \quad F_d=\begin{pmatrix} a & b & c & d & f & g \\ d & f & g & c & b & a \end{pmatrix}$$

$$F_f \,.\, F_d=\begin{pmatrix} a & b & c & d & f & g \\ b & a & c & f & d & g \end{pmatrix},$$

což není projekce, neboť pořadí (b, a, c, f, d, g) není řádkem tabulky 1.

Ve zbývající části tohoto paragrafu si připomeneme pojem generování struktur.

Definice. *Nechť $(G, \cdot)$ je grupa, M libovolná podmnožina v G, pak průnik všech podgrup grupy G, které obsahují množinu M, je podgrupa v G, která se nazývá* podgrupa generovaná množinou *M a značí se $[M]$. Množina M se nazývá* systém generátorů grupy *$[M]$ a její prvky* generátory *této grupy.*

Tato definice se opírá o větu (viz kapitola II, § 3, věta 4), která říká, že průnik libovolného (neprázdného) systému podgrup nějaké grupy je opět podgrupa této grupy.

Připomeňme ještě, že grupa může mít různé systémy generátorů. Například je-li $(G, \cdot)$ grupa, je zřejmě $[G]=G$ a také $[G-\{1\}]=G$.

Pokud nemáme přehled o všech podgrupách dané grupy, není definice podgrupy

generované v grupě $(G, \cdot)$ množinou $M \subseteqq G$ příliš vhodná pro praktickou konstrukci podgrupy $[M]$. Obvykle je výhodnější uvědomit si, že M je nejmenší (ve smyslu množinové inkluze $\subseteqq$) podgrupa, která obsahuje M; tj. pro libovolnou podgrupu H grupy G platí

$$M \subseteqq H \Rightarrow [M] \subseteqq H$$

a samozřejmě též $M \subseteqq [M]$.

Proto při konstrukci podgrupy $[M]$ (při dané množině M) můžeme postupovat též tak, že k prvkům z M připojíme vhodné prvky z G tak, abychom dostali podgrupu, a přitom budeme dbát toho, aby těchto připojených prvků bylo co nejméně.

Při tomto postupu využijeme větu 2 a k prvkům množiny M přidáme všechny jejich součiny, pak všechny prvky inverzní k takto získaným prvkům, dále všechny součiny takto vzniklých prvků, inverzní prvky k nim atd., až obdržíme množinu, která je podgrupou.

Tuto konstrukci si nejprve ukážeme na příkladě.

Příklad 5. Vezměme grupu $(G, \cdot)$, která modeluje sčítání na hodinovém ciferníku s číslicemi 1, 2, ..., 24 (srovnej též s příkladem 5 z kapitoly II, § 4). Operace v G je tedy definována takto: pro libovolná čísla $a, b \in \{1, 2, ..., 23, 24\}$ je

$$a \,.\, b = a+b \quad \text{pro} \quad a+b \leqq 24,$$

$$a \,.\, b = a+b-24 \quad \text{pro} \quad a+b > 24,$$

kde na pravé straně rovností je obvyklé sčítání celých čísel. Tuto operaci ještě znázorníme v tabulce 2.

$\cdot$	24	1	2	3	...	21	22	23
24	24	1	2	3	...	21	22	23
1	1	2	3	4	...	22	23	24
2	2	3	4	5	...	23	24	1
3	3	4	5	6	...	24	1	2
...	...	...	...	...	...	...	...	...
21	21	22	23	24	...	18	19	20
22	22	23	24	1	...	19	20	21
23	23	24	1	2	...	20	21	22

Tab. 2

a) Vezměme dále množinu $M=\{2, 8\} \subseteqq G$ a zkusme nalézt $[M]$. K množině M připojíme neutrální prvek grupy G, tj. 24, a prvky $2 \,.\, 2=4$, $2 \,.\, 8=10$ a $8 \,.\, 8=16$, takže obdržíme množinu

$$M_1 = \{2, 4, 8, 10, 16, 24\}.$$

Ta zřejmě není podgrupou v G, neboť neobsahuje například inverzní prvky ke všem svým prvkům. Proto k M_1 přidáme ještě prvky $2^{-1} = 22$, $4^{-1} = 20$, $8^{-1} = 16$, $10^{-1} = 14$, $16^{-1} = 8$ a vytvoříme množinu

$$M_2 = \{2, 4, 8, 10, 14, 16, 20, 22, 24\}.$$

Ani tato množina není ještě podgrupou v G, neboť neobsahuje například součin $2 . 4 = 6$. Připojíme tudíž k M_2 všechny součiny jejích prvků, které do ní nepatří. Jsou to prvky $2 . 4 = 6$, $2 . 10 = 12$ a $2 . 16 = 18$. O takto vzniklé množině

$$M_3 = \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24\}$$

se lze již snadno přesvědčit, že je podgrupou v G. Ze způsobu, jakým byla konstruována, vyplývá, že je nejmenší podgrupou v G, která obsahuje množinu M, takže musí být

$$[M] = [2, 8]^{*)} = [M_3].$$

b) Zvolíme-li $M = \{18, 24\}$, lze obdobně nalézt

$$[M] = [18, 24] = \{6, 12, 18, 24\}.$$

c) Je-li $M = \emptyset$ anebo $M = \{24\}$, je zřejmě $[M] = \{24\}$.

Z naší úvahy o podgrupě $[M]$ a z předchozího příkladu vyplývá, že množina $[M]$ se skládá právě ze všech prvků tvaru

$$(6) \qquad a_1^{k_1} a_2^{k_2} \dots a_m^{k_m},$$

kde m je nějaké přirozené číslo, $a_1, a_2, \dots, a_m$ jsou prvky z M a $k_1, k_2, \dots, k_m$ čísla 1 nebo -1.

Snadno ověříme, že množina všech prvků tvaru (6) je podgrupou v uvažované grupě G: součin libovolných dvou prvků tohoto tvaru má díky asociativnosti opět tento tvar a inverzní prvek k (6), tj. prvek

$$a_m^{-k_m} a_{m-1}^{-k_{m-1}} \dots a_2^{-k_2} a_1^{-k_1},$$

je též zmíněného tvaru. Naopak je rovněž ihned zřejmé, že každá podgrupa v G obsahující množinu M musí obsahovat i každý prvek tvaru (6).

Poznamenejme ještě, že v řadě konkrétních případů se mohou některé prvky tvaru (6) sobě rovnat, i když jejich zápisy (6) se budou lišit. Výsledná množina může být i konečná, jako tomu bylo třeba v příkladě 5. Zřejmě obdržíme konečnou množinu $[M]$ vždy, když grupa G sama bude konečná. Avšak ke konečné množině

---

*) Místo zápisu $[\{2, 8\}]$ píšeme stručně jen $[2, 8]$; obdobně i v dalším textu.

můžeme dospět i v případě nekonečné grupy G; například pro $M = \{1\}$, kde 1 je neutrální prvek v G, je $[M] = \{1\}$.

Všimneme si nyní speciálního případu, kdy množina M je jednoprvková.

Definice. *Grupa G, která má jednoprvkový systém generátorů, se nazývá cyklická grupa.*

Řád cyklické grupy $G = [a]$ generované prvkem a se nazývá rovněž řád prvku a.

Vyšetřeme nyní, jaké možnosti mohou nastat pro cyklické grupy. Mějme tedy dánu grupu $(G, \cdot)$ a nechť $M = \{a\}$, kde $a \in G$. Podgrupa $[M] = [a]$ se — jak již víme — skládá ze všech těch prvků grupy G, které lze zapsat ve tvaru (6), kde ovšem nyní je

$$a_1 = a_2 = \dots = a_m = a.$$

Proto díky asociativnosti můžeme každý takový prvek zapsat ve tvaru

$$(6') \qquad a^k, \quad k \in \mathbf{Z}.$$

Je tedy (označíme-li neutrální prvek grupy G symbolem e, abychom jej odlišili od celého čísla $1 \in \mathbf{Z}$)

$$(7) \qquad [M] = [a] = \{\dots, a^{-2}, a^{-1}, a^0 = e, a^1 = a, a^2, a^3, \dots\}.$$

Pro tuto množinu zřejmě nastane právě jeden z těchto případů:

1. všechny mocniny prvku a s různými exponenty jsou navzájem různé;
2. alespoň dvě mocniny prvku a s různými exponenty jsou si rovny.

Nastane-li případ 1, je $[a]$ nekonečná grupa, takzvaná nekonečná cyklická grupa (a prvek a se pak nazývá prvek nekonečného řádu).

V následující větě ukážeme důležitou vlastnost nekonečných cyklických grup.

Věta 5. *Každá nekonečná cyklická grupa je izomorfní s aditivní grupou celých čísel $(\mathbf{Z}, +)$, a tedy libovolné dvě nekonečné cyklické grupy jsou navzájem izomorfní.*

Důkaz. Nechť a je prvek grupy $(G, \cdot)$ a nechť

$$[a] = \{\dots, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\}$$

je nekonečná cyklická grupa. Definujme zobrazení φ tímto způsobem:

$$(\forall k \in \mathbf{Z}) \quad \varphi(a^k) = k$$

Díky našemu předpokladu o $[a]$ je zřejmě φ prosté zobrazení množiny $[a]$ na množinu všech celých čísel $\mathbf{Z}$. Jsou-li a^k, a^l libovolné prvky z $[a]$, je

$$\varphi(a^k \cdot a^l) = \varphi(a^{k+l}) = k + l = \varphi(a^k) + \varphi(a^l),$$

takže φ je izomorfismus $([a], \cdot)$ na $(\mathbf{Z}, +)$.

Tedy libovolná nekonečná cyklická grupa je izomorfní se $(\mathbf{Z}, +)$, z čehož již snadno nahlédneme, že každé dvě nekonečné cyklické grupy jsou navzájem izomorfní. Tím je věta 5 dokázána.

Vyšetříme nyní druhou možnost, kdy pro množinu $[a]$ z (7) nastane případ 2, tj. když platí

(8) $$(\exists r, s \in \mathbf{Z})\, r \neq s \wedge a^r = a^s.$$

Ukážeme, že v tomto případě je $[a]$ konečná množina, takzvaná konečná cyklická grupa.

Nechť pro $a \in G$ platí (8). Bez omezení obecnosti můžeme předpokládat, že $r < s$. Vynásobením rovnosti $a^r = a^s$ prvkem $a^{-r} = (a^{-1})^r$ obdržíme (e značí neutrální prvek grupy G)

$$a^0 = e = a^{s-r},$$

přičemž $s - r$ je díky našemu předpokladu kladné přirozené číslo. Množina všech těch kladných přirozených čísel n, pro něž

$$a^n = e,$$

je tedy neprázdná. Takže podle tvrzení (A) z kapitoly V, § 1 existuje nejmenší kladné přirozené číslo této vlastnosti, označíme je m.

Ukážeme, že v tomto případě je

$$[a] = \{a^0 = e, a, a^2, \ldots, a^{m-1}\}.$$

Z definice čísla m plyne, že pro libovolná dvě celá čísla r, s, kde $r < s$ a pro něž platí $s - r < m$, musí být $a^r \neq a^s$. Tedy speciálně libovolné dva z prvků

$$a^0, a, a^2, \ldots, a^{m-1}$$

jsou různé.

Je-li k libovolné celé číslo, existují podle věty o dělení se zbytkem v $\mathbf{Z}$ (viz kapitola VII, § 1, věta 8) celá čísla p a z tak, že platí

$$k = mp + z, \quad 0 \leqq z < m.$$

Tedy potom

$$a^k = a^{mp+z} = (a^m)^p a^z = e \cdot a^z = a^z,$$

a proto každá celočíselná mocnina čísla a patří do množiny $\{a^0, a, a^2, \ldots, a^{m-1}\}$.

Cyklická grupa $[a]$ je tedy v tomto případě konečná a má řád m (takže i prvek a je řádu m).

Z předchozí úvahy je ihned vidět, jak postupovat při zjišťování řádu daného prvku (nějaké grupy): utvoříme posloupnost

(9) $$a, a^2, a^3, \ldots$$

Jestliže v této posloupnosti nenarazíme na neutrální prvek e grupy G, je prvek a nekonečného řádu. V opačném případě najdeme první člen v posloupnosti (9), který je roven neutrálnímu prvku; jeho exponent pak udává řád prvku a.

Postup si zopakujeme v následujícím příkladě, jímž současně ukážeme, že k libovolnému přirozenému číslu m lze nalézt grupu, která obsahuje alespoň jeden prvek řádu m.

P ř í k l a d 6. Nechť je dáno libovolné (kladné) přirozené číslo m. Vezměme symetrickou grupu S_m a v ní prvek

$$a = \begin{pmatrix} 1 & 2 & 3 & \ldots & m-1 & m \\ 2 & 3 & 4 & \ldots & m & 1 \end{pmatrix}.$$

Potom postupně

$$a^2 = \begin{pmatrix} 1 & 2 & 3 & \ldots & m-1 & m \\ 3 & 4 & 5 & \ldots & 1 & 2 \end{pmatrix},$$

$$a^3 = \begin{pmatrix} 1 & 2 & 3 & \ldots & m-1 & m \\ 4 & 5 & 6 & \ldots & 2 & 3 \end{pmatrix},$$

....

$$a^{m-1} = \begin{pmatrix} 1 & 2 & 3 & \ldots & m-1 & m \\ m & 1 & 2 & \ldots & m-2 & m-1 \end{pmatrix},$$

$$a^m = \begin{pmatrix} 1 & 2 & 3 & \ldots & m-1 & m \\ 1 & 2 & 3 & \ldots & m-1 & m \end{pmatrix} = e.$$

Protože a^m je mocnina s nejmenším exponentem, která je rovna neutrálnímu prvku v S_m, jímž je identická permutace, je řád prvku a skutečně roven m.

