

# O grupách

---

6. kapitola. Rozdělení prvků grupy do tříd dle podgrupy. Homomorfní zobrazení, normální podgrupa, faktorová grupa. 1. a 2. věta o isomorfismu. Pojem jednoduché grupy

In: Ladislav Rieger (author): O grupách. (Czech). Praha: Mladá fronta, 1974, pp. 69–[100].

**Terms of use:**

© Institute of Mathematics of the Czech Academy of Sciences  
Persistent URL: <http://dml.cz/dmlcz/403817>

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://dml.cz>

**ROZDĚLENÍ PRVKŮ GRUPY DO TŘÍD  
DLE PODGRUPY.  
HOMOMORFNÍ ZOBRAZENÍ,  
NORMÁLNÍ PODGRUPA, FAKTOROVÁ GRUPA.  
1. A 2. VĚTA O ISOMORFISMU.  
POJEM JEDNODUCHÉ GRUPY**

Budiž  $G$  nějaká grupa a  $H$  nějaká její podgrupa. Vynásobme si libovolně zvoleným prvkem  $x$  grupy  $G$  postupně všechny prvky z podgrupy  $H$  zleva, tedy utvořme si všechny prvky tvaru  $x \cdot h$ , kde  $h$  probíhá celou podgrupu  $H$ . Souhrn těchto prvků si označíme jako  $x \cdot H$  a nazýváme jej *levou třídou prvku  $x$  podle podgrupy  $H$* .

Ukážeme si dva pozoruhodné fakty. Za prvé, pro prvky  $x_1$  a  $x_2$  jsou jen dvě možnosti: buďto obě třídy splývají (obsahují tytéž prvky grupy), anebo obě třídy nemají společné prvky. Jsou totiž jistě jen dva možné případy: buďto obě třídy  $x_1 H$  a  $x_2 H$  mají společný prvek, anebo společný prvek nemají. V prvním případě budiž  $x$  takový společný prvek. Potom je  $x = x_1 \cdot h_1 = x_2 \cdot h_2$  při vhodných prvcích  $h_1$  a  $h_2$  z podgrupy  $H$ . Libovolný prvek z levé třídy  $x_1 H$  má tvar  $x_1 \cdot h$ , kde  $h$  je prvek z podgrupy  $H$ . Dosazením z předchozího máme

$$x_1 \cdot h = x_2 \cdot h_2 \cdot h_1^{-1} \cdot h$$

Protože  $H$  je podgrupa, leží v ní s prvky  $h_1$ ,  $h_2$ ,  $h$  i součin  $h_2 \cdot h_1^{-1} \cdot h$ , takže libovolný prvek  $x_1 \cdot h$  z levé třídy prvku  $x_1$  patří do levé třídy prvku  $x_2$ . Právě tak dokážeme, že

i obráceně libovolný prvek z levé třídy prvku  $x_2$  patří do levé třídy prvku  $x_1$ . Je tedy v případě společného prvku opravdu dokázáno, že obě levé třídy splývají, čímž je náš prvý fakt prokázán.

Druhý fakt vyslovíme jen pro konečné grupy, ačkoli v příslušném zobecnění pojmu počtu prvků na nekonečné souhrny (viz pozn. 3) platí rovněž. Zní takto: všechny levé třídy dle téže podgrupy obsahují týž počet prvků grupy, tak veliký, kolik je prvků podgrupy.

Libovolná levá třída  $xH$  obsahuje jistě nejvýše tolik prvků grupy, tj. násobků prvky z podgrupy  $H$ , kolik je v  $H$  prvků. Avšak žádné dva různé prvky  $h_1$  a  $h_2$  z podgrupy  $H$  nemohou dát vynásobením týž prvek levé třídy, protože z  $x \cdot h_1 = x \cdot h_2$  by plynulo vynásobením prvkem  $x^{-1}$  zleva, že  $h_1 = h_2$ .

Oba poznatky spojeny tedy praví, že prvky grupy jsou každou její podgrupou rozděleny do jistého počtu „příhrádek“, to jest levých tříd podle dané podgrupy, při čemž počet prvků ve třídě je týž pro každou z nich. Mezi levými třídami ovšem vystupuje i podgrupa sama jakožto třída jednotkového prvku grupy. Z toho máme tento důsledek:

### Věta 5

*V každé konečné grupě je řád (tj. počet prvků) grupy násobkem řádu každé z jejích podgrup.*

Skutečně, řád podgrupy je tolikrát obsažen v řádu grupy, kolik je levých tříd dle této podgrupy. Výsledek dělení řádu grupy řádem podgrupy se nazývá *indexem* dané podgrupy.

Rozumí se, že podobné úvahy lze dělat právě tak pro podobně definované pravé třídy dle podgrupy, což si tu odпустíme.

Zvláště jednoduše tvořenými podgrupami, které nalézáme v každé grupě jsou tzv. *cyklické podgrupy*. Je-li  $G$  daná grupa a  $a$  její prvek, pak cyklická podgrupa je tvořena všemi mocninami prvku  $a$

$$\dots, a^{-2}, a^{-1}, a^0 = j, a^1, a^2, \dots$$

Jestliže grupa  $G$  je konečná, nemohou být ani mocniny

$$a = a^1, a^2, a^3, \dots$$

všechny různé, nýbrž musí být při jistém přirozeném mocniteli  $m$  větším než jiné přirozené  $k$   $a^m = a^k$ , čili  $a^{m-k} = j$ ; některé přirozené mocniny prvku  $a$  dávají jednotku (grupy)  $j$ . Nejmenší přirozený kladný mocnitel  $n$ , pro nějž je  $a^n = j$ , — existuje-li ovšem — je tzv. *řád prvku*. Je to zároveň i řád cyklické podgrupy, vytvořené prvkem  $a$ , protože prvky této cyklické podgrupy jsou mocniny  $a, a^2, a^3, \dots, a^{n-1}, a^n = j$  v počtu  $n$ . (Nepřekvapuje nás, že pak je třeba pro prvek  $a$  řádu 7

$$a^{-4} = a^3, a^9 = a^2)$$

Neexistuje-li takové  $n$ , aby  $a^n = j$ , pak říkáme, že prvek je nekonečného řádu. V tom případě jsou vesměs různé mocniny

$$\dots, a^{-3}, a^{-2}, a^{-1}, a^0 = j, a^1, a^2, a^3, \dots$$

a tvoří tzv. nekonečnou cyklickou grupu. Nekonečné cyklické grupy jsou zřejmě isomorfní s aditivní grupou všech celých čísel, totiž mocnitelů vytvářejícího prvku  $a$ . Berouce speciálně v úvahu cyklické podgrupy můžeme vyslovit tento *důsledek věty 5*:

*Řád prvku konečné grupy je dělitelem řádu grupy.*

Z tohoto tvrzení plyne tzv. malá Fermatova<sup>18)</sup> věta číselné teorie.