Pro cyklické grupy konečného řádu lze odvodit větu obdobnou větě 5. Úlohu grupy $(\mathbf{Z}, +)$ v ní budou hrát grupy $(\mathbf{Z}_m, \oplus)$ zbytkových tříd Z modulo m, modelující sčítání na ciferníku o m číslicích.

Je-li dáno kladné přirozené číslo m, bude

$$\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$$

a tabulka operace má tvar uvedený v tabulce 3 (nulový prvek nebudeme značit m, nýbrž v souladu s aditivní formou zápisu symbolem 0).

$\oplus$	0	1	2	...	$m-2$	$m-1$
0	0	1	2	...	$m-2$	$m-1$
1	1	2	3	...	$m-1$	0
2	2	3	4	...	0	1
...	...	...	...	...	...	...
$m-2$	$m-2$	$m-1$	0	...	$m-4$	$m-3$
$m-1$	$m-1$	0	1	...	$m-3$	$m-2$

Tab. 3

Operaci v $\mathbf{Z}_m$ můžeme zapsat též tímto způsobem:

$$(\forall a, b \in \mathbf{Z}_m) \quad a \oplus b = a + b + d \,.\, m,$$

kde „+“ značí sčítání celých čísel, $d = 0$, když $a + b < m$, a $d = -1$ pro $a + b > m$.

Věta 6. *Nechť $m > 0$ je libovolné přirozené číslo. Pak každá cyklická grupa řádu m je izomorfní s grupou $(\mathbf{Z}_m, \oplus)$, a tedy každé dvě cyklické grupy téhož (konečného) řádu jsou navzájem izomorfní.*

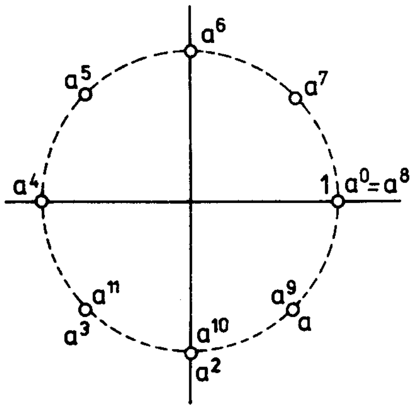
Důkaz přenecháváme čtenáři (viz cvičení 2).

Příklad 7. Nechť $(\mathbf{K}_0, \cdot)$ je multiplikativní grupa komplexních čísel (tj. $\mathbf{K}_0$ je množina všech nenulových komplexních čísel a operací je obvyklé násobení komplexních čísel).

a) Nechť

$$a = k - k\mathrm{i}, \text{ kde } k = \sqrt{2}/2.$$

Máme určit cyklickou podgrupu generovanou prvkem a (a tedy i jeho řád).



Obr. 1

Určíme tedy

$$\begin{array}{ll} a^2 = -2k^2\mathrm{i} = -\mathrm{i}, & a^3 = -k - k\mathrm{i}, \\ a^4 = -1, & a^5 = -k + k\mathrm{i}, \\ a^6 = 2k^2\mathrm{i} = \mathrm{i}, & a^7 = k + k\mathrm{i}, \\ a^8 = 2k^2 = 1. & \end{array}$$

Takže cyklická grupa $[a]$ má řád 8. Znázorníme-li její prvky v Gaussově rovině (viz obr. 1), leží jejich obrazy na kružnici a nápadně ukazují souvislost s počítáním na ciferníku o osmi číslicích.

b) Stanovme obdobně $[b]$ pro prvek

$$b = 1 + \mathrm{i} \in \mathbf{K}_0.$$

Vypočteme postupně

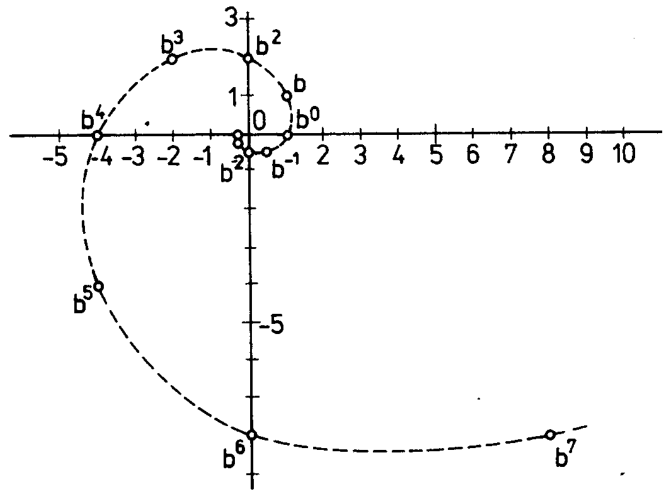
$$\begin{array}{ll} b^2 = 2\mathrm{i}, & b^3 = -2 + 2\mathrm{i}, \\ b^4 = -4, & b^5 = -4 - 4\mathrm{i}, \\ b^6 = -8\mathrm{i}, & b^7 = 8 - 8\mathrm{i}, \\ b^8 = 16, & b^9 = 16 + 16\mathrm{i}. \end{array}$$

Lze ukázat, že pro libovolné kladné celé číslo k takové, že $k = 8r + s$, kde $0 < s < 8$, platí

$$b^k = 16^r b^s \tag{10}$$

(přičemž $b^0 = 1$). Je tedy vidět, že v posloupnosti

$$b^0, b, b^2, b^3, \ldots$$



Obr. 2

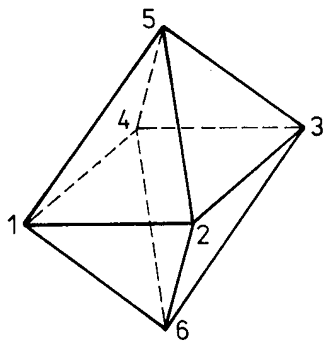
jsou všechny prvky navzájem různé, takže $[b]$ je nekonečná cyklická grupa. V $[b]$ proto musí být též prvky

$$b^{-1} = 1/2 - i/2, \qquad b^{-2} = -i/2,$$
$$b^{-3} = 1/4 - i/4, \qquad b^{-4} = -1/4$$

atd. Lze ostatně snadno nahlédnout, že vzorec (10) platí i pro k záporná. Znázorníme-li několik z prvků nekonečné cyklické grupy $[b]$ v Gaussově rovině, vidíme (viz obr. 2), že leží na spirále. Umístění mocnin b^k na této spirále je „obdobné" jako umístění obrazů celých čísel na číselné ose, což nás podobně jako v případě a) upozorňuje na izomorfismus grupy $[b]$ a grupy $(\mathbf{Z}, +)$.

V následujícím příkladě vyšetříme grupu tzv. zákrytových pohybů pravidelného osmistěnu.

P ř í k l a d 8. Mějme dán pravidelný osmistěn, jehož vrcholy označíme čísly 1, 2, 3, 4, 5, 6 (viz obr. 3). Zákrytovým pohybem (viz též kapitola II, § 4, příklad 8) daného osmistěnu rozumíme takové jeho přemístění, při němž tento osmistěn jako celek splyne s původní polohou. Přitom ovšem jednotlivé vrcholy, hrany i stěny uvažovaného osmistěnu mohou změnit své místo, ale pouze tak, že každý vrchol přejde opět v některý vrchol, a tedy i hrana v hranu a stěna ve stěnu.



Obr. 3

Zákrytové pohyby daného osmistěnu budeme popisovat pomocí permutací, které udávají přemístění vrcholů. Tedy permutací

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ i_1 & i_2 & i_3 & i_4 & i_5 & i_6 \end{pmatrix}$$

zapíšeme zákrytový pohyb, při němž vrchol 1 přejde ve vrchol označený i_1, atd.

Je zřejmé, že provedení dvou zákrytových pohybů po sobě dá opět zákrytový pohyb uvažovaného osmistěnu, takže jde o operaci, a můžeme proto hovořit

o struktuře zákrytových pohybů daného osmistěnu. Asociativnost této struktury je jasná. Rovněž je ihned vidět, že jejím neutrálním prvkem je „pohyb", při němž všechny vrcholy osmistěnu zůstanou na svých místech; je popsán identickou permutací. Pro libovolný zákrytový pohyb, který převádí náš osmistěn z výchozího postavení do nějaké pozice, je pohyb převádějící ho z této pozice do polohy výchozí zřejmě opět zákrytový pohyb, který je inverzní k pohybu výchozímu. Tedy struktura zákrytových pohybů pravidelného osmistěnu je grupa; značíme ji Z_8.

Prvkům grupy Z_8 lze — jak jsme již uvedli — přiřadit (a to vzájemně jednoznačně) permutace ze symetrické grupy S_6. Při tomto přiřazení operaci v Z_8 (tj. skládání zákrytových pohybů) odpovídá zřejmě skládání těchto permutací. Proto je grupa Z_8 izomorfní s jistou podgrupou grupy S_6. Při vyšetřování grupy Z_8 můžeme tedy pracovat s odpovídajícími prvky této podgrupy.

Neutrální prvek grupy Z_8 označíme E; jak jsme již řekli, odpovídá mu identická permutace, což zapíšeme

$$E = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}.$$

Dalšími prvky grupy Z_8 jsou otáčení (o 90°, 180° a 270°) kolem os osmistěnu procházejících vždy protilehlými vrcholy, dále otáčení kolem os procházejících středy protějších stěn (rovnostranných trojúhelníků) o 120° či 240° a konečně překlápění kolem os procházejících středy protějších hran osmistěnu.

Označme otočení (o 90°) kolem osy jdoucí vrcholy 5, 6 symbolem A, tj.

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 5 & 6 \end{pmatrix}.$$

Prvek A je řádu 4, takže cyklická podgrupa jím vytvořená

$$[A] = \{A, A^2, A^3, E\}, \quad A^4 = E,$$

přičemž

$$A^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix},$$

$$A^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix}.$$

Podobně označíme

$$B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 5 & 2 & 4 \end{pmatrix}$$

otočení o 90° kolem osy procházející vrcholy označenými 1, 3; platí obdobně

$$[B] = \{B, B^2, B^3, E\}, \quad B^4 = E$$

a konečně

$$C = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 2 & 6 & 4 & 3 & 1 \end{pmatrix}$$

je otočení o 90° kolem osy jdoucí vrcholy 2, 4; platí přitom

$$[C] = \{C, C^2, C^3, E\}, \quad C^4 = E.$$

Tím jsme získali zatím celkem 10 prvků grupy Z_8; zřejmě prvky A^3, B^3, C^3 mají řád 4 a prvky A^2, B^2, C^2 mají řád 2.

Snadno ověříme, že platí

$$A^2B^2 = B^2A^2 = C^2 \tag{11}$$

a obdobné rovnosti, jež lze obdržet cyklickou záměnou znaků A, B, C.

Součin

$$AB = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 2 & 3 & 5 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 6 & 3 & 5 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 3 & 2 & 4 \end{pmatrix}$$

je zřejmě otočení (o 120°) kolem osy procházející středy trojúhelníků o vrcholech 152 a 364, takže je prvkem řádu 3, tj.

$$[AB] = \{AB, (AB)^2, E\}, \quad (AB)^3 = E.$$

Přepočtením můžeme snadno ověřit, že platí

$$AB = BC = CA,$$
$$(AB)^2 = B^3A^3 = C^3B^3 = A^3C^3.$$

Obdobně můžeme zjistit, že

$$AC = B^3A = CB^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 2 & 6 & 3 & 1 \end{pmatrix},$$

$$BA = AC^3 = C^3B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 5 & 1 & 3 \end{pmatrix},$$

$$CB = A^3C = BA^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 4 & 5 & 3 & 1 \end{pmatrix}$$

jsou po řadě otáčení (o 120°) kolem os procházejících středy trojúhelníků o vrcholech 146 a 253, respektive 145 a 263, respektive 126 a 345. Jsou to vesměs prvky řádu 3, takže jsme získali dalších 8 prvků grupy Z_8: AB, $(AB)^2$, AC, $(AC)^2$, BA, $(BA)^2$, CB, $(CB)^2$.

Zbývajících 6 prvků grupy Z_8, jež jsou otáčení (o 180°) kolem os procházejících

středy protějších hran, obdržíme tímto způsobem:

$$AB^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 3 & 6 & 5 \end{pmatrix} \quad \text{pro hrany 12 a 34,}$$

$$BA^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 6 & 1 & 5 & 4 & 2 \end{pmatrix} \quad \text{pro hrany 26 a 45,}$$

$$AC^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 6 & 5 \end{pmatrix} \quad \text{pro hrany 14 a 23,}$$

$$CA^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 1 & 3 \end{pmatrix} \quad \text{pro hrany 15 a 36,}$$

$$BC^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 2 & 4 \end{pmatrix} \quad \text{pro hrany 25 a 46,}$$

$$CB^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 5 & 2 & 3 & 1 \end{pmatrix} \quad \text{pro hrany 16 a 35.}$$

Nalezli jsme tedy všech 24 prvků grupy Z_8 a současně známe všechny její cyklické podgrupy. V přehledu jsou to:

9 cyklických podgrup řádu 2 generovaných šesti výše jmenovanými prvky

$$AB^2, BA^2, AC^2, CA^2, BC^2, CB^2$$

a dále prvky

$$A^2, B^2, C^2,$$

4 cyklické podgrupy řádu 3

$$[AB] = \{AB, (AB)^2 = B^3A^3, E\},$$
$$[BA] = \{BA, (BA)^2 = A^3B^3, E\},$$
$$[AC] = \{AC, (AC)^2 = A^3B, E\},$$
$$[CB] = \{CB, (CB)^2 = AB^3, E\},$$

3 cyklické podgrupy řádu 4 generované prvky A, B, C.

Grupa Z_8 je — jak vyplývá např. z (6) — generována prvky A, B, C, tj. $Z_8 = [A, B, C]$.

Na závěr tohoto příkladu uvedeme přehled všech podgrup grupy Z_8. K jejich nalezení lze s výhodou užít — vedle již vpředu uvedených — těchto vztahů mezi generátory A, B, C:

$$A = BAC, \quad B = CBA, \quad C = ABC$$
$$AB^2 = BCB = CBC = CAB = C^2A$$
$$BC^2 = CAC = ACA = ABC = A^2B$$
$$CA^2 = ABA = BAB = BCA = B^2C$$

(Jejich platnost může čtenář nejsnáze ověřit přechodem k odpovídajícím permutacím; přitom lze využít možnosti cyklické záměny generátorů.)

Přehled podgrup grupy Z_8, jež nejsou cyklické:

a) podgrupy řádu 4

$$A_4 = \{A^2, B^2, C^2, E\}$$
$$B_4 = \{A^2, AB^2, AC^2, E\}$$
$$C_4 = \{B^2, BC^2, BA^2, E\}$$
$$D_4 = \{C^2, CA^2, CB^2, E\}$$

b) podgrupy řádu 6

$$A_6 = \{AB^2, BA^2, CA^2, AC, (AC)^2, E\}$$
$$B_6 = \{BC^2, CB^2, AB^2, BA, (BA)^2, E\}$$
$$C_6 = \{CA^2, AC^2, BC^2, CB, (CB)^2, E\}$$
$$D_6 = \{AC^2, CB^2, BA^2, AB, (AB)^2, E\}$$

c) podgrupy řádu 8

$$A_8 = \{AB^2, AC^2, B^2, C^2, A, A^2, A^3, E\}$$
$$B_8 = \{BC^2, BA^2, C^2, A^2, B, B^2, B^3, E\}$$
$$C_8 = \{CA^2, CB^2, A^2, B^2, C, C^2, C^3, E\}$$

d) podgrupa řádu 12

$$A_{12} = \{AB, (AB)^2, BA, (BA)^2, AC, (AC)^2, CB, (CB)^2, A^2, B^2, C^2, E\}$$

Doporučujeme čtenáři, aby tohoto příkladu využíval k ilustraci pojmů zavedených v tomto i v následujících paragrafech této kapitoly.

Cvičení

1. Ukažte, že pro libovolné permutace $A, B \in S_n$ je součet počtu inverzí obou těchto permutací buď roven počtu inverzí složené permutace AB, anebo je o sudé číslo menší (viz lemma 1).

[Dané permutace označte

$$A = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 2 & \dots & n \\ j_1 & j_2 & \dots & j_n \end{pmatrix}$$

a zvolte libovolná dvě čísla $r, s \in \{1, 2, \dots, n\}$, $r < s$. Ověřte nejprve tyto dva případy:

a) Nechť i_r, i_s tvoří inverzi v A, tj. $i_s < i_r$. Pak

$$B = \begin{pmatrix} 1 & \dots & i_s & \dots & i_r & \dots & n \\ j_1 & \dots & j_{i_s} & \dots & j_{i_r} & \dots & j_n \end{pmatrix},$$

$$AB = \begin{pmatrix} 1 & \dots & r & \dots & s & \dots & n \\ j_{i_1} & \dots & j_{i_r} & \dots & j_{i_s} & \dots & j_{i_n} \end{pmatrix}$$

a dvojice čísel j_{i_r}, j_{i_s} tvoří inverzi v AB právě tehdy, když netvoří inverzi v B.

b) Nechť i_r, i_s netvoří inverzi v A, tj. $i_r < i_s$. Pak

$$B = \begin{pmatrix} 1 & \dots & i_r & \dots & i_s & \dots & n \\ j_1 & \dots & j_{i_r} & \dots & j_{i_s} & \dots & j_n \end{pmatrix}$$

a j_{i_r}, j_{i_s} tvoří inverzi v AB, právě když tvoří inverzi v B.]

2. Dokažte větu 6.

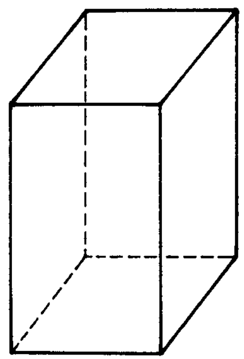
[Postupujte analogicky jako při důkazu věty 5.]

3. Vyšetřete v multiplikativní grupě tělesa komplexních čísel $(\mathbf{K}, \cdot)$ cyklickou podgrupu generovanou prvkem a, pro nějž platí $2a = \mathrm{i} - \sqrt{3}$.

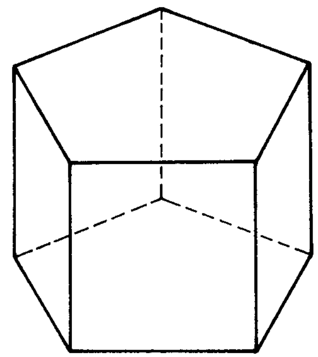
4. Vyšetřete obdobně jako v příkladu 8 grupu zákrytových pohybů

a) čtyřbokého hranolu o čtvercové základně (viz obr. 4),

b) pětibokého hranolu, jehož základnou je pravidelný pětiúhelník a jehož výška je rovna délce strany podstavy (viz obr. 5).



Obr. 4



Obr. 5

§ 2. Lagrangeova věta

Jednoduchá, ale důležitá věta v teorii grup je takzvaná Lagrangeova*) věta. Říká, že řád každé podgrupy dané (konečné) grupy je dělitelem řádu této grupy. Tato věta usnadňuje hledání podgrup dané grupy, neboť značně zmenšuje počet podmnožin grupy, které přitom musíme přezkoumat. Nejprve se zaměříme na vybudování aparátu, který nám umožní uvedenou větu dokázat.

Definice. Komplexem *(v dané grupě) nazveme každou neprázdnou podmnožinu této grupy.*

Je-li $(G, \cdot)$ daná grupa, tvoří všechny komplexy v G množinu $P(G) - \{\emptyset\}$,**) kterou označíme symbolem $\hat{G}$.

Je účelné v množině $\hat{G}$ definovat (binární) operaci „$\odot$" násobení komplexů tímto způsobem:

(1) $$(\forall X, Y \in \hat{G})\; X \odot Y = \{z \in G;\; (\exists x \in X)(\exists y \in Y) z = x \,.\, y\}$$

$X \odot Y$ je tedy množina všech těch prvků z G, které lze psát jako „součin" libovolného prvku z X a libovolného prvku z Y.

Příklad 1. Buď $(G, *)$ grupa zadaná následující tabulkou:

$*$	A	B	C
A	A	B	C
B	B	C	A
C	C	A	B

Množina $\hat{G} = P(G) - \{\emptyset\}$ má $2^3 - 1 = 7$ prvků:

$$\hat{G} = \{\{A\}, \{B\}, \{C\}, \{A, B\}, \{A, C\}, \{B, C\}, \{A, B, C\}\}$$

Dále je například

$$\{B\} \odot \{A, C\} = \{z \in G;\; z = x * y \wedge x \in \{B\} \wedge y \in \{A, C\}\} = \{B, A\};$$
$$\{A, B, C\} \odot \{C\} = \{C, A, B\}$$

a podobně.

Snadno nahlédneme, že $\odot$ je operací v množině $\hat{G}$: Nechť $X, Y \in \hat{G}$, pak $X \neq \emptyset$, $Y \neq \emptyset$, takže existují $x \in X$, $y \in Y$. Prvek $x \,.\, y$ leží v $X \odot Y \subseteq G$, a tedy $X \odot Y \neq \emptyset$, takže $X \odot Y \in \hat{G}$.

*) Joseph Louis Lagrange (1736—1813) — vynikající francouzský matematik.

**) Pro libovolnou množinu X označujeme symbolem $P(X)$ potenci množiny X, tj. systém všech podmnožin množiny X (viz kapitola I, § 4).

Prozkoumejme nyní strukturu $(\hat{G}, \odot)$. Velmi snadno zjistíme — vyplývá to téměř ihned z asociativnosti $(G, \cdot)$ — že $(\hat{G}, \odot)$ je pologrupa. Dále je zřejmé, že prvek $\{1\} \in \hat{G}$ (kde 1 je jednotkový prvek v G) je neutrálním prvkem v $(\hat{G}, \odot)$. Tedy platí:

Lemma 1. *Struktura $(\hat{G}, \odot)$ je pologrupa s neutrálním prvkem. Jestliže výchozí grupa G má alespoň dva různé prvky, není $(\hat{G}, \odot)$ grupou; tj. nemá vlastnost existence inverzních prvků.*

Ukažme si to na grupě z příkladu 1. Zde $(\hat{G}, \odot)$ má neutrální prvek $\{A\}$. Zvolme si prvek $\{B, C\} \in \hat{G}$; snadno se pomocí tabulky přesvědčíme, že pro každé $X \in \hat{G}$ je $\{B, C\} \odot X \neq \{A\}$.

Přestože $(\hat{G}, \odot)$ není strukturou s inverzními prvky, ukazuje se účelné zavést pojem inverzního komplexu:

Nechť $X \in \hat{G}$, pak komplexem inverzním k X — označujeme ho X^{-1} — rozumíme množinu

$$X^{-1} = \{y \in G;\quad (\exists x \in X) y = x^{-1}\},$$

tj. množinu všech prvků inverzních k jednotlivým prvkům množiny X.

Znovu upozorňujeme, že inverzní komplex nehraje v $\hat{G}$ roli inverzního prvku; existují $X \in \hat{G}$ tak, že $X \odot X^{-1} \neq \{1\}$. Položíme-li v příkladu 1 např. $X = \{A, B\}$, je $X^{-1} = \{A, C\}$ a $X \odot X^{-1} = \{A, B, C\} \neq \{A\}$.

Poněvadž $(\hat{G}, \odot)$ není grupou, budeme se zajímat, zda neexistuje alespoň její podstruktura, která by grupou byla. Odpověď dává následující úvaha.

Označme symbolem $\hat{G}_0$ množinu všech jednoprvkových komplexů grupy G, tj.

$$\hat{G}_0 = \{\{x\};\; x \in G\}.$$

Jsou-li $\{x\}, \{y\} \in \hat{G}_0$, je

$$\{x\} \odot \{y\} = \{x, y\},$$

což je rovněž prvek z $\hat{G}_0$, takže $(\hat{G}_0, \odot)$ je struktura. Poněvadž operace $\odot$ v $\hat{G}_0$ je zúžení operace $\odot$ v G, je $(\hat{G}_0, \odot)$ dokonce podstruktura struktury $(\hat{G}, \odot)$. Jde opět zřejmě o pologrupu s neutrálním prvkem. Navíc má $(\hat{G}_0, \odot)$ vlastnost inverzních prvků: buď $\{x\}$ libovolný prvek z $\hat{G}_0$, pak pro prvek $\{x^{-1}\} \in \hat{G}_0$ platí $\{x\} \odot \{x^{-1}\} = \{1\}$. Dokázali jsme tedy:

Lemma 2. *Struktura $(\hat{G}_0, \odot)$ je grupa.*

Dokonce — jak hned ukážeme — je $(\hat{G}_0, \odot)$ grupou izomorfní s $(G, \cdot)$. K důkazu stačí definovat zobrazení φ množiny $\hat{G}_0$ na G takto:

$$(\forall \{x\} \in \hat{G}_0) \quad \varphi(\{x\}) = x$$

Ověření, že jde opravdu o izomorfní zobrazení, je triviální a přenecháme je čtenáři.

V grupě z příkladu 1 je $\hat{G}_0 = \{\{A\}, \{B\}, \{C\}\}$, což je zřejmě (při zvolené operaci $*$) struktura izomorfní s $G = \{A, B, C\}$.

Protože $(\hat{G}_0, \odot)$ a $(G, \cdot)$ jsou izomorfní struktury, můžeme je ztotožnit. To znamená, že každý prvek struktury $\hat{G}_0$ budeme považovat za totožný s tím prvkem v G, který je jeho obrazem při zobrazení φ (například: $\{x\} = x$), a navíc nebudeme činit rozdíl mezi operacemi v obou strukturách. Po přijetí této úmluvy můžeme tedy říci, že $(G, \cdot)$ je podgrupa v $(\hat{G}, \odot)$. Proto budeme od této chvíle operaci v $\hat{G}$ (která je nyní jen rozšířením operace v G) značit také „$\cdot$“. Díky našim úmluvám píšeme tedy nyní i při práci v $\hat{G}$ místo $X \odot Y$, resp. $\{a\} \odot Y$, resp. $\{a\} \odot \{b\}$ jen $X . Y$, resp. $a . Y$, resp. $a . b$.

Strukturu $(\hat{G}, \cdot)$ využijeme k zavedení pojmu rozkladu grupy podle její podgrupy. Mějme dánu libovolnou grupu $(G, \cdot)$ a nechť H je libovolná její podgrupa. Budeme se zajímat o speciální prvky z $(\hat{G}, \cdot)$ — totiž o ty, které lze psát ve tvaru $x . H$, kde x je libovolný prvek z G.

Nejprve ukážeme, že platí:

Lemma 3. *Nechť* $(G, \cdot)$ *je grupa, H její podgrupa; pak systém*

(2) $$S = \{x . H\}_{x \in G}$$

je rozklad množiny G (definice rozkladu množiny viz kapitola II, § 2).

Důkaz. Neprázdnost množin $x . H$ (pro každé $x \in G$) je díky faktu $H \neq \emptyset$ (jde o podgrupu) zřejmá, stejně tak jako podmínka $x . H \subseteq G$ (tj. $xH \in \hat{G}$). Rovněž platnost inkluze $\bigcup_{x \in G} \{xH\} \supseteq G$ je evidentní: když $z \in G$ (z libovolné), lze psát $z = z . 1$, a tedy $z \in z . H$, odkud plyne ihned $z \in \bigcup_{x \in G} \{xH\}$.