Malá Fermatova věta praví toto: Jestliže  $a$  je celé číslo nesoudělné s celým kladným číslem  $n$ , a jestliže označíme jako  $\varphi(n)$  počet celých kladných čísel menších než  $n$  a nesoudělných s  $n$  (krátce nesoudělných zbytků<sup>19)</sup>) — číslo 1 v to počítaje — potom mocnina  $a^{\varphi(n)}$  částečně vydělena číslem  $n$  zanechává zbytek 1. Krátce tvrzení vypisujeme symbolem

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

smluvivše si, že  $x \equiv y \pmod{n}$  (čti:  $x$  kongruentní s  $y$  modulo  $n$ ) znamená obecně, že rozdíl  $x - y$  je násobkem celého kladného čísla,  $n$  tzv. modulu ( $0 = 0 \cdot n$  je rovněž násobek čísla  $n$ ).  $\varphi$  je tzv. Eulerova<sup>20)</sup> funkce číselné teorie.

Odvození malé Fermatovy věty z našeho důsledku věty 5 bude ukázkou aplikace abstraktní poučky z teorie grup na konkrétním matematickém materiálu. Provedme je proto důkladně.

Běží vlastně pouze o vytčení vhodné grupy tak, aby téměř bezprostředním užitím našeho tvrzení (že totiž řád prvku konečné grupy je dělitelem řádu grupy) na tuto grupu vyplynula malá Fermatova věta. K tomu cíli musíme učinit dvě věci: předně vytknout, co budou

---

<sup>18)</sup> Fermat byl veliký francouzský matematik ze 17. stol., jeden ze zakladatelů novověké matematiky. (Pojem grupy ovšem ještě neznal.)

<sup>19)</sup>  $\varphi(1)$  definujeme rovno 1

<sup>20)</sup> L. Euler byl znamenitý německý matematik 18. stol., který prožil část života v Rusku v tehdejší Petrohradě (Leningradě).

prvky naší grupy, a za druhé určit pro ně grupové násobení.

Prvky naší grupy budou nikoli snad jednotlivá čísla, nýbrž jisté celé tzv. zbytkové třídy dle dělitele, tzv. modulu  $n$ , tj. budou to od sebe oddělené skupiny celých čísel a každá z těchto skupin bude obsahovat nekonečně mnoho celých čísel. Do jedné takové skupiny dáme všechna celá čísla, která dávají týž celý nezáporný zbytek při dělení modulem  $n$ . Jinými slovy, dvě celá čísla  $a$  a  $b$  patří do téže zbytkové třídy dle modulu  $n$ , což píšeme  $a \equiv b \pmod{n}$ , tehdy a jen tehdy, když rozdíl  $a - b$  je dělitelný modulem  $n$  (slovem dělitelný rozumí se vždy dělitelný beze zbytku); totéž platí ovšem i o rozdílu  $b - a = -(a - b)$ . (Např. pro  $n = 12$  patří  $5^4 = 625 = 52 \cdot 12 + 1$  do téže zbytkové třídy modulo 12 jako 1;  $-3 \equiv 9 \pmod{12}$  protože  $-3 - 9 = -12 = -1 \cdot 12$ .)

Zbytkovou třídu, do níž patří číslo  $a$ , vyznačujeme někdy pomocí pruhu nahoře, tedy jako  $\overline{a}$ , takže  $\overline{a} = \overline{b}$  značí, že zbytková třída čísla  $a$  je táž, jako zbytková třída čísla  $b$ ; chceme-li však přesněji vyznačit i modul  $n$ , dáme přednost způsobu psaní obvyklému v teorii čísel:

$$a \equiv b \pmod{n}$$

Je snadné nahlédnout, že všechna čísla celá se vlivem daného modulu  $n$  rozpadají do zbytkových tříd při čemž žádné číslo nepatří do dvou tříd současně a že tedy zbytkových tříd je právě tolik, kolik je nezáporných zbytků, které můžeme dostat při (částečném) dělení číslem  $n$ . Tyto třídy jsou tedy  $\overline{0}$ ,  $\overline{1}$ ,  $\overline{2}$ , ...,  $\overline{n-1}$ .

Ze zbytkových tříd si nyní vybereme za prvky naší grupy jen zbytkové třídy těch zbytků, které jsou s modulem  $n$  nesoudělné (mají za největšího společného

dělitele číslo 1). Počet takových zbytků a tedy takových příslušných zbytkových tříd je  $\varphi(n)$ , pro  $n = 12$  např.  $\varphi(12) = 4$ . Zde je třeba si uvědomit dvojí věc. Předně zbytek 0 není nesoudělný (= je soudělný) s číslem  $n$ , neboť  $0 = n \cdot 0$  a  $n = n \cdot 1$ , tedy čísla 0 a  $n$  mají za největší společný násobek číslo  $n$ , čili třída  $\bar{0}$ , tj. třída všech násobků modulu  $n$  do naší grupy nepatří zatím co třída  $\bar{1}$  samozřejmě do naší grupy patří. Za druhé, jestliže číslo  $a$  zanechává celý nezáporný zbytek  $r_a$  (při dělení modulem  $n$ ) nesoudělný s  $n$ , pak i samo číslo  $a$  je s  $n$  nesoudělné. Takové číslo lze totiž vyjádřit (částečným dělením) jako

$$a = q \cdot n + r_a$$

(kde číslo  $q$  je výsledek částečného dělení). Kdyby číslo  $a$  bylo dělitelno nějakým kladným dělitelem  $c$  modulu  $n$ , pak by tímto dělitelem  $c$  musel být dělitelný i rozdíl  $a - q \cdot n = r_a$  proti předpokladu. Ale právě tak i obráceně, jestliže číslo  $a$  je nesoudělné s modulem  $n$ , pak z právě naznačeného dělení čísla  $a$  modulem  $n$ , plyne nesoudělnost zbytku  $r_a$  s  $n$ , neboť jinak by i  $a$  bylo soudělné s  $n$ . Můžeme tedy prostě říci, že prvky naší grupy budou zbytkové třídy takových celých čísel, která jsou nesoudělná s modulem  $n$  a že naše grupa obnáší  $\varphi(n)$  prvků.