Konečně nechť prvky $x, y \in G$ jsou takové, že $x . H \cap y . H \neq \emptyset$. Dokážeme, že pak $xH = yH$; přesněji řečeno dokážeme pouze $xH \subseteq yH$; důkaz „obrácené“ inkluze se provádí analogicky. Nechť tedy u je libovolný prvek z množiny xH. Potom existuje $h_1 \in H$ tak, že $u = x . h_1$. Poněvadž průnik xH a yH je neprázdný, existuje prvek z tak, že $z \in xH$ a současně $z \in yH$, což znamená, že existují prvky h_2, h_3 takové, že $z = x . h_2$ a také $z = y . h_3$. Odtud $x . h_2 = y . h_3$ a podle pravidel počítání v grupě $x = y . h_3 . h_2^{-1}$. Tedy lze psát $u = x . h_1 = y . h_3 . h_2^{-1} . h_1$. Protože součin $h_3 . h_2^{-1} . h_1 \in H$, je $u \in y . H$, takže $xH \subseteq yH$.

Systém S z lemmatu 3 nazýváme rozkladem grupy G na levé třídy podle podgrupy H a jeho prvky, tj. množiny xH, se nazývají levé třídy (podle podgrupy H).

Úvahou zcela obdobnou lze zavést rozklad grupy G na pravé třídy podle

podgrupy H, jímž je systém

(3) $$S' = \{H . x\}_{x \in G}.$$

Při konstrukci struktury $(G, \cdot)$ i při důkazech lemmat 1 a 3 jsme nikde nepoužívali existenci inverzních prvků ve výchozí struktuře $(G, \cdot)$. Proto všechny naše úvahy zůstanou v platnosti, i když předpokládáme, že struktura $(G, \cdot)$ je pouze pologrupa s neutrálním prvkem. Speciálně tedy pro libovolnou podgrupu H uvažované pologrupy G (s neutrálním prvkem) můžeme zavést pojem levé (pravé) třídy podle H (v pologrupě G) i pojem rozkladu pologrupy G na levé (pravé) třídy podle podgrupy H.

Další úvahy budeme formulovat opět pouze pro grupy a přenecháváme čtenáři, aby sám prověřil, které z nich zůstávají v platnosti i pro pologrupy.

Nejprve se budeme zabývat otázkou „počtu“ prvků v levých, respektive pravých rozkladových třídách dané grupy podle podgrupy a souvislostí s „počtem“ prvků podgrupy H.

Lemma 4. *Buď* $(G, \cdot)$ *grupa, H její podgrupa. Pak pro každé $x \in G$ existuje vzájemně jednoznačné zobrazení φ množiny H na xH.*

Důkaz. Buď $x \in G$ pevné, pak zřejmě stačí zvolit φ takto:

$$(\forall h \in H)\varphi(h) = xh$$

Zobrazení φ je zřejmě zobrazením H na xH. Buďte h_1, $h_2 \in H$, $h_1 \neq h_2$; potom $xh_1 \neq xh_2$ (v opačném případě díky vlastnosti krácení v G dostaneme $h_1 = h_2$), a tedy φ je prosté zobrazení.

Z lemmatu 4 vyplývá, že lze na sebe vzájemně jednoznačně zobrazit i libovolné dvě levé třídy rozkladu (2). Když například $\varphi_1 : H \leftrightarrow x_1H$, $\varphi_2 : H \leftrightarrow x_2H$, pak složené zobrazení $\varphi_1^{-1} \circ \varphi_2$ zobrazí vzájemně jednoznačně x_1H na x_2H.

Formulaci a důkaz tvrzení, které je analogické s lemmatem 4 a které vypovídá o pravých rozkladových třídách grupy G podle podgrupy H, přenecháváme čtenáři.

Lemma 5. *Nechť* $(G, \cdot)$ *je grupa, H její podgrupa. Pak pro libovolné prvky x, $y \in G$ platí:*

$$xH = yH \Leftrightarrow y^{-1}x \in H \Leftrightarrow x^{-1}y \in H$$

$$Hx = Hy \Leftrightarrow y . x^{-1} \in H \Leftrightarrow x . y^{-1} \in H$$

Důkaz. Na ukázku ověříme implikaci $xH = yH \Rightarrow y^{-1}x \in H$. Z předpokladu $xH = yH$ plyne existence h_1, $h_2 \in H$ takových, že $xh_1 = yh_2$. „Vynásobíme-li“ tuto rovnost zleva prvkem y^{-1} a zprava h^{-1}, dostaneme $y^{-1}x = h_2 . h_1^{-1} \in H$. Dále například ekvivalenci $y^{-1} . x \in H \Leftrightarrow x^{-1} . y \in H$ ověříme takto:

$$y^{-1}x \in H \Leftrightarrow (y^{-1}.x)^{-1} \in H \Leftrightarrow x^{-1}.y \in H.$$

Zbývající části důkazu nechť si čtenář provede jakožto cvičení (viz cvičení 2).

Z lemmatu 5 plyne, že i pro různé prvky x, $y \in G$ může platit $xH = yH$ či $Hx = Hy$. Díváme-li se na rozklady (2) a (3) jako na množiny, tj. považujeme-li všechny jejich sobě rovné třídy za jediný jejich prvek, lze ukázat, že množiny S a S' mají (při daném G a H) týž „počet" prvků. Tuto skutečnost precizujeme v následujícím lemmatu.

Lemma 6. *Nechť S (resp. S') je rozklad grupy G na levé (resp. pravé) třídy podle její podgrupy H. Pak existuje vzájemně jednoznačné zobrazení množiny S na množinu S'.*

Důkaz. Definujme zobrazení φ množiny S na množinu S' tímto způsobem:

$$(\forall xH \in S) \quad \varphi(xH) = Hx \in S'$$

Ukážeme, že φ je prosté zobrazení. Nechť tedy xH a yH jsou libovolné prvky z S a nechť $xH \neq yH$. Pak podle lemmatu 5 platí

$$(4) \qquad x^{-1}y \notin H.$$

Předpokládejme, že $\varphi(xH) = \varphi(yH)$, tj. $Hx = Hy$. Pak opět podle lemmatu 5 je $y^{-1}x \in H$, a tedy také

$$(y^{-1}x)^{-1} = x^{-1}y \in H,$$

což je ve sporu s (4). Musí tedy být $Hx \neq Hy$, takže φ je prosté zobrazení S na S'.

Právě dokázané lemma nám umožňuje zavést následující pojem.

Definice. *Nechť $(G, \cdot)$ je grupa, H její podgrupa a S rozklad G na levé (pravé) třídy podle H. Je-li S konečná množina, nazývá se počet jejích prvků (tj. počet levých či pravých tříd podle H) index podgrupy H v grupě G. Je-li S nekonečná množina, říkáme, že podgrupa H má nekonečný index v G.*

Věta 1. (Lagrangeova) *Nechť $(G, \cdot)$ je grupa řádu n, H její podgrupa řádu k a indexu m. Pak platí:*

$$n = k.m$$

Důkaz plyne ihned z předchozích úvah: Utvoříme rozklad S grupy G na levé (či pravé) třídy podle podgrupy H. Potom S má m prvků (jimiž jsou po dvou disjunktní třídy, jejichž sjednocení je množina G), z nichž každý má k prvků. Poněvadž řád G je n, platí $n = k.m$.

Důsledek. *Když $(G, \cdot)$ je konečná grupa a H její podgrupa, musí řád podgrupy H dělit řád grupy G.*

Příklad 2. Buď $(G, \cdot)$ grupa zadaná následující tabulkou 4 (jde o grupu zobrazení, která v rovině „reprodukují" čtverec, tzv. grupu zákrytových pohybů čtverce s operací skládání zobrazení).

$\cdot$	1	z_1	z_2	z_3	z_4	z_5	z_6	z_7
1	1	z_1	z_2	z_3	z_4	z_5	z_6	z_7
z_1	z_1	z_2	z_3	1	z_7	z_4	z_5	z_6
z_2	z_2	z_3	1	z_1	z_6	z_7	z_4	z_5
z_3	z_3	1	z_1	z_2	z_5	z_6	z_7	z_4
z_4	z_4	z_5	z_6	z_7	1	z_1	z_2	z_3
z_5	z_5	z_6	z_7	z_4	z_3	1	z_1	z_2
z_6	z_6	z_7	z_4	z_5	z_2	z_3	1	z_1
z_7	z_7	z_4	z_5	z_6	z_1	z_2	z_3	1

Tab. 4

Řád grupy G je 8.

Zvolme podgrupu H_1 v G takto: $H_1 = \{1, z_1, z_2, z_3\}$. Proveďme rozklad G na levé a pravé třídy podle H_1. Podgrupa H_1 má řád 4, takže podle Lagrangeovy věty má v G index 2. To znamená, že množina S bude mít dva prvky.

Je $S = \{x.H_1\}_{x \in G} = \{1.H_1, z_1.H_1, \ldots, z_7.H_1\}$. Je $1H_1 = z_1H_1 = z_2H_1 = z_3H_1 = H_1$. Hledejme tedy $z_4.H_1$. Podle definice násobení komplexů je $z_4.H_1 = \{z_41, z_4z_1, z_4z_2, z_4z_3\} = \{z_4, z_5, z_6, z_7\}$. Díky předchozí úvaze již není nutné vytvářet $z_5.H_1$, $z_6.H_1$ a $z_7.H_1$, neboť jsme již dvě různé levé třídy nalezli a více jich nemůže existovat, tj. $S = \{\{1, z_1, z_2, z_3\}, \{z_4, z_5, z_6, z_7\}\}$. Rovněž množina S' je dvouprvková. Čtenář se snadno přesvědčí, že rozklad G na levé třídy podle H_1 je roven rozkladu na pravé třídy, tedy $S = S'$.

Nechť $H_2 = \{1, z_4\}$. Snadno ověříme, že H_2 je také podgrupa v G. Na rozdíl od H_1 však $S = \{xH_2\}_{x \in G} \neq \{H_2x\}_{x \in G} = S'$. Z Lagrangeovy věty vyplývá, že index H_2 v G je roven číslu 4. Hledejme tedy 4 levé a 4 pravé třídy rozkladů G podle H_2. Z tabulky plyne, že

$$S = \{\{1, z_4\}, \{z_1, z_7\}, \{z_2, z_6\}, \{z_3, z_5\}\},$$
$$S' = \{\{1, z_4\}, \{z_1, z_5\}, \{z_2, z_6\}, \{z_3, z_7\}\},$$

takže $S \neq S'$.

Na závěr tohoto paragrafu ještě výslovně upozorněme na to, že z Lagrangeovy věty neplyne, že ke každému děliteli d řádu konečné grupy nutně existuje její podgrupa řádu d (příklad viz cvičení 4).

Cvičení

1. Dokažte, že libovolný komplex H grupy $(G, \cdot)$ je její podgrupou, právě když platí zároveň

a) $H.H=H$,
b) $H^{-1}=H$.

(Povšimněte si, že tvrzení platí i v případě, když rovnosti v a) a b) nahradíme inkluzí $\subseteq$.)

2. Proveďte úplný důkaz lemmatu 5.

3. Nechť $(G, \cdot)$ je grupa z příkladu 2. Sestrojte rozklady grupy G na levé i pravé třídy podle podgrup

$$H_1=\{1\}, \quad H_2=\{1, z_2\}, \quad H_3=\{1, z_3\}.$$

4. Ukažte, že v alternující grupě A_4 neexistuje žádná podgrupa řádu 6. [Použijte výsledků z příkladu 2 z § 1 a využijte Cayleyho tabulky 6 pro operaci v A_4 z příkladu 2 v následujícím paragrafu.]

5. Dokažte, že platí následující tvrzení.
Nechť $(G, \cdot)$ je konečná grupa řádu n, pak pro libovolný prvek $a \in G$ je $a^n=1$.
[Užijte věty 1 na cyklickou podgrupu $[a]$.]

§ 3. Faktorové grupy

V předchozím paragrafu jsme hovořili o rozkladu grupy G podle podgrupy na levé a pravé třídy. Každý takový rozklad je vlastně systémem podmnožin grupy G, a tedy částí množiny $\hat{G}$ (kde $\hat{G}=P(G)-\{\emptyset\}$, viz § 2). Nyní se budeme zabývat otázkou, zda je možné — eventuálně za jakých podmínek — aby rozklad grupy G podle některé její podgrupy byl nejen podmnožinou $\hat{G}$, ale dokonce — při vhodně zvolené operaci na prvcích rozkladu — i podstrukturou struktury $(\hat{G}, \cdot)$, která je, jak již víme, pologrupou s neutrálním prvkem.

Mějme tedy grupu $(G, \cdot)$ a nějakou její podgrupu H. Uvažujme rozklad G podle H například na levé třídy, tj. systém

$$S=\{x.H\}_{x\in G}.$$

Aby $(S, *)$ byla podstrukturou $(\hat{G}, \cdot)$, musí být $S \subseteq \hat{G}$, což je evidentní, a dále operaci $*$ je třeba definovat tak, aby byla zúžením operace „$\cdot$" na množinu S. Zřejmě přichází v úvahu pouze operace násobení komplexů, takže dále místo $*$ budeme užívat označení „$\cdot$". Je nutné ověřit, zda jde skutečně o operaci v S, tj. zda pro libovolné dvě třídy xH, $yH \in S$ je jejich „součin" opět prvkem S. Zapsáno

formulí to znamená

(1) $$(\forall x, y \in G)\ xH.yH \in S$$

neboli

(2) $$(\forall x, y \in G)\ (\exists z \in G)\ xH.yH=zH.$$

Na následujícím příkladě si ukážeme, že tato podmínka není vždy splněna.

Příklad 1. Vezměme symetrickou grupu S_3 (viz kapitola II, § 4, příklad 4). Její prvky jsme označili

$$i=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad a=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}, \quad b=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},$$

$$c=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \quad d=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \quad e=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

Operaci „$\circ$", tj. skládání permutací, můžeme popsat tabulkou 5.

$\circ$	i	a	b	c	d	e
i	i	a	b	c	d	e
a	a	b	i	e	c	d
b	b	i	a	d	e	c
c	c	d	e	i	a	b
d	d	e	c	b	i	a
e	e	c	d	a	b	i

Tab. 5

Zvolíme podgrupu $H=\{i, e\}$, která je řádu 2, a tedy podle Lagrangeovy věty má index 3. To znamená, že systém S obsahuje tři (různé) levé třídy:

$$S=\{H, H_1, H_2\},$$

kde

$$H_1=\{a, d\}=aH=dH,$$
$$H_2=\{b, c\}=bH=cH$$

a samozřejmě

$$H=\{i, e\}=iH=eH.$$

Vynásobíme-li nyní např.

$$iH.eH=H.H=H=iH,$$

dostaneme stejně, jako když utvoříme „součin"

$$aH.eH=H_1.H=\{a, d\}.\{i, e\}=\{a, d\}=dH,$$

jako výsledek prvek z S. Naproti tomu například $eH \,.\, aH = H \,.\, H_1 = \{a, d, c, b\} \notin S$. Když si čtenář vyzkouší všech 9 „součinů“, zjistí, že převážná většina z nich nejsou levé třídy rozkladu S_3 podle H. Pro zvolenou podgrupu H tedy podmínka (1) neplatí.

Zvolme si jinou, „vhodnější“ podgrupu S_3, například $\overline{H} = \{i, a, b\}$, pak $S = \{\overline{H}, \overline{H}_1\}$, kde

$$\overline{H} = i\overline{H} = a\overline{H} = b\overline{H},$$

$$\overline{H}_1 = \{c, d, e\} = c\overline{H}_1 = d\overline{H}_1 = e\overline{H}_1 \,.$$

Lehce ověříme, že nyní je „součin“ libovolných dvou levých tříd z S opět levou třídou v S.

Z uvedeného příkladu je vidět, že je asi zapotřebí omezit se — požadujeme-li platnost (1) — jenom na jisté podgrupy dané grupy. Budeme-li například předpokládat, že pro podgrupu H platí

$$(\forall y \in G)\; Hy = yH,$$

jinak řečeno, požadujeme-li, aby rozklady na levé a pravé třídy se sobě rovnaly, bude podmínka (1), a tudíž i (2) jistě splněna. Stačí totiž v (2) položit $z = x \,.\, y$, jak vyplývá z následujících vztahů:

$$(xH) \,.\, (yH) = x \,.\, (Hy) \,.\, H = x \,.\, (yH) \,.\, H = xy \,.\, (H \,.\, H) = xy \,.\, H$$

Definice. *Buď $(G, \cdot)$ grupa. Řekneme, že podgrupa N grupy G je* normální podgrupa *v G, právě když*

$$(3) \qquad (\forall g \in G)\; g \,.\, N = N \,.\, g.$$

Z této definice je ihned vidět, že každá podgrupa Abelovy grupy je normální podgrupou. Avšak i každá nekomutativní grupa G má vždy normální podgrupy, jimiž jsou jednotková podgrupa $\{1\}$ (kde 1 je neutrální prvek uvažované grupy G) a grupa G sama. V prvním případě se skládá příslušný rozklad na levé a pravé třídy vesměs z jednoprvkových podmnožin množiny G (a tedy jsou si oba rozklady rovny). Ve druhém případě rozklad G podle G obsahuje jediný prvek, jímž je množina G. Existují (nekomutativní) grupy, které nemají jiné normální podgrupy než zmíněné dvě „samozřejmé“, $\{1\}$ a G.

Pojem normální podgrupy si ještě procvičíme v následujících příkladech.

Příklad 2. Vezmeme grupu všech sudých permutací čtyřprvkové množiny $\{1, 2, 3, 4\}$. Je to (viz § 1) tzv. alternující grupa A_4. Její prvky (je jich 12) označíme takto:

$$E = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \quad a^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix},$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}, \quad b^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix},$$

$$c^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}, \quad d^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

Operaci v A_4 lze popsat tabulkou 6.

$\cdot$	E	A	B	C	a	a^2	b	b^2	c	c^2	d	d^2
E	E	A	B	C	a	a^2	b	b^2	c	c^2	d	d^2
A	A	E	C	B	b^2	c	d	a	a^2	d^2	b	c^2
B	B	C	E	A	c^2	d	c	d^2	b	a	a^2	b^2
C	C	B	A	E	d^2	b	a^2	c^2	d	b^2	c	a
a	a	c^2	d^2	b^2	a^2	E	A	d	B	b	C	c
a^2	a^2	b	c	d	E	a	c^2	C	d^2	A	b^2	B
b	b	a^2	d	c	C	d^2	b^2	E	a	B	c^2	A
b^2	b^2	d^2	c^2	a	c	A	E	b	C	d	B	a^2
c	c	d	a^2	b	A	b^2	d^2	B	c^2	E	a	C
c^2	c^2	a	b^2	d^2	d	B	C	a^2	E	c	A	b
d	d	c	b	a^2	B	c^2	a	A	b^2	C	d^2	E
d^2	d^2	b^2	a	c^2	b	C	B	c	A	a^2	E	d

Tab. 6

Grupa A_4 má — jak si čtenář snadno ověří — právě tyto cyklické podgrupy:

$$[E] = \{E\},\; [A] = \{A, E\},\; [B] = \{B, E\},\; [C] = \{C, E\},$$
$$[a] = \{a, a^2, E\},\; [b] = \{b, b^2, E\},\; [c] = \{c, c^2, E\},$$
$$[d] = \{d, d^2, E\}$$

a dále — mimo A_4 — jedinou podgrupu, jež není cyklická, a to

$$[A, B] = [A, C] = [B, C] = \{A, B, C, E\}.$$

Normální podgrupy v A_4 jsou zřejmě $[E]$ a A_4 sama. Vyšetříme, které z ostatních podgrup jsou v A_4 normální.

Začneme podgrupou $[A]$. Protože levá a pravá třída

$$a[A] = \{c^2, a\},\; [A]a = \{b^2, a\}$$

rozkladů podle $[A]$ jsou různé množiny, které mají neprázdný průnik, nemůže se rozklad na levé třídy podle $[A]$ rovnat rozkladu na třídy pravé, takže $[A]$ není normální podgrupa v A_4.

Obdobně ukážeme, že žádná z dalších cyklických podgrup není normální v A_4:

$$a[B]=\{d^2, a\}\neq[B]a=\{c^2, a\}$$
$$a[C]=\{b^2, a\}\neq[C]a=\{d^2, a\}$$
$$A[a]=\{b^2, c, A\}\neq[a]A=\{c^2, b, a\}$$
$$c[b]=\{d^2, B, c\}\neq[b]c=\{a, C, c\}$$
$$a[c]=\{B, b, a\}\neq[c]a=\{A, d, a\}$$
$$a[d]=\{C, c, a\}\neq[d]a=\{B, b, a\}$$

Avšak podgrupa $[A, B]$ je normální v A_4, neboť pro její rozklady na levé a pravé třídy platí:

$$C[A, B]=\{A, B, C, E\}=[A, B]C$$
$$a[A, B]=\{c^2, d^2, b^2, a\}=[A, B]a$$
$$b[A, B]=\{a^2, d, c, b\}=[A, B]b$$

V závěru příkladu si ještě všimněme této skutečnosti obecnějšího dosahu: podgrupa $[A]$ není, jak jsme ukázali, normální podgrupou v A_4, je však normální podgrupou — jak lze snadno nahlédnout — v grupě $[A, B]$. Tedy táž podgrupa může být normální podgrupou v jedné grupě a nebýt normální podgrupou v grupě druhé. Proto, když hovoříme o normální podgrupě, musíme vždy (pokud to nevyplývá ze souvislosti) uvést, ve které grupě je zkoumaná podgrupa normální.

Ověřování, zda nějaká podgrupa je v dané grupě normální, přímo pomocí podmínky (3) je často poměrně obtížné. Uvedeme proto v dalším textu několik podmínek s (3) ekvivalentních, které jsou pro ověřování normálnosti podgrup zpravidla pohodlnější.

Poznamenejme ještě, že definice normální podgrupy nepožaduje, aby pro každé $g\in G$ a pro každé $n\in N$ platilo $g.n=n.g$, což zřejmě obecně ani neplatí — stačí vzít například za G grupu S_3 (viz příklad 1) a $N=\overline{H}=\{a, b, i\}$. Pak $c.a=d\neq e=a.c$ a přesto N je normální podgrupa. Definice pouze říká, že množina všech prvků tvaru $g.n_1$, kde $g\in G$, $n_1\in N$, je rovna množině všech prvků tvaru $n_2.g$, kde n_2 je jistý prvek z N. Přesná formulace této podmínky je uvedena v následujícím lemmatu.

Lemma 1. *Podgrupa N grupy G je normální podgrupou v G, právě když platí*

(4) $$(\forall g\in G)\,(\forall n_0\in N)\,(\exists n_1, n_2\in N)\,(gn_0=n_1g \wedge n_0g=gn_2).$$

Důkaz lemmatu je snadný a přenecháváme ho do cvičení.

Jinou, ekvivalentní formulaci podmínky (3) dává

Lemma 2. *Podgrupa N je normální podgrupou v G, právě když platí*

(5) $$(\forall g\in G)\; g.N.g^{-1}\subseteq N$$

neboli

(5′) $$(\forall g\in G)\,(\forall n\in N)\; g.n.g^{-1}\in N.$$

Důkaz (pro formuli (5)). Buď nejprve N normální podgrupa v G, $g\in G$ a $x\in g.N.g^{-1}$. Pak existuje $n\in N$ tak, že $x=g.n.g^{-1}$. Díky normalitě N lze psát (viz lemma 1) $g.n=n_1.g$ pro jisté $n_1\in N$. Tedy

$$x=g.n.g^{-1}=n_1.(g.g^{-1})=n_1\in N$$

a podmínka (5) je ověřena.

Nechť naopak (5) platí. Dokážeme, že pro libovolné $g\in G$ je $gN\subseteq Ng$ (obrácená inkluze se ověří analogicky). Buď tedy $g\in G$, $x\in gN$; potom existuje $n\in N$ tak, že $x=g.n$. „Vynásobením" prvkem g^{-1} zprava dostáváme $x.g^{-1}=g.n.g^{-1}$. Podle (5) existuje $n_1\in N$ tak, že $g.n.g^{-1}=n_1$, a proto i $x.g^{-1}=n_1$, odkud $x.g^{-1}.g=n_1.g$, takže $x=n_1.g$, což je prvek z Ng.

Pojem normální podgrupy v grupě $(G, \cdot)$ byl definován tak, že rozklad G (na levé či pravé třídy) podle libovolné její normální podgrupy tvoří vzhledem k operaci násobení komplexů podstrukturu pologrupy $(\hat{G}, \cdot)$. Následující věta ukazuje, že tato podstruktura je dokonce podgrupou v $(\hat{G}, \cdot)$.

Věta 1. *Nechť N je normální podgrupou grupy $(G, \cdot)$ a S rozklad G podle N na levé třídy. Pak struktura $(S, \cdot)$ je grupou.*

Důkaz. Buď $(G, \cdot)$ grupa, N její normální podgrupa. Vytvořme rozklad

$$S=\{xN\}_{x\in G}$$

a zkoumejme vlastnosti struktury $(S, \cdot)$.

Poněvadž $(S, \cdot)$ je podstruktura pologrupy $(\hat{G}, \cdot)$, plyne asociativnost struktury S ihned z téže vlastnosti struktury $\hat{G}$.

Buď dále e neutrální prvek v G. Pak zřejmě $eN=N$. Snadno ověříme, že N je neutrální prvek v $(S, \cdot)$: Nechť xN je libovolný prvek v S. Potom

$$(xN).N=(xN)(eN)=xeNN=xeN=xN$$

a také

$$N(xN)=(eN)(xN)=e(Nx)N=exNN=xN.$$

Je-li xN libovolný prvek z S, je $x^{-1}N$ rovněž prvkem S a platí

$$(xN)(x^{-1}N)=x(Nx^{-1})N=xx^{-1}NN=eN=N$$

a rovněž

$$(x^{-1}N)\,(xN) = x^{-1}(Nx)N = x^{-1}xNN = eN = N.$$

Tedy $(S, \cdot)$ je také struktura s inverzními prvky, a tím je věta 1 dokázána.

Připomeňme, že normální podgrupa N v grupě G byla definována tak, že pro každé $x \in G$ platí $xN = Nx$. Proto věta 1 zůstane v platnosti, když místo rozkladu na levé třídy uvažujeme rozklad na pravé třídy grupy G podle N.

Definice. *Nechť $(G, \cdot)$ je grupa, N normální podgrupa v G. Pak grupa $(S, \cdot)$ resp. $(S', \cdot)$ se nazývá faktorová grupa grupy G podle normální podgrupy N a značí se G/N, přesněji $(G/N, \cdot)$.*

Příklad 3. Uvažujme symetrickou grupu S_3 (viz příklad 1, tabulka 5) a nechť $N = \{i, a, b\}$. Víme již, že N je normální podgrupa v S_3. Lze tedy vytvořit faktorovou grupu S_3/N. Je $S_3/N = \{N, H\}$, kde $H = \{c, d, e\}$. Tato grupa má řád 2 a jí příslušná Cayleyho tabulka má zřejmě tento tvar:

$\cdot$	N	H
N	N	H
H	H	N

Poznamenejme ještě, že lze vytvořit S_3/S_3 a $S_3/\{i\}$ (poněvadž S_3 a $\{i\}$ jsou normální podgrupy v S_3). Snadno nahlédneme, že $S_3/S_3 = \{S_3\}$, takže jde o jednoprvkovou grupu. Faktorová grupa $S_3/\{i\}$ má za prvky všechny jednoprvkové podmnožiny množiny S_3 a je tedy izomorfní s S_3.