Grupové násobení nyní zavedeme prostě takto: součinem  $\bar{a} \cdot \bar{b}$  dvou zbytkových tříd rozumíme tu zbytkovou třídu, do níž náleží (obyčejný) součin  $ab$ . Můžeme tedy definici našeho násobení tříd psát rovností

$$\bar{a} \cdot \bar{b} = \overline{ab}$$

Např. pro modul  $n = 12$  je  $\bar{5} \cdot \bar{7} = \overline{35} = \overline{11}$ , protože  $35 = 2 \cdot 12 + 11$ .

Jde již jen o to zjistit platnost grupových zákonů v naší, tzv. multiplikatívni modulu  $n$ .

Axiom (1) neomezenosti a jednoznačnosti bude splněn, jestliže předně — kvůli jednoznačnosti — výsledek násobení  $\overline{ab}$  třídy  $\bar{a}$  třídou  $\bar{b}$  bude týž, ať jej provedeme pomocí jakkoli zvolených čísel v té které zbytkové třídě. Věc tedy není nikterak samozřejmá, nýbrž máme ukázat, že jestliže  $a'$  patří do třídy  $\bar{a}$  a  $b'$  do třídy  $\bar{b}$ , potom součin  $a'b'$  patří do třídy  $\overline{ab}$ , čili že  $\overline{a'b'} = \overline{ab}$ . Skutečně, jestliže oba rozdíly  $a' - a$  a  $b' - b$  jsou dělitelné modulem  $n$ , pak i rozdíl

$$a'b' - ab = a'b' - a'b + a'b - ab = a'(b' - b) + b(a' - a)$$

je číslem dělitelným modulem  $n$  — jakožto součet dvou čísel jistě dělitelných číslem  $n$ .

Za druhé — kvůli neomezené proveditelnosti násobení musíme ukázat, že výsledek násobení dvou zbytkových tříd čísel nesoudělných s modulem  $n$  i součin těchto tříd (jak jsme si jej právě zavedli) je nejen vždy definován (což je již dostatečně zřejmo), ale že je to opět třída, do níž patří čísla nesoudělná s modulem. K tomu však stačí si uvědomit, že součin  $ab$  dvou čísel  $a$  a  $b$  obou nesoudělných s modulem  $n$  je opět číslo nesoudělné s  $n$ .

Axiom (2) asociativity je dán téměř bezprostředně pro naše násobení zbytkových tříd přenesením z asociativity násobení čísel samých. Neboť jsou-li  $a, b, c$  tři libovolná celá čísla, pak platí

$$\bar{a} \cdot (\bar{b} \cdot \bar{c}) = \bar{a} \cdot \overline{bc} = \overline{a(bc)} = \overline{(ab)c} = \overline{ab} \cdot \bar{c} = (\bar{a} \cdot \bar{b}) \cdot \bar{c}$$

Axiom (3) jednotkového prvku je splněn pro zbytkovou třídu  $\bar{1}$  (čísel, zanechávajících zbytek 1 při dělení modulem), jak ukáže následující úvaha: Nechť  $i = q \cdot n +$



+ 1 je číslo z třídy  $\bar{1}$  (tj.  $\bar{1} = \bar{i}$ ). Nechť dále libovolné celé číslo  $x$  je ze třídy  $\bar{x} = \bar{r}$  kde  $r$  je nejmenší celý nezáporný zbytek při dělení čísla  $x$  modulem  $n$ . Pak lze psát  $x = p \cdot n + r$  (kde  $p$  je výsledek částečného dělení čísla  $x$  modulem  $n$ ). Tedy

$$xi = ix = (pn + r)(qn + 1) = pqn^2 + n(p + rq) + r$$

takže součin  $xi = ix$  dává při dělení modulem  $n$  týž zbytek  $r$  jako číslo  $x$ . Lze tedy psát opravdu pro zbytkové třídy žádanou rovnost

$$\bar{x} \cdot \bar{1} = \bar{1} \cdot \bar{x} = \bar{x}$$

Konečně axiom (4) inverzního prvku si ověříme takto: Vypišme si jednotlivé nezáporné zbytky, nesoudělné s dělitelem  $n$

$$a_1 = 1, a_2, a_3, \dots, a_{\varphi(n)}$$

(Např. 1, 5, 7, 11 pro  $n = 12$ ,  $\varphi(n) = 4$ .)

Když jsme zvolili libovolné číslo celé  $a$ , máme ukázat, že lze vždy nalézt celé číslo  $x$  tak, aby jeho zbytková třída  $\bar{x}$  splňovala

$$\bar{x} \cdot \bar{a} = \bar{a} \cdot \bar{x} = \bar{1}$$

čili aby  $ax \equiv 1 \pmod{n}$ , to jest aby  $\bar{x} = \bar{a}^{-1}$ .

Vynásobme si proto po řadě naše nezáporné  $a$  s  $n$  nesoudělné zbytky s  $n$  nesoudělným číslem  $a$ , tj. utvořme čísla

$$aa_1 = a, aa_2, aa_3, \dots, aa_n$$

(Např. tedy třeba pro  $a = 7$ ,  $n = 12$  čísla 7, 35, 49, 77.)

Ukažme, že není možné, aby mezi těmito součiny ani jeden nedával po dělení číslem  $n$  zbytek 1. Protože již víme, že všechna čísla  $a, aa_1, \dots, aa_{\varphi(n)}$  dávají vesměs zbytky nesoudělné s dělitelem  $n$ , znamenala by taková

možnost (kterou vyloučit je naším okamžitým cílem) to, že alespoň dvě čísla, řekněme  $aa_h$  a  $aa_k$  (pro  $h \neq k$ ) z čísel  $aa_1, aa_2, \dots, aa_{\varphi(n)}$  by dávala tentýž nezáporný zbytek při dělení modulem  $n$ . Jinými slovy, rozdíl  $aa_h - aa_k = a(a_h - a_k)$  by bylo číslo dělitelné modulem  $n$ . Protože  $a$  je číslo s číslem  $n$  nesoudělné, musel by být rozdíl  $a_h - a_k$  dělitelný modulem  $n$ . To však právě není možné, protože  $a_k$  a  $a_h$  jsou čísla různá, nezáporná a menší než  $n$ .

Tedy aspoň jedno číslo  $aa_t$  (pro jedno z čísel  $t = 1, 2, \dots, n$ ) dá nezáporný zbytek 1 při dělení číslem  $n$ , takže pak lze položit  $x = a_t$  a je  $\bar{x} \cdot \bar{a} = \bar{a} \cdot \bar{x} = \bar{1}$ . (V našem příkladě mezi čísla 7, 35, 49, 77 nalézáme  $49 = 4 \cdot 12 + 1 \equiv 1 \pmod{12}$ , takže pro  $\bar{a} = 7$  zrovna náhodou  $\bar{a}^{-1} = \bar{7} = \bar{a}$ .)