Příklad 4. Vezměme grupu A_4 z příkladu 2 a její podgrupu $H = [A, B] = \{A, B, C, E\}$, o níž jsme dokázali, že je normální (v A_4). Třídy rozkladu označme

$$H\ = C\,.\,H = C\,.\,[A, B] = \{A, B, C, E\},$$
$$H_1 = a\,.\,H = a\,.\,[A, B] = \{a, b^2, c^2, d^2\},$$
$$H_2 = b\,.\,H = b\,.\,[A, B] = \{a^2, b, c, d\}.$$

Užitím tabulky 6 snadno ukážeme, že operace „$\cdot$" ve faktorové grupě A_4/H má tuto tabulku:

$\cdot$	H	H_1	H_2
H	H	H_1	H_2
H_1	H_1	H_2	H
H_2	H_2	H	H_1

Příklad 5. Uvažujme grupu $(\mathbf{Z}, +)$ všech celých čísel s operací sčítání. Buď $N = \{x = 4k\,;\ k \in \mathbf{Z}\}$; je ihned vidět, že $(N, +)$ je podgrupou v $(\mathbf{Z}, +)$. Vytvořme

rozklad $\mathbf{Z}$ podle N; tj. např. $\{x + N\}_{x\in\mathbf{Z}}$ — užili jsme zde sugestivnější aditivní zápis $x + N$ namísto xN. Dostaneme

$$\{x + N\}_{x\in\mathbf{Z}} = \{N, H_1, H_2, H_3\},$$

kde $H_1 = \{x = 4k + 1\,;\ k \in \mathbf{Z}\}$, $H_2 = \{x = 4k + 2\,;\ k \in \mathbf{Z}\}$ a $H_3 = \{x = 4k + 3\,;\ k \in \mathbf{Z}\}$. Poněvadž $(\mathbf{Z}, +)$ je Abelova grupa, je N normální podgrupou, a tedy $(\{x + N\}_{x\in\mathbf{Z}}, +)$ je faktorová grupa $\mathbf{Z}/N$.

V závěru tohoto paragrafu si ukážeme ještě jiný způsob zavedení faktorové struktury. Při definici faktorové grupy G/N jsme vycházeli z rozkladu grupy G podle normální podgrupy N. Máme-li však dánu nějakou grupu $(G, \cdot)$, může být rozklad množiny G zadán také jako rozklad podle jisté ekvivalence R definované v G. Tento rozklad (viz kapitola II, § 2) se nazývá rozklad indukovaný ekvivalencí R a značí se G/R. Připomeňme, že třídy tohoto rozkladu jsou podmnožiny $\square Rx$ množiny G definované takto:

$$(\forall x \in G)\,\square Rx = \{y \in G\,;\ yRx\}$$

Je tedy

$$G/R = \{\square Rx\}_{x\in G}.$$

Ptejme se nyní — obdobně jako při vytváření rozkladu G podle podgrupy — jaké podmínky musí splňovat relace R, aby operace násobení komplexů byla operací v množině G/R, tj. aby platilo

$$(6)\qquad (\forall x, y \in G)\,(\exists z \in G)\,\square Rx\,.\,\square Ry = \square Rz.$$

To znamená, že (při daných $x, y \in G$) pro každé $x_1 \in \square Rx$ a každé $y_1 \in \square Ry$ má být $x_1y_1 \in \square Rz$ pro jisté $z \in G$; zapsáno formulí:

$$(6')\qquad (\forall x, y \in G)\,(\exists z \in G)\,(\forall x_1, y_1 \in G)\,(x_1Rx \wedge y_1Ry) \Rightarrow x_1y_1Rz.$$

Lze snadno nahlédnout, že uvedeným podmínkám (6) a (6′) vyhovuje každá relace R v G, která je ekvivalencí a která má vlastnost

$$(7)\qquad (\forall x_1, x_2, y_1, y_2 \in G)\,(x_1Rx_2 \wedge y_1Ry_2) \Rightarrow x_1y_1Rx_2y_2.$$

Pro libovolné prvky $x, y \in G$ pak můžeme položit $z = xy$ (anebo vzít za z součin libovolného prvku $x_1 \in \square Rx$ s libovolným prvkem $y_1 \in \square Ry$). Tato úvaha nás vede k následující definici.

Definice. *Nechť $(G, \cdot)$ je grupa, R relace v množině G. Pak R se nazývá kongruence v grupě $(G, \cdot)$, právě když R je ekvivalence a platí pro ni (7).*

Vybereme-li si tedy na G takovou relaci, která je kongruencí, je $(S, \cdot) = (G/R, \cdot)$ podstruktura $(\hat{G}, \cdot)$ a pro libovolné $\square Rx, \square Ry \in G/R$ je

$$(8)\qquad \square Rx\,.\,\square Ry = \square Rxy.$$

Věta 2. *Nechť* $(G, \cdot)$ *je grupa,* R *relace kongruence na* G. *Pak struktura* $(G/R, \cdot)$ *je také grupou.*

Důkaz. Asociativnost $(G/R, \cdot)$ vyplývá z téže vlastnosti na struktuře $(G, \cdot)$, neboť $(G/R, \cdot)$ je její podstrukturou. Buď e neutrální prvek v G. Pak třída $\square Re$ je neutrálním prvkem v G/R: je-li $\square Rx$ libovolný prvek z G/R, je podle (8)

$$\square Rx \,.\, \square Re = \square Rxe = \square Rx,$$
$$\square Re \,.\, \square Rx = \square Rex = \square Rx.$$

Nechť dále $\square Rx \in G/R$ pro libovolné $x \in G$, pak prvek $\square Rx^{-1} \in G/R$ je k němu inverzní:

$$\square Rx \,.\, \square Rx^{-1} = \square Rx \,.\, x^{-1} = \square Re$$

a obdobně platí

$$\square Rx^{-1} \,.\, \square Rx = \square Rx^{-1} \,.\, x = \square Re.$$

Tedy $(G/R, \cdot)$ je grupa.

Definice. *Grupu* $(G/R, \cdot)$ *z předchozí věty nazýváme* <u>*faktorovou grupou*</u> *grupy* G <u>*podle kongruence*</u> R.

Příklad 6. Vezměme aditivní grupu celých čísel $(\mathbf{Z}, +)$ a definujme v ní relaci R tímto způsobem:

$$(\forall x, y \in \mathbf{Z}) xRy \Leftrightarrow (\exists k \in \mathbf{Z}) x = y + 4k$$

Ověříme, že relace R je kongruence v grupě $(\mathbf{Z}, +)$. Reflexívnost i symetričnost relace R je zřejmá. Zvolme libovolná celá čísla x, y, z taková, že xRy a yRz; pak existují čísla $k, m \in \mathbf{Z}$ tak, že

$$x = y + 4k \wedge y = z + 4m.$$

Potom však

$$x = z + 4m + 4k = z + 4(m + k),$$

takže xRz, což dokazuje, že R je tranzitivní, a tedy ekvivalence v $\mathbf{Z}$.

Zbývá tedy ověřit vlastnost (7). Zvolme proto libovolně $x_1, x_2, y_1, y_2 \in \mathbf{Z}$ a nechť

$$x_1 R x_2 \wedge y_1 R y_2,$$

neboli nechť existují $k, m \in \mathbf{Z}$ tak, že

$$x_1 = x_2 + 4k \wedge y_1 = y_2 + 4m.$$

Potom

$$x_1 y_1 = (x_2 + 4k)(y_2 + 4m) = x_2 y_2 + 4(m x_2 + k y_2 + 4km),$$

takže skutečně $x_1 y_1 R x_2 y_2$.

Rozklad $\mathbf{Z}/R$ zřejmě obsahuje tyto třídy:

$$\square R0 = \{\ldots, -4, 0, 4, 8, 12, \ldots\} = \bar{0}$$
$$\square R1 = \{\ldots, -3, 1, 5, 9, 13, \ldots\} = \bar{1}$$
$$\square R2 = \{\ldots, -2, 2, 6, 10, 14, \ldots\} = \bar{2}$$
$$\square R3 = \{\ldots, -1, 3, 7, 11, 15, \ldots\} = \bar{3}$$

Tedy faktorová grupa $\mathbf{Z}/R$ je řádu 4. Snadno přepočteme, že její operace je popsána touto tabulkou:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Čtenář si jistě povšiml, že grupu $(\mathbf{Z}/R, +)$ bychom mohli též získat jako faktorovou grupu grupy $(\mathbf{Z}, +)$ podle podgrupy N generované číslem 4 (viz příklad 5). Tato skutečnost není náhodná. Dokážeme, že u grup dojdeme k témuž výsledku, ať uvažujeme faktorové grupy podle nějaké normální podgrupy, či podle vhodné kongruence.

Věta 3. *Nechť* $(G, \cdot)$ *je grupa,* R *kongruence na* G. *Potom existuje normální podgrupa* N *v* G *tak, že* $(G/R, \cdot) = (G/N, \cdot)$.

Důkaz. Nechť jsou splněny předpoklady věty. Definujeme

$$N = \{a \in G;\ aRe\}, \tag{9}$$

kde e je neutrální prvek v G. Zřejmě $N \neq \emptyset$ (neboť $e \in N$) a $N \subseteq G$. Buďte $a, b \in N$; pak je aRe a zároveň bRe. Díky podmínce kongruence (7) je též $abRe$, a tedy $ab \in N$. Nechť $a \in N$, tj. aRe. Relace R je reflexívní, takže je $a^{-1}Ra^{-1}$. Podle (7) dostáváme

$$(aRe \wedge a^{-1}Ra^{-1}) \Rightarrow eRa^{-1}$$

a vzhledem k symetričnosti relace R též vztah $a^{-1}Re$, což znamená, že $a^{-1} \in N$.

Tedy $(N, \cdot)$ je podgrupou v G. Lehce ověříme, že N je normální podgrupa: buď $g \in G$, $x \in N$ libovolné; ukážeme, že platí $g \,.\, x \,.\, g^{-1} \in N$. Je xRe, neboť $x \in N$, a poněvadž gRg (R je reflexívní), dostáváme podle (7) $gxRg$. Dále platí (díky (7))

$$(gxRg \wedge g^{-1}Rg^{-1}) \Rightarrow gxg^{-1}Re,$$

odkud ihned plyne (viz definice N) hledaný vztah $g \,.\, x \,.\, g^{-1} \in N$.

Zbývá ověřit rovnost $G/R = G/N$. Nejprve dokážeme inkluzi $G/R \subseteq G/N$. Nechť tedy A je libovolný prvek z rozkladu $G/R = \{\Box Rx\}_{x\in G}$; pak existuje $x_1 \in G$ tak, že $A = \Box Rx_1$. Máme dokázat, že

$$A \in G/N = \{gN\}_{g\in G},$$

tj. že existuje $g_1 \in G$, pro něž $A = g_1 N$. Položme $g_1 = x_1$. Pak pro libovolný prvek $t \in A$ platí tRx_1 neboli tRg_1 a protože $g_1^{-1}Rg_1^{-1}$ (neboť R je reflexívní), dostáváme podle (7) $g_1^{-1}tRe$. Tedy podle definice množiny N je $g_1^{-1}t \in N$, takže $t \in g_1N$. Je tudíž $A \subseteq g_1N$. Jestliže naopak u je libovolný prvek z g_1N, je $g_1^{-1}u \in N$, neboli $g_1^{-1}uRe$. Protože R je kongruence, platí také uRg_1, což znamená

$$u \in \Box Rg_1 = \Box Rx_1 = A.$$

Tedy dohromady $A = g_1N$, takže $A \in G/N$ a inkluze $G/R \subseteq G/N$ je dokázána.

Důkaz obrácené inkluze $G/N \subseteq G/R$ je obdobný a přenecháváme jej čtenáři.

Věta 4. *Nechť $(G, \cdot)$ je grupa, N normální podgrupa v G. Pak existuje kongruence R v G taková, že $(G/R, \cdot) = (G/N, \cdot)$.*

Důkaz. Nechť jsou splněny předpoklady tvrzení. Budeme definovat relaci R na G takto:

$$(\forall a, b \in G)\ aRb \Leftrightarrow a\,.\,b^{-1} \in N \tag{10}$$

Relace R je reflexívní, neboť pro každé $a \in G$ je $a\,.\,a^{-1} = e \in N$. Buďte $a, b \in G$ takové, že aRb, tj. $a\,.\,b^{-1} \in N$. Poněvadž N je grupa, platí $(a\,.\,b^{-1})^{-1} = b\,.\,a^{-1} \in N$, a tedy bRa. Jestliže a, b, c jsou takové prvky z G, že aRb a zároveň bRc, dostáváme (podle (10)) $ab^{-1} \in N$ a současně $bc^{-1} \in N$. Tedy $a\,.\,b^{-1}\,.\,b\,.\,c^{-1} = ac^{-1} \in N$, a proto aRc. Tím jsme dokázali, že R je ekvivalence.

Ještě ověříme podmínku (7): Nechť a_1, a_2, b_1, b_2 jsou takové prvky z G, že platí $(a_1Ra_2 \wedge b_1Rb_2)$, tj. $(a_1a_2^{-1} \in N \wedge b_1b_2^{-1} \in N)$. Chceme dokázat, že $a_1b_1Ra_2b_2$ neboli $(a_1b_1)\,.\,(a_2b_2)^{-1} \in N$, což znamená $(a_1b_1)\,(b_2^{-1}a_2^{-1}) \in N$. Upravme si tento poslední výraz na tvar $a_1(b_1b_2^{-1})a_2^{-1}$. Protože $b_1b_2^{-1} \in N$, prvek $a_2^{-1} \in G$ a N je normální podgrupa, existuje (viz lemma 1, § 3) prvek $n_1 \in N$ tak, že $(b_1b_2^{-1})a_2^{-1} = a_2^{-1}n_1$. Potom lze psát $a_1(b_1\,.\,b_2^{-1})a_2^{-1} = a_1\,.\,a_2^{-1}\,.\,n_1$, což je zřejmě prvek z N.

K dokončení důkazu věty ještě zbývá ověřit rovnost rozkladů grupy G podle kongruence a normální podgrupy. Opět se omezíme na důkaz jedné z inkluzí, tentokrát (na rozdíl od důkazu předchozí věty) na inkluzi $G/N \subseteq G/R$.

Nechť tedy A je libovolný prvek, pro nějž platí

$$A \in G/N = \{gN\}_{g\in G},$$

pak existuje $g_1 \in G$ tak, že $A = g_1N$. Máme ukázat, že

$$A \in G/R = \{\Box Rx\}_{x\in G}$$

neboli, že existuje $x_1 \in G$, pro něž $A = \Box Rx_1$. Položíme $x_1 = g_1$ a ukážeme, že $A = g_1N = \Box Rg_1$. Nechť $t \in g_1N$, pak $g_1^{-1}t \in N$, takže $g_1^{-1}tRe$ a tedy tRg_1. To však znamená

$$t \in \Box Rg_1 = \Box Rx_1,$$

a proto je $A = g_1N \subseteq \Box Rx_1$. Je-li $u \in \Box Rx_1$, je také $x_1^{-1}uRe$ neboli $x_1^{-1}u \in N$. Potom však $u \in x_1N = g_1N = A$, takže $\Box Rx_1 \subseteq A$, což spolu s dokázaným již vztahem $A \subseteq \Box Rx_1$, dává $A = \Box Rx_1$. Tedy $A \in G/R$ a $G/N \subseteq G/R$ je dokázáno. Protože obrácená inkluze se ověří analogicky, můžeme tím větu 4 považovat za dokázanou.

Z definice kongruence je zřejmé, že k jejímu vyslovení nepotřebujeme žádné vlastnosti typické pro grupy. Můžeme tedy kongruenci R definovat (stejným způsobem) na libovolné struktuře $(G, *)$ s jednou binární operací.

Podmínka (7) zřejmě i v tomto obecnějším případě dává možnost definovat operaci na rozkladu G/R a tedy zavést pojem faktorové struktury $(G/R, *)$.

Pokud ovšem $(G, *)$ není grupa, nemusí platit tvrzení obdobné větě 3. Podstata důkazu této věty totiž spočívá v tom, že mezi třídami rozkladu G/R můžeme nalézt jednu „významnou" třídu, která je (normální) podgrupou; je jí ta třída, která obsahuje neutrální prvek grupy G. V obecném případě, například když struktura $(G, *)$ nemá vlastnost neutrálního prvku, jsou všechny prvky rozkladu G podle kongruence „rovnocenné", žádný z nich není „významný", a proto nelze nalézt vhodnou podstrukturu, která by hrála roli normální podgrupy.

Z tohoto hlediska kongruence poskytují obecnější přístup k zavedení pojmu faktorové struktury.

Cvičení

1. Ukažte, že každá podgrupa H, jejíž index v grupě G je 2, je normální podgrupa v G.
   [Uvědomte si, že jedna z tříd rozkladu G/H je H.]

2. Ukažte, že v grupě zákrytových pohybů pravidelného osmistěnu $(Z_8, \cdot)$ (viz § 1, příklad 8, z něhož přejímáme značení) platí
   a) podgrupy $\{E\}$, $\{A^2, B^2, C^2, E\}$, A_{12} a Z_8 jsou normální podgrupy v Z_8;
   b) podgrupa $\{AB^2, AC^2, A^2, E\}$ není normální v Z_8, ale je normální podgrupou v podgrupě A_8. [Využijte též cvičení 1.]
   c) Sestrojte rozklady grupy Z_8 na levé a pravé třídy podle podgrupy B_8.

3. Proveďte podrobně důkaz lemmatu 1.

4. Ukažte, že pro libovolnou grupu G a libovolnou její normální podgrupu N platí:
   $$\text{řád}\,(G/N) = \text{řád}\ G : \text{řád}\ N$$

5. Najděte několik kongruencí na grupě $(\mathbf{Z}, +)$ a popište příslušné faktorové grupy.

6. Dokažte tvrzení: Ekvivalence R na grupě $(G, \cdot)$ je kongruencí na G, právě když platí
$$(\forall a, b, c \in G) aRb \Rightarrow (acRbc \wedge caRcb).$$

§ 4. Homomorfní zobrazení grup

S pojmem homomorfního a izomorfního zobrazení grup i jiných algebraických struktur se čtenář již seznámil v kapitole II, § 4 a dále pak v kapitole III, § 2 a v kapitole IV, § 3. Zde si proto pouze připomeneme jeho definici, přičemž pro zjednodušení formulací budeme pro všechny uvažované struktury užívat multiplikativní zápis.

Definice. *Nechť $(G, \cdot)$ a $(G', \cdot)$ jsou libovolné algebraické struktury (s jednou binární operací). Řekneme, že $(G', \cdot)$ je homomorfním obrazem struktury $(G, \cdot)$, právě když existuje zobrazení φ množiny G na množinu G', které splňuje tzv. podmínku homomorfismu*

(1) $$(\forall x, y \in G) \varphi(x \,.\, y) = \varphi(x) \,.\, \varphi(y).$$

Zobrazení φ nazýváme homomorfní zobrazení (krátce homomorfismus) struktury $(G, \cdot)$ na strukturu $(G', \cdot)$.

Je-li φ navíc prosté zobrazení množiny G na množinu G', mluvíme o izomorfním zobrazení (izomorfismu) struktury $(G, \cdot)$ na strukturu $(G', \cdot)$.

Budeme se nejprve zajímat o to, které vlastnosti struktur se homomorfismem „přenášejí". Přesněji formulováno to znamená: je-li struktura $(G', \cdot)$ homomorfním obrazem struktury $(G, \cdot)$ s nějakou vlastností, kdy lze ukázat, že tutéž vlastnost má i struktura $(G', \cdot)$.

Z věty 2' z kapitoly II, § 4 vyplývá, že na homomorfní obraz se přenáší vlastnost existence neutrálního prvku (v G' je jím obraz neutrálního prvku struktury G) i existence inverzních prvků. Ukážeme, že lze přenést též asociativnost a další vlastnosti struktur.

Lemma 1. *Je-li $(G', \cdot)$ homomorfní obraz struktury $(G, \cdot)$ a je-li $(G, \cdot)$ asociativní, je rovněž struktura $(G', \cdot)$ asociativní.*

Důkaz. Příslušný homomorfismus G na G' označme φ a zvolme libovolné tři prvky $x', y', z' \in G'$. Protože φ je zobrazení G na G', existují prvky $x, y, z \in G$ tak, že platí
$$\varphi(x) = x', \quad \varphi(y) = y', \quad \varphi(z) = z'.$$

Užitím vlastnosti homomorfismu a asociativnosti struktury G snadno ukážeme, že platí
$$x'(y'z') = \varphi(x)\,(\varphi(y)\varphi(z)) = \varphi(x)\varphi(yz) = \varphi(x(yz)) =$$
$$= \varphi((xy)z) = \varphi(xy)\varphi(z) = (\varphi(x)\varphi(y))\varphi(z) = (x'y')z'.$$

Odtud již plyne asociativnost struktury $(G', \cdot)$.

Je vidět, že způsobem zcela obdobným důkazu lemmatu 1 lze pro $(G', \cdot)$ ověřit každou vlastnost struktury $(G, \cdot)$, kterou lze popsat jako rovnost mezi termy $\tau(x_1, \ldots, x_n)$, $\sigma(x_1, \ldots, x_n)$ struktury $(G, \cdot)$. Tuto skutečnost zapíšeme ve formě lemmatu.

Lemma 2. *Nechť struktura $(G', \cdot)$ je homomorfní obraz struktury $(G, \cdot)$ a nechť $(G, \cdot)$ má vlastnost, kterou lze popsat formulí*

(2) $$(\forall x_1, x_2, \ldots, x_n \in G) \tau(x_1, \ldots, x_n) = \sigma(x_1, \ldots, x_n),$$

kde τ a σ jsou termy struktury $(G, \cdot)$. Pak $(G', \cdot)$ má touž vlastnost.

Z dosud uvedených vlastností homomorfismu ihned vyplývá tato věta:

Věta 1. *Nechť $(G, \cdot)$ je grupa a struktura $(G', \cdot)$ její homomorfní obraz; pak $(G', \cdot)$ je rovněž grupa. Je-li $(G, \cdot)$ Abelova grupa, je Abelovou grupou i $(G', \cdot)$.*

V další části tohoto paragrafu budeme vyšetřovat souvislost mezi homomorfními zobrazeními grup a faktorovými grupami.

Věta 2. *Buď $(G, \cdot)$ grupa, N normální podgrupa v G. Pak faktorová grupa G/N je homomorfním obrazem grupy G.*

Důkaz. Nechť jsou splněny předpoklady věty. Vytvořme faktorovou grupu G/N a definujme zobrazení φ grupy G na G/N takto:
$$(\forall x \in G) \varphi(x) = xN.$$

Zobrazení φ je zřejmě zobrazením G na G/N. Rovněž ověření podmínky (1) je snadné: buďte $x, y \in G$, pak
$$\varphi(xy) = xyN = xyNN = xNyN = \varphi(x)\varphi(y),$$
takže φ je homomorfní zobrazení G na G/N.

Zdůrazněme, že věta 2 nám umožňuje sestrojit řadu různých konkrétních homomorfních zobrazení. Čtenář může k tomu účelu využít příklady z paragrafu 3.

Víme již, že když grupa $(G', \cdot)$ je homomorfním obrazem grupy $(G, \cdot)$, zobrazí příslušný homomorfismus φ neutrální prvek 1 grupy G na neutrální prvek $1'$ grupy G'. Poněvadž homomorfismus není obecně prosté zobrazení, může v G existovat více prvků, které φ zobrazí na $1'$. Množina všech takových prvků hraje při studiu homomorfních zobrazení důležitou roli, a proto pro ni zavedeme zvláštní název.

Definice. *Nechť φ je homomorfní zobrazení grupy $(G, \cdot)$ na grupu $(G', \cdot)$, jejíž neutrální prvek označíme $1'$. Jádrem homomorfismu φ — označíme ho J_φ — rozumíme množinu všech těch prvků z G, které se v zobrazení φ zobrazí na prvek $1'$, tj.*

$$J_\varphi = \{x \in G\,;\ \varphi(x) = 1'\}.$$

Příklad 1. Nechť G je libovolná grupa a φ homomorfní zobrazení grupy G na její faktorovou grupu G/N (viz věta 2). Pak jádro homomorfismu φ je totožné s normální podgrupou N: neutrálním prvkem v $(G/N, \cdot)$ je třída N a pro libovolný prvek $x \in G$ je zřejmě $\varphi(x) = xN$ rovno N, právě když $x \in N$.

Výsledek obsažený v tomto příkladě není náhodný, jak ukazuje následující tvrzení.

Lemma 3. *Nechť φ je homomorfní zobrazení grupy $(G, \cdot)$ na grupu $(G', \cdot)$. Pak jádro homomorfismu φ je normální podgrupa v G.*

Důkaz. Nechť je dán libovolný homomorfismus φ grupy G (s neutrálním prvkem 1) na grupu G' (jejíž neutrální prvek označíme $1'$).

Nejprve — podle věty 2 z § 1 této kapitoly — ukážeme, že množina J_φ je podgrupou v G. Zřejmě $J_\varphi \neq \emptyset$, neboť $1 \in J_\varphi$ $(\varphi(1) = 1')$. Dále pro libovolné prvky $x, y \in J_\varphi$ platí:

$$\varphi(x) = 1' \wedge \varphi(y) = 1'$$

a tedy, využijeme-li vlastností homomorfismu φ,

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)[\varphi(y)]^{-1} = 1' \,.\, (1')^{-1} = 1',$$

takže $xy^{-1} \in J_\varphi$.

Skutečnost, že jde o normální podgrupu, ověříme užitím podmínky (5') z paragrafu 2, která má v našem případě tvar

$$(\forall x \in J_\varphi)\,(\forall y \in G)\,yxy^{-1} \in J_\varphi.$$

Zvolme libovolné $y \in G$, $x \in J_\varphi$, takže $\varphi(x) = 1'$. Potom

$$\varphi(yxy^{-1}) = \varphi(y)\varphi(x)\varphi(y^{-1}) = \varphi(y) \,.\, 1' \,.\, [\varphi(y)]^{-1} = 1',$$

a proto $yxy^{-1} \in J_\varphi$. Tím je lemma 3 ověřeno.

Příklad 2. Označme $(W_1, +)$ aditivní grupu aritmetického vektorového prostoru $(\mathbf{R}^5, +, \mathbf{R})$ nad tělesem reálných čísel (viz kapitola III, § 1) a obdobně označme $(W_2, +)$ aditivní grupu vektorového prostoru $(\mathbf{R}^3, +, \mathbf{R})$. Ukážeme, že zobrazení φ definované předpisem

$$(\forall x_1, x_2, x_3, x_4, x_5 \in \mathbf{R})\varphi((x_1, x_2, x_3, x_4, x_5)) = (x_1, x_2, x_3)$$

je homomorfní zobrazení grupy W_1 na grupu W_2, a vyšetříme, co je jádrem tohoto homomorfismu. Pro libovolné vektory

$$\mathbf{x} = (x_1, x_2, x_3, x_4, x_5),\quad \mathbf{y} = (y_1, y_2, y_3, y_4, y_5) \in W_1$$

zřejmě platí

$$\begin{aligned}\varphi(\mathbf{x} + \mathbf{y}) &= \varphi((x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4, x_5 + y_5)) = \\ &= (x_1 + y_1, x_2 + y_2, x_3 + y_3) = (x_1, x_2, x_3) + (y_1, y_2, y_3) = \\ &= \varphi(\mathbf{x}) + \varphi(\mathbf{y}),\end{aligned}$$

takže φ je homomorfní zobrazení, neboť φ je evidentně zobrazení množiny W_1 na množinu W_2.