Tím je tedy dokončen důkaz, že zbytkové třídy čísel nesoudělných s dělitelem = modulem  $n$  tvoří při vytčném násobení grupu řádu  $\varphi(n)$ , kde  $\varphi(n)$  je počet s číslem  $n$  nesoudělných zbytků, jaké mohou vzniknout při částečném dělení číslem  $n$ .

Tím jsme však již také u našeho konečného cíle, tj. u malé Fermatovy věty. Jestliže totiž  $m$  je řád zbytkové třídy  $\bar{a}$  (čísla  $a$  dle modulu  $n$ ) jakožto prvku naší grupy, pak jednak platí

$$\bar{a}^m = \bar{1}$$

čili obšírněji

$$a^m \equiv 1 \pmod{n}$$

Za druhé však řád  $m$  prvku  $\bar{a}$  naší grupy dělí řád  $\varphi(n)$  této grupy, tedy  $\varphi(n) = m \cdot q$ , kde  $q$  je celé kladné. Z toho ovšem plyne  $\bar{a}^{\varphi(n)} = \bar{a}^{mq} = (\bar{a}^m)^q = \bar{1}^q = \bar{1}$  čili opravdu

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Poznamenejme ještě, že multiplikativní grupy tříd celých čísel nesoudělných s modulem  $n$ , jichž jsme právě užili ke grupově teoretickému důkazu malé Fermatovy věty, dávají bohatství příkladů konečných Abelových grup. V našem příkladě pro  $n = 12$  to byla — až na isomorfii — nám známá Kleinova grupa čili grupa zákrytových pohybů obdélníka.

Rozumí se, že poslední úsudkový krok, který jsme učinili při důkazu malé Fermatovy věty lze učinit zcela stejně v libovolné konečné grupě. Tak dostáváme tzv. Fermatovu větu teorie grup, to jest tvrzení, že v grupě řádu  $N$  je  $N$ -tá mocnina libovolného prvku rovna jednotce grupy, tj.  $a^N = j$ , kde  $a$  je libovolně zvolený prvek,  $j$  je jednotka dané grupy.

— Uvedme ještě dva důsledky rozdělení konečné grupy na (levé) třídy dle podgrupy. Předtím však je vhodné upozornit, že mezi podgrupy dané grupy počítáme logicky důsledně i ty dvě, které se vyskytují vždy, totiž grupu samu a podgrupu, skládající se jen z jediného prvku, jednotky dané grupy. Těmto podgrupám říkáme triviální podgrupy. (Kdybychom je z podgrup vyloučili, zkomplikovali bychom nevhodně znění příslušných pouček spoustou výjimek.)

## Věta 6

*Grupa, která má jen triviální podgrupy je konečná cyklická grupa řádu prvočíselného. Obráceně, konečné grupy prvočíselného řádu mají jen triviální podgrupy.*

Důkaz je dán větou 5. Budiž totiž  $G$  nějaká grupa (konečná nebo nekonečná), o níž víme, že má jen triviální podgrupy. Zvolme v ní libovolný prvek různý od jednotky což lze učinit vždy kromě případu, že celá naše grupa  $G$  se skládá jen z jednotky. (V tom případě však

nemáme dále co dokazovat, jestliže považujeme i číslo 1 důsledně za prvočíslo, jakožto číslo nemající jiných kladných celých dělitelů kromě čísla 1 a sebe sama.)

Je-li tedy  $a \neq j$  prvek z grupy, pak jsou dvě možnosti:

1.  $a$  je řádu konečného  $n$  a vytváří tedy cyklickou podgrupu řádu  $n$ , což je slučitelné s předpokladem jen tehdy, jestliže se tato cyklická podgrupa shoduje s celou grupou, takže  $G$  je v tomto případě konečná cyklická grupa řádu  $n$ . Kdyby  $n$  bylo číslo složené,  $n = r \cdot s$ , kde  $r, s$  jsou nesoudělná čísla celá, kladná, různá od jednotky, pak by prvek  $a^r \neq j$  vytvářel cyklickou podgrupu řádu  $s$ , skládající se z mocnin  $a^r, a^{2r}, a^{3r}, \dots, a^{sr} = j$ , což předpoklad vylučuje. Tedy řád  $n = p$  naší grupy  $G$  pouze s triviálními podgrupami, která se ukázala být cyklickou konečnou grupou, je prvočíslo  $p$ .

2. možnost:  $a$  vytváří v  $G$  nekonečnou cyklickou podgrupu

$$\dots, a^{-2}, a^{-1}, j, a^1, a^2, \dots$$

Potom však prvek  $a^2$  vytváří v  $G$  netriviální cyklickou podgrupu, takže možnost 2 dle předpokladu odpadá.

Obrácené tvrzení, že grupy prvočíselného řádu nemají netriviální podgrupy, je bezprostředním důsledkem věty 5.

Věta 6 je jednoduchým příkladem na úplné určení typu isomorfie grupy předpokladem o řádu.

### Věta 7

*K tomu, aby část prvků konečné grupy tvořila podgrupu, stačí (a ovšem je i nutno), aby taková část obsahovala s každými dvěma prvky i jejich součin.*

Důkaz: Předně dle předpokladu s prvkem  $a$  obsahuje předpokládaná část prvků grupy i mocninu  $a^N$ , kde

$N$  je řád grupy; ta je však dle zmíněné tzv. Fermatovy věty teorie grup rovna jednotce.

Za druhé, je-li v naší části prvků grupy nějaký prvek  $x$  řádu  $n$ , pak dle předpokladu je tam i prvek  $x^{n-1} = x^{-1}$ . Více však k důkazu nepotřebujeme. — Je důležité si povšimnout nezbytnosti předpokladu konečnosti grupy: bez něho můžeme narazit na prvky nekonečného řádu a náš úsudek padá. V tom případě je nutno a stačí ještě dokázat přítomnost inverzního prvku ke každému prvku v naší části, jež má být podgrupou, neboť přítomnost jednotky je již důsledkem.

Obraťme se k zásadně důležitému pojmu tzv. homomorfního zobrazení jedné grupy na druhou grupu.

Tento pojem je rozšířením nám již známého pojmu isomorfního zobrazení. Isomorfní zobrazení jedné grupy na druhou grupu věrně zachovává všechny grupové vlastnosti zobrazované grupy (originální), přenášejíc je dokonale na grupu obrazovou (na níž se zobrazuje originální grupa). V hrubém přirovnání je to tak, jako když znázorňujeme řecké součást stroje školním modelem, který je sice z jiného materiálu (a popř. menších rozměrů), ale jehož tvar je přesně shodný s tvarem originálu.

Pro mnohé účely však stačí zmíněnou součást stroje kolmo *promítnout* na jednu průmětnu, to jest zobrazit útvar prostorový na útvar rovinný. Tím ovšem některé prostorové vlastnosti zanedbáme (nevystihneme), neboť různé body originálu se promítnou do jediného bodového obrazu v průmětně (celé hrany, kolmé k průmětně se zobrazí vždy jediným bodem). Zato však bývá průmět jednodušší a přehlednější než model a často dovoluje snadno nahlédnout (na výkrese) polohu promítané součásti ve stroji a její souvislost s ostatními částmi.

Abstraktní obdobu toho máme v teorii grup (a i v ostatních partiích abstraktní algebry): pojem vzájemně jednoznačného, isomorfního zobrazování jedné grupy na druhou rozšiřujeme v pojem homomorfního zobrazení jedné grupy na druhou. Zde tedy již i více prvků zobrazované originální grupy se může zobrazit na jeden jediný prvek grupy obrazové, při čemž se ovšem nadále součin dvou prvků zobrazované grupy zobrazí součinem příslušných obrazů. Homomorfní obraz grupy je tedy již obecně grupa, která podržuje jen některé grupové vlastnosti zobrazované grupy, neboť ostatní vlastnosti se při homomorfním zobrazování mohou porušit.

Uvedme si alespoň dva příklady homomorfního zobrazení (které nejsou isomorfními zobrazeními); je třeba si uvědomit, že isomorfní zobrazení se jeví zvláštním případem homomorfního zobrazení, kde *mohou*, ale *nemusí*, existovat dva a víc prvků majících týž obraz.

1. V prvním příkladě bude zobrazovanou grupou známá symetrická grupa  $S_n$  všech permutací stupně  $n$  (z  $n$  předmětů). Přitom si zavedeme několik pojmů, které budeme potřebovat i později.

Říkáme, že permutace  $\pi$  provedená na  $n$  čísel  $1, 2, \dots, n$  je sudá anebo lichá podle toho, zda v pořadí čísel  $\pi(1), \pi(2), \dots, \pi(n)$  došlo k sudému či lichému počtu porušení přirozeného sledu dvou čísel, čili k sudému, či lichému počtu inverzí. Např. v permutaci  $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$  číslo 3 předešlo jednak 1 a jednak 2, 4 předešlo 2, máme tedy tři inverze a permutace  $\pi$  je lichá. Permutace  $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}$  je sudá, protože má celkem 8 inverzí.

Přiřadíme libovolně zvolené permutaci  $\pi$  stupně  $n$ , jakožto prvku symetrické grupy  $S_n$ , číslo  $+1$  anebo  $-1$

podle toho, je-li tato permutace sudá či lichá. Takto přiřazené číslo  $k$  permutaci  $\pi$  označme jako  $\varepsilon(\pi)$ . Ukažme, že tím definované zobrazení je homomorfním zobrazením grupy  $S_n$  na (multiplikativní) grupu čísel  $+1$  a  $-1$ , což je zřejmě cyklická grupa řádu 2. K tomu účelu vystihneme číslo  $\varepsilon(\pi)$  (k dané permutaci  $\pi$ ) takto: Znásobme si všechny rozdíly  $\pi(h) - \pi(k)$ , kde  $h > k$ . Pak součin (o zřejmém počtu  $(n-1) + (n-2) + \dots + 1 = \frac{(n-1) \cdot n}{2}$

činitelů) bude mít tolik záporných činitelů, kolikrát došlo k inverzi při permutaci  $\pi$ , tedy to bude číslo kladné pro permutaci sudou a záporné pro permutaci lichou. Dělíme-li ještě tento součin jeho absolutní hodnotou, to jest součinem všech rozdílů  $h - k$ , kde  $h, k = 1, 2, 3, \dots, n$  a  $h > k$ , obdržíme právě číslo  $\varepsilon(\pi)$ . Krátce to lze vyjádřit formulkou

$$\varepsilon(\pi) = \prod_{h>k} \frac{\pi(h) - \pi(k)}{h - k},$$

kterou čteme:  $\varepsilon(\pi)$  je součin přes všechna čísla

$$\frac{\pi(h) - \pi(k)}{h - k},$$

která lze utvořit, probíhají-li  $h$  i  $k$  všechna čísla od 1 do  $n$ , za podmínky, že  $h$  je větší než  $k$ .

Tato, zdánlivě neužitečně složitá formule (vzhledem k tomu, že  $\varepsilon(\pi) = \pm 1$ ) dovoluje nejúsporněji dokázat, že  $\varepsilon(\pi)$  dává skutečně homomorfní zobrazení grupy  $S_n$  na grupu  $(+1, -1)$ . Protože zřejmě existují jak permutace sudé, tak i liché každého stupně  $n > 1$ , takže jak čísla  $+1$ , tak i čísla  $-1$  opravdu bude jako obrazů permutací vždy použito, jde jen o to dokázat, že součin permutací

se zobrazuje vždy součinem číselných obrazů jednotlivých násobených permutací, to jest, že platí

$$\varepsilon(\rho\pi) = (\varepsilon)\rho \cdot \varepsilon(\pi)$$

Skutečně, pišme číslo  $\varepsilon(\rho\pi) = \prod_{h>k} \frac{\rho\pi(h) - \rho\pi(k)}{h - k}$  po rozšíření jednotlivých zlomkových činitelů jako číslo

$$\prod_{h>k} \frac{\rho\pi(h) - \rho\pi(k)}{\pi(h) - \pi(k)} \cdot \frac{\pi(h) - \pi(k)}{h - k}$$

Znásobme si první zlomky zvlášť a druhé také zvlášť. Dostaneme tak

$$\varepsilon(\rho\pi) = \prod_{h>k} \frac{\rho(\pi(h)) - \rho(\pi(k))}{\pi(h) - \pi(k)} \cdot \prod_{h>k} \frac{\pi(h) - \pi(k)}{h - k}$$

Zde druhý součin je již číslo  $\varepsilon(\pi)$ . První součin však není nic jiného, než číslo  $\varepsilon(\rho)$ . Neboť probíhají-li  $h, k$  čísla  $1, 2, \dots, n$ , pak i  $\pi(h)$  a  $\pi(k)$  probíhají (obecně v jiném pořadí) tato čísla, takže i rozdíly  $\pi(h) - \pi(k)$  proběhnou — až snad na znaménko — všechny kladné rozdíly různých dvou čísel, utvořené z čísel  $1, 2, \dots, n$ . Stane-li se však, že rozdíl  $\pi(h) - \pi(k)$  je záporný (zatím co jsme předpokládali ve jmenovateli rozdíl kladný), pak to nevádí, neboť lze psát v takovém případě

$$\frac{\rho(\pi(h)) - \rho(\pi(k))}{\pi(h) - \pi(k)} = \frac{\rho(\pi(k)) - \rho(\pi(h))}{\pi(k) - \pi(h)}$$

kde  $\pi(k) - \pi(h)$  je kladný rozdíl. Je tedy jedno, zda v prvním součinu násobíme přes všechny indexy  $h, k$  anebo přes odpovídající indexy  $\pi(h), \pi(k)$ , takže první součin opravdu je vlastně  $\varepsilon(\rho)$ . Máme tedy skutečně rov-



nost  $\varepsilon(\rho\pi) = \varepsilon(\rho) \varepsilon(\pi)$  čili zobrazení  $\varepsilon$  je vskutku homomorfním zobrazením.

Je jasné, že zde homomorfní obraz, tj. cyklická grupa řádu 2, je hrubý a vystihuje symetrickou grupu permutací velmi málo.<sup>21)</sup>

2. V druhém příkladě bude homomorfní obraz věrnější.

Budiž  $K$  (ze školy v podstatě známá) multiplikativní grupa komplexních čísel různých od nuly, vzhledem k násobení, danému rovností

$$(x_1 + i \cdot y_1) (x_2 + i \cdot y_2) = (x_1 x_2 - y_1 y_2) + \\ + i \cdot (x_1 y_2 + x_2 y_1)$$

(kde  $i$  je známá komplexní imaginární jednotka).

Zobrazme grupu  $K$  do multiplikativní grupy  $R$  všech reálných čísel kladných tím, že přiřadíme komplexnímu číslu  $x + iy$  jeho tzv. absolutní hodnotu  $\sqrt{x^2 + y^2}$ . Pak zobrazení

$$f(x + i \cdot y) = \sqrt{x^2 + y^2}$$

je homomorfním zobrazením grupy  $K$  na grupu  $R$ .

Neboť opravdu, jednak každé komplexní číslo různé od nuly má jedinou kladnou absolutní hodnotu a každé reálné číslo je absolutní hodnotou komplexního čísla. A za druhé, absolutní hodnota součinu rovná se součinu absolutních hodnot jednotlivých komplexních činitelů, jak si čtenář ihned ověří na identitě

$$(x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + x_2 y_1)^2 = (x_1^2 + y_1^2) (x_2^2 + y_2^2)$$

---

<sup>21)</sup> Říká jen, že sudá kráté sudá a lichá kráté lichá permutace je sudá, lichá kráté sudá a sudá kráté lichá permutace je lichá permutace.

Nyní je již na místě přesná abstraktní definice.

## Definice

Budtež  $G$  a  $H$  dvě grupy.

Říkáme, že grupa  $G$  je zobrazením  $f$  homomorfně zobrazena na grupu  $H$ , jestliže ke každému prvku  $x$  grupy  $G$  je zobrazením  $f$  přiřazen přesně jeden prvek  $y = f(x)$  z grupy  $H$  tak, že jsou splněny tyto podmínky:

(i) Každý prvek  $y$  z grupy  $H$  splňuje vztah  $y = f(x)$  alespoň pro jeden prvek  $x$  z grupy  $G$ . Slovy: Každý prvek grupy  $H$  je obrazem nějakého prvku, tzv. originálu neboli vzoru, z grupy  $G$ .

(ii) Pro libovolné prvky  $x_1$  a  $x_2$  z grupy  $G$  platí

$$f(x_1 x_2) = f(x_1) \cdot f(x_2)$$

(jestliže tečkou  $\cdot$  odlišujeme grupové násobení v  $H$  od grupového násobení v  $G$ , jež zvláště nevyznačujeme). Slovy: Obraz součinu se rovná součinu obrazů.

Říkáme též, že grupa  $H$  je (jako celek) homomorfním obrazem grupy  $G$  (při zobrazení  $f$ ). Možnost takového homomorfního zobrazení značíme symbolem

$$H \sim G$$

Uvědomíme si několik bezprostředních důsledků této definice. Každou grupu lze homomorfně zobrazit na grupu, skládající se jedině z jednotkového prvku; obrazem každého prvku je pak tento jediný (jednotkový) prvek. Takové zobrazení ovšem není příliš užitečné, protože naprosto deformuje zobrazovanou grupu.

Homomorfní zobrazení dává inverznímu prvku za obraz inverzní prvek k obrazu,  $f(x^{-1}) = f(x)^{-1}$ , a jednotce  $j_G$  zobrazované grupy  $G$  přiřazuje jako obraz jednotku  $j_H$  grupy obrazů,  $f(j_G) = j_H$ .

Neboť  $f(j_G) = f(j_G j_G) = f(j_G) \cdot f(j_G)$ , z čehož druhý fakt plyne vynásobením prvkem  $f(j_G)^{-1}$ . První fakt pak již vyplývá z rovností

$$f(x^{-1}) \cdot f(x) = f(x^{-1}x) = f(j_G) = j_H$$

Nyní již není třeba zvláště podrobně vysvětlovat, co je to homomorfní reprezentace dané grupy grupou permutací anebo grupou matic. Je to přirozené a důležité rozšíření pojmu isomorfní reprezentace, s nímž jsme se již seznámili. Je zajímavé, že homomorfní reprezentace grupy (grupami permutací, nebo grupami matic) jakožto jakési „promítání“ (při čemž za jednotlivé „průmětny“ slouží symetrické grupy permutací stupně  $n$ , po případě grupy veškerých regulárních matic stupně  $n$ ) prohlubuje zmíněnou obdobu s promítáním tělesa na dvě kolmé průmětny. I tu lze totiž úplně rekonstruovat původní grupu z jejich „průmětů“, tj. homomorfních reprezentací (podobně jako si těleso zrekonstruujeme z jeho nárysu a půdorysu), jestliže známe tzv. úplný systém homomorfních reprezentací<sup>22)</sup> dané grupy, z něhož lze sestavit isomorfní obraz dané grupy. Vedlo by nás příliš daleko, kdybychom měli na to podat příklady; čtenář, který se odhodlá k hlubšímu studiu teorie grup, je nalezne v obšírnějších učebnicích teorie grup.

Obrátíme se k dalšímu důležitému pojmu abstraktní teorie grup, který úzce souvisí s pojmem homomorfního zobrazení; je to již zmíněný pojem normální podgrupy, k němuž můžeme dospět takto:

Při každém homomorfním zobrazení  $f$  grupy  $G$  na grupu  $H$  nalézáme následující rozdělení prvků grupy  $G$

---

<sup>22)</sup> Úplným nazýváme takový systém homomorfních reprezentací, v němž každý nikoli jednotkový originál obdrží alespoň jednou nikoli jednotkový obraz.

do tříd bez společných prvků: Každá taková třída sestává ze všech prvků  $x$  z grupy  $G$ , které mají týž obraz

$$y = f(x)$$

Tak v prvním předchozím příkladě se symetrická grupa  $S_n$  (všech permutací stupně  $n$ ) rozbíjí homomorfním zobrazením  $f = \varepsilon$  (na cyklickou multiplikatívni grupu z čísel  $\pm 1$ ) ve dvě třídy, třídu sudých a třídu lichých permutací. V druhém předchozím příkladě se multiplikatívni grupa všech od nuly různých komplexních čísel, znázorněných body komplexní roviny (mimo počátek) rozbíjí ve třídy čísel, znázorněných body na téže kružnici opsané okolo počátku.

Dále zjišťujeme, že třída všech originálů k jednotkovému prvku  $j_H$  — to jest třída všech  $x$  z  $G$ , pro něž  $f(x) = j_H$  — tvoří podgrupu grupy  $G$ . — Neboť předně jestliže  $x_1$  i  $x_2$  jsou originály jednotky,  $f(x_1) = j_H$ ,  $f(x_2) = j_H$ , potom i  $f(x_1 x_2) = f(x_1) \cdot f(x_2) = j_H \cdot j_H = j_H$ , to jest pak i součin  $x_1 x_2$  je originálem jednotky  $j_H$  v  $H$ . [To nám v případě konečné grupy již stačí (viz větu 7)]. Snadno se předveddíme, že i ostatní podmínky, aby souhrn originálů jednotky (v homomorfním zobrazení) byl podgrupou, jsou splněny, takže naše tvrzení platí obecně. Neboť je nám již známo, že v homomorfním zobrazení je obrazem jednotky jednotka a obrazem inverzního prvku je inverzní prvek k obrazu původního prvku. Podgrupu (grupy  $G$ ) originálů jednotky v našem homomorfním zobrazení grupy  $G$  na grupu  $H$  nazveme například  $N$ .

Vzniká přirozené podezření, zda ostatní třídy originálů se stejným obrazem (v homomorfním zobrazení) nejsou snad právě nám již známými levými třídami podle podgrupy  $N$  utvořenými v zobrazované grupě  $G$ . Toto podezření je oprávněné. Neboť jestliže  $x$  je daný

prvek v zobrazované grupě  $G$  a  $u$  je libovolný prvek z podgrupy  $N$ , potom součin  $xu$  má v grupě  $H$  za obraz prvek

$$f(xu) = f(x) \cdot f(u) = f(x) \cdot j_H = f(x)$$

tedy též jako  $x$ . Stejně tak ovšem i obráceně, je-li  $xu$  (při  $u$  ležícím v podgrupě  $N$ ) libovolný prvek levé třídy prvku  $x$ , pak jeho obraz  $f(xu)$  je roven obrazu  $f(x)$  libovolného prvku  $x$  z téže levé třídy v grupě  $G$  podle podgrupy  $N$ .

Utvoření tříd originálů se společným obrazem je tedy skutečně vlastně totéž co rozdělení prvků zobrazované grupy do levých tříd podle podgrupy, tvořené všemi originály jednotky. — Tím však celá věc zdaleka nekončí. Zjišťujeme totiž, že podgrupa  $N$  originálů jednotky se vyznačuje touto zvláštní vlastností: s každým prvkem  $x$  patří do  $N$  i každý prvek tvaru

$$zxz^{-1}$$

kde  $z$  je libovolný prvek ze zobrazované grupy  $G$ . Neboť jestliže je  $f(x) = j_H$ , pak následkem homomorfnosti zobrazení  $f$  je

$$f(zxz^{-1}) = f(z) \cdot f(x) \cdot f(z^{-1}) = f(z) \cdot j_H \cdot (f(z))^{-1} = j_H$$

Podgrupám s touto důležitou vlastností (nezávisle na jakémkoli homomorfním zobrazení  $f$ ) říkáme *normální podgrupy*.

## Definice

Podgrupa  $N$  grupy  $G$  se nazývá *normální podgrupou*, jestliže s každým prvkem  $x$  patřícím do  $N$  patří do  $N$  i každý prvek  $zxz^{-1}$ , tzv. konjugovaný prvek k prvku  $x$  pomocí (libovolného) prvku  $z$  z grupy  $G$ .

Tak např. ze dvou nám známých podgrup grupy eu-

klidovských pohybů roviny (př. 2 ve 4. kap.) je podgrupa čistých posuvů normální podgrupou, kdežto podgrupa čistých otočení normální podgrupou není. — To vyplývá snadno z okolnosti, že provedeme-li otočení, pak posuv a nakonec zpětné otočení, dostáváme celkem opět čistý posuv (obecně ovšem jiný). Naproti tomu jestliže provedeme posuv, pak otočení a nakonec zpětný posuv, nedostáváme nikdy (pokud jde o neidentické pohyby) čisté otočení, nýbrž smíšený pohyb.

V příkladě s permutacemi všechny sudé permutace v symetrické grupě  $S_n$  tvoří tzv. alternující grupu  $A_n$  stupně  $n$ , která je normální podgrupou v grupě  $S_n$ . — V každé Abelově (komutativní) grupě je ovšem zřejmé každá podgrupa normální. (Obrácené tvrzení neplatí, viz cvič. 7 z 5. kap.)<sup>23)</sup>.

Důležitost normálních podgrup v grupě vyplývá z toho, že pomocí nich lze z dané grupy tvořit potřebné nové grupy, jejímiž prvky se stávají celé (levé) třídy podle takové normální podgroupy. Násobení v takové grupě levých tříd dle normální podgroupy  $N$  grupy  $G$  je dáno takto: Jsou-li  $xN$  a  $yN$  dvě levé třídy (prvků  $x$  a  $y$  z  $G$ ), potom za jejich součin  $xN \cdot yN$  položíme tu levou třídu, která obsahuje součin  $xy$ , to jest klademe

$$xN \cdot yN = xyN$$

Dokažme, že axiomy grupy jsou pro toto násobení levých tříd splněny. K axiomu (1) máme vlastně jen zaručit, že výsledek násobení dvou tříd nezáleží na tom, jaké prvky si vybereme v jednotlivých třídách k vytvoření součinu tříd. To jest, máme ukázat, že jestliže

<sup>23)</sup> V grupě základních kvaternionů ze cvič. 7 z 5. kap. je každá podgrupa normální podgrupou, ačkoli grupa není Abelova.

$x' = xu_1$  a  $y' = yu_2$ , kde prvky  $u_1$  a  $u_2$  jsou z normální podgrupy  $N$ , potom součin  $x'y' = xu_1yu_2$  patří do levé třídy součinu  $xy$ .

Skutečně lze psát  $xu_1yu_2 = xyy^{-1}u_1yu_2$  a podle předpokladu normálnosti podgrupy  $N$  prvek  $y^{-1}u_1yu_2$  patří do  $N$ , což právě potřebujeme.

Ostatní axiomy si ověříme ještě snadněji.

Axiom (2) nyní již lze dokázat prostým přenesením z celé grupy  $G$  do naší grupy levých tříd (dle  $N$ ) rovnostmi

$$xyN \cdot zN = (xy)zN = x(yz)N = xN \cdot yzN$$

Axiom (3): úlohu jednotkového prvku v naší grupě tříd patrně bude hrát (následkem toho, jak jsme zaručili axiom (1) levá třída obsahující jednotku  $j_G$  grupy  $G$ , to jest sama normální podgrupa  $N$ .

Axiom (4): inverzním prvkem k prvku (tj. ke třídě)  $xN$  je patrně třída  $x^{-1}N$ , protože součin  $xN \cdot x^{-1}N$  stejně jako  $x^{-1}N \cdot xN$  obsahuje jednotku  $j_G$ .

Grupě levých tříd v grupě  $G$  dle normální podgrupy  $N$  říkáme faktorová grupa grupy  $G$  dle normální podgrupy  $N$  a značíme ji  $G/N$ ; normální podgrupě  $N$  se pak také někdy říká normální dělitel. Podle věty 5 je řád grupy  $G$  roven součinu řádu normální grupy  $N$  s řádem faktorové grupy  $G/N$ .

Jaký je zobrazovací vztah faktorové grupy  $G/N$  k původní grupě?

Odpověď je nasnadě: faktorová grupa  $G/N$  je homomorfním obrazem původní grupy  $G$  při zobrazení, přiřazujícím prostě prvku  $x$  z grupy  $G$  jeho levou třídu  $xN$  jakožto prvek z faktorové grupy  $G/N$ . Neboť to přímo říká definice  $xN \cdot yN = xyN$  násobení v  $G/N$ .

Vraťme se nyní k případu, že normální podgrupa  $N$  grupy  $G$  je souhrnem originálů jednotky v jakémsi homo-

morfním zobrazení  $f$  grupy  $G$  na grupu  $H$ . Jaký bude vztah faktorové grupy  $G/N$  ke grupě  $H$ ?

Snadno nahlédneme, že tyto grupy jsou isomorfní. Zobrazení zprostředkující tento isomorfismus přiřazuje prostě třídě  $xN$  obraz  $f(x)$ , který má prvek  $x$  z grupy  $G$  v grupě  $H$  při výchozím homomorfním zobrazení  $f$ . Neboť takové zobrazení faktorové grupy  $G/N$  na grupu  $H$  je zřejmě homomorfní a kromě toho vzájemně jednoznačné. Shrňme si tedy výsledek předchozích úvah do následující tzv. první věty o isomorfismu teorie grup.

### Věta 8

*Jakmile podgrupa  $N$  grupy  $G$  je normální podgrupou, pak levé třídy  $xN$  ( $x$  je z  $G$ ), do nichž se rozpadají prvky grupy  $G$ , tvoří tzv. faktorovou grupu  $G/N$  vzhledem k násobení  $xN \cdot yN = xyN$ . Faktorová grupa  $G/N$  je homomorfním obrazem grupy  $G$  při homomorfním zobrazení  $x \rightarrow xN$  přiřazujícím prvku  $x$  jeho levou třídu.*

*Je-li obráceně dána grupa  $H$ , která je homomorfním obrazem grupy  $G$  při zobrazení  $f$ , pak je tím určena normální podgrupa  $N$  všech originálů jednotky  $j_H$  grupy  $H$  tak, že faktorová grupa  $G/N$  je isomorfně zobrazena na grupu  $H$  zobrazením  $f$ , daným rovností*

$$f(xN) = f(x)$$

Uvedená 1. věta o isomorfismu teorie grup (tento dlouhý titul je nutný, protože podobné věty o isomorfismu vystupují i v jiných částech abstraktní algebry) udává prostou, ale důležitou souvislost pojmu homomorfního zobrazení s pojmem normální podgrupy. Ve shora uvedených dvou příkladech se projevuje takto:

Faktorová grupa  $S_n/A_n$  symetrické grupy stupně  $n$



podle její normální alternující podgrupy  $A_n$  je isomorfní s kteroukoli cyklickou grupou řádu 2, např. s podgrupou  $(+1, -1)$  multiplikatívni grupy všech zlomků.

Multiplikatívni grupa kladných reálných čísel je isomorfní s faktorovou grupou všech komplexních čísel různých od nuly dle (normální) podgrupy všech komplexních čísel o absolutní hodnotě 1.

Uvedme ještě jeden důležitý příklad na tvoření faktorové grupy. Za grupu  $G$  vezměme aditivní grupu všech celých čísel; podgrupa  $N$ , která bude následkem komutativity samozřejmě normální, budiž tvořena všemi násobky pevně zvoleného celého kladného čísla  $n$ . Levé třídy dle  $N$  jsou nyní nám již známé zbytkové třídy dle modulu  $n$ , každá obsahuje všechna celá čísla, jež jsou navzájem kongruentní modulo  $n$ , tj. jež dávají při dělení modulem  $n$  týž nezáporný nejmenší zbytek.

Faktorová grupa  $G/N$  je tzv. aditivní grupa modulo  $n$ . (Pozor, něco jiného byla tzv. multiplikatívni grupa modulo  $n$ , která se skládala jen ze zbytkových tříd, naplněných vesměs čísly, nesoudělnými s modulem, kdežto aditivní grupa modulo  $n$  obsahuje všechny zbytkové třídy.) Je-li  $H$  jakákoli cyklická grupa řádu  $n$ , např. multiplikatívni grupa všech  $n$ -tých odmocnin z 1, pak první věta o isomorfii nám zde říká, že aditivní grupa modulo  $n$  je isomorfní s touto cyklickou grupou.

Tvořením faktorové grupy z grupy  $G$  podle normální podgrupy  $N$  ztotožňujeme vlastně prvky, patřící do téže levé třídy dle  $N$  v  $G$ . Zanedbávající rozdílnosti mezi prvky téže levé třídy, počínáme si obrazně řečeno asi tak, jako bychom se na naši grupu dívali (z jisté strany) z přiměřeně veliké dálky, až nám prvky z téže levé třídy splývají. Takový pohled dle první věty o isomorfismu je rovnocenný s daným „promítnutím“ (tj