Neutrální prvky v grupách $(W_1, +)$ a $(W_2, +)$ jsou příslušné nulové vektory; označme je

$$\mathbf{0}_1 = (0, 0, 0, 0, 0),\quad \mathbf{0}_2 = (0, 0, 0).$$

Jádrem J_φ homomorfismu φ je pak množina všech vektorů z W_1 tvaru $(0, 0, 0, x_4, x_5)$, kde $x_4, x_5 \in \mathbf{R}$, neboť zřejmě pro libovolný vektor $\mathbf{x} = (x_1, x_2, x_3, x_4, x_5) \in W_1$ je

$$\mathbf{x} \in J_\varphi \Leftrightarrow \varphi(\mathbf{x}) = \mathbf{0}_2 \Leftrightarrow x_1 = x_2 = x_3 = 0.$$

Množina J_φ je vektorový podprostor prostoru $(\mathbf{R}^5, +, \mathbf{R})$, a tedy i podgrupa v grupě $(W_1, +)$. Protože W_1 je komutativní grupa, je J_φ (v souladu s lemmatem 3) normální podgrupa ve W_1.

Máme-li homomorfní zobrazení φ grupy $(G, \cdot)$ na grupu $(G', \cdot)$, které je izomorfismem, je zřejmě J_φ jednoprvková množina ($J_\varphi = \{1\}$, kde 1 je neutrální prvek grupy G). Toto tvrzení však lze i obrátit, jak ukazuje následující lemma.

Lemma 4. *Nechť φ je homomorfní zobrazení grupy $(G, \cdot)$ na grupu $(G', \cdot)$. Pak φ je izomorfní zobrazení, právě když J_φ je jednoprvková množina.*

Důkaz. Je-li dané zobrazení φ izomorfismus, je — jak jsme již uvedli — příslušné tvrzení zřejmé.

Nechť tedy dále φ je homomorfní zobrazení G na G', které není izomorfismus, tj. které není prosté. Existují tedy prvky $x, y \in G$ takové, že $x \neq y$ a $\varphi(x) = \varphi(y)$. Potom — označíme-li opět 1 a $1'$ neutrální prvky v G a G' — platí $xy^{-1} \neq 1$ a přitom

$$\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = \varphi(x)\,[\varphi(y)]^{-1} = \varphi(x)\,[\varphi(x)]^{-1} = 1',$$

takže J_φ vedle prvku 1 obsahuje ještě další prvek xy^{-1}, a není tedy jednoprvkovou množinou.

Právě ověřeného lemmatu 4 se často užívá k důkazu toho, že dvě grupy jsou izomorfní. Postupujeme tak, že najdeme homomorfní zobrazení jedné na druhou a pak ukážeme, že jádro tohoto homomorfismu je jednoprvková množina.

Příklad 3. Nechť $(\mathbf{Z}, +)$ je aditivní grupa celých čísel a $(S, +)$ grupa všech sudých čísel s obvyklým sčítáním. Zobrazení φ definované vztahem

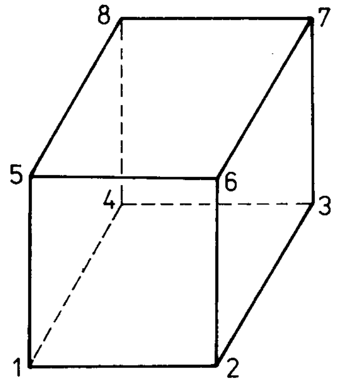
$$(\forall x \in \mathbf{Z})\varphi(x) = 2x$$

je zřejmě homomorfismus grupy $\mathbf{Z}$ na grupu S. Poněvadž evidentně $J_\varphi = \{0\}$ je jednoprvková množina, je φ izomorfním zobrazením $(\mathbf{Z}, +)$ na $(S, +)$.

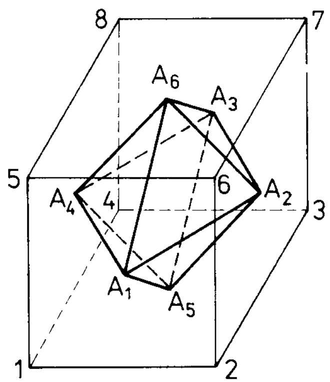
Příklad 4. Vytkněme si za cíl studovat (obdobně jako v příkladu 8 z § 1) grupu K všech zákrytových pohybů krychle. Označíme-li její vrcholy po řadě čísly 1, 2, ..., 8 (viz obr. 6), můžeme zákrytové pohyby krychle popsat permutacemi těchto čísel. Například otočení dané krychle o 90° kolem „svislé“ osy by bylo popsáno permutací

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix}.$$

Práci s vyšetřováním grupy zákrytových pohybů krychle si můžeme zjednodušit, uvědomíme-li si, že do dané krychle lze vepsat pravidelný osmistěn (viz obr. 7),



Obr. 6



Obr. 7

jehož vrcholy jsou označeny A_1, ..., A_6. Potom každému zákrytovému pohybu krychle odpovídá zákrytový pohyb s ní spojeného osmistěnu, který umíme popsat permutací indexů 1, 2, ..., 6 u označení jeho vrcholů, tj. prvkem grupy, kterou jsme v citovaném příkladu označili Z_8. Toto zobrazení množiny K na množinu Z_8 označme φ. Je tedy například:

$$\varphi\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{pmatrix}$$

$$\varphi\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 7 & 3 & 2 & 5 & 8 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 5 & 1 & 2 & 4 \end{pmatrix} \quad \text{atd.}$$

Je ihned zřejmé, že zobrazení φ musí splňovat podmínku (1), takže jde o homomorfismus. Přitom na neutrální prvek grupy Z_8 se — jak je ihned vidět — zobrazí pouze identická permutace

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

grupy K, takže jádro J_φ je jednoprvková množina a podle lemmatu 4 je φ izomorfismus. Není tedy třeba podrobně studovat grupu K, neboť je izomorfní s důkladně vyšetřenou grupou Z_8.

Doplněním věty 2 je následující věta, která v matematické literatuře bývá též nazývána větou o homomorfismu pro grupy.

Věta 3. *Buď grupa $(G', \cdot)$ homomorfním obrazem grupy $(G, \cdot)$. Pak existuje v G normální podgrupa N tak, že G/N je izomorfní s G'.*

Důkaz. Buď φ homomorfismus G na G'. Položme $N = J_\varphi$. Pak N je normální podgrupa — viz lemma 3 — a lze tedy vytvořit faktorovou grupu G/N.

Ukážeme, že předpis

$$(3) \qquad (\forall gN \in G/N)\psi(gN) = \varphi(g)$$

definuje izomorfní zobrazení G/N na G'.

Nejprve ověříme, že ψ je zobrazení: nechť $g_1N = g_2N \in G/N$; pak podle lemmatu 5 z § 2 je $g_2^{-1}g_1 \in N$, takže podle definice N je $\varphi(g_2^{-1}g_1) = 1'$ ($1'$ je jednotkový prvek grupy G'). Z vlastnosti homomorfismu φ ihned plyne $\varphi(g_1) = \varphi(g_2)$ neboli $\psi(g_1N) = \psi(g_2N)$.

Zvolme libovolný prvek $x \in G'$; protože φ je zobrazení G na G', existuje $y \in G$ tak, že $\varphi(y) = x$. Podle (3) pak $\psi(yN) = \varphi(y) = x$, takže ψ je zobrazení na G'.

Dále ukážeme, že ψ je prosté zobrazení: nechť xN, $yN \in G/N$ takové, že $\psi(xN) = \psi(yN)$, tj. $\varphi(x) = \varphi(y)$. Potom $[\varphi(y)]^{-1}\varphi(x) = 1'$ a s využitím toho, že φ je homomorfismus, dostáváme

$$\varphi(y^{-1}x) = \varphi(1),$$

což znamená $y^{-1}x \in N$, takže podle lemmatu 5 z § 2 $xN = yN$.

Platnost podmínky homomorfismu (1) pro zobrazení ψ vyplývá z této úvahy: jsou-li g_1N, g_2N libovolné prvky z G/N, je

$$\psi(g_1Ng_2N) = \psi(g_1g_2N) = \varphi(g_1g_2),$$

avšak φ je homomorfismus, a tedy

$$\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1N)\psi(g_2N).$$

Věta o homomorfismu je tím dokázána.

Vzhledem k tomu, co již bylo řečeno o souvislosti mezi normálními podgrupami a jádry homomorfismu, lze větu 3 formulovat též takto:

Věta 3'. *Buď φ homomorfismus grupy G na grupu G', J_φ jádro homomorfismu. Pak G/J_φ a G' jsou izomorfní struktury.*

Příklad 5. Buď $(V_2, +)$ množina všech vektorů v rovině s operací obvyklého sčítání vektorů; zřejmě jde o grupu. Nechť je dána dále grupa $(\mathbf{R}, +)$ všech reálných čísel. Definujme zobrazení φ grupy $(V_2, +)$ na $(\mathbf{R}, +)$ takto: $\varphi((a, b)) = a$. Snadno nahlédneme, že φ je homomorfismus. Podle věty 2 existuje ve V_2 normální podgrupa N a izomorfismus ψ struktury V_2/N na $\mathbf{R}$. Vytvořme N a ψ podle návodu v důkazu věty: je $N = \{(a, b) \in V_2;\ \varphi((a, b)) = 0\}$ — tj. N odpovídá v rovině osa y; $V_2/N = \{(a, b) + N\}_{(a, b) \in V_2}$ a $\psi((x, y) + N) = \varphi((x, y)) = x$.

Doporučujeme čtenáři, aby si podrobně promyslel „význam" V_2/N a ψ, popřípadě si nakreslil příslušný obrázek.

Příklad 6. Označme $(\mathbf{K}_0, \cdot)$ multiplikativní grupu všech nenulových komplexních čísel a vezměme zobrazení ψ, které libovolnému prvku $a + bi \in \mathbf{K}_0$ přiřadí číslo

$$\psi(a + bi) = |a + bi| = \sqrt{a^2 + b^2}.$$

Zřejmě ψ je zobrazení množiny $\mathbf{K}_0$ na množinu všech kladných reálných čísel $\mathbf{R}_0^+$. Díky známé vlastnosti absolutní hodnoty komplexních čísel

$$(\forall a + bi, c + di \in \mathbf{K}_0)\ |(a + bi) . (c + di)| = |a + bi| . |c + di|$$

je zobrazení ψ homomorfním zobrazením grupy $(\mathbf{K}_0, \cdot)$ na grupu $(\mathbf{R}_0^+, \cdot)$ (multiplikativní grupu kladných reálných čísel).

Protože neutrálním prvkem v grupě $(\mathbf{R}_0^+, \cdot)$ je číslo 1, je jádrem J_ψ tohoto homomorfismu množina všech těch komplexních čísel $a + bi$, pro něž platí

$$\psi(a + bi) = |a + bi| = 1,$$

tj. množina tzv. komplexních jednotek.

Cvičení

1. Nechť S_3 je grupa z příkladu 1 z § 3. Ukažte, že zobrazení φ definované předpisem

$$\varphi(i) = \varphi(a) = \varphi(b) = i,$$
$$\varphi(e) = \varphi(c) = \varphi(d) = e$$

je homomorfní zobrazení grupy S_3 na její podgrupu $\{i, e\}$.

2. Ukažte, že grupa $(G, \cdot)$, jejíž operace je dána tabulkou

$\cdot$	1	-1
1	1	-1
-1	-1	1

je homomorfním obrazem multiplikativní grupy tělesa reálných čísel $(\mathbf{R} - \{0\}, \cdot)$.

3. Nechť M je množina všech regulárních matic tvaru

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \text{ kde } a, b, c, d \in \mathbf{R}.$$

Ukažte, že struktura $(M, \cdot)$, kde „·" je operace násobení matic, je grupa a že zobrazení φ definované předpisem

$$\left(\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M\right)\ \varphi\begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc,$$

je homomorfní zobrazení $(M, \cdot)$ na grupu $(\mathbf{R} - \{0\}, \cdot)$.

4. Nechť grupa $(G', \cdot)$ je homomorfním obrazem grupy $(G, \cdot)$. Ukažte (užitím lemmatu 2), že platí

a) je-li $(G, \cdot)$ komutativní, je i $(G', \cdot)$ komutativní;

b) je-li $(G, \cdot)$ metakomutativní, má $(G', \cdot)$ touž vlastnost. Přitom vlastnost grupy $(G, \cdot)$ být metakomutativní lze definovat takto:

$$(\forall x, y, z \in G) xyx^{-1}y^{-1}z = zxyx^{-1}y^{-1}$$

(Všimněte si též, že tato podmínka je zobecněním komutativnosti.)

5. Promyslete si, že na grupu $(G, \cdot)$ se můžeme též dívat jako na strukturu se třemi operacemi: s jednou operací binární, jíž je grupové „násobení" „·", s jednou operací unární, totiž tvoření inverzního prvku — označíme ji „$^{-1}$" — a s jednou operací nulární, tj. zvolení neutrálního prvku — tuto operaci označíme stejně jako neutrální prvek, totiž „1" (definice operací četnosti jedna a nula viz kapitola II, § 1). Strukturu s těmito třemi operacemi označíme $(G, \cdot, ^{-1}, 1)$. Aby taková struktura byla grupou, musí platit

a) $(\forall x, y, z \in G)$ $\quad (x . y) . z = x . (y . z)$,

b) $(\forall x \in G)$ $\quad x . 1 = x$,

c) $(\forall x \in G)$ $\quad 1 . x = x$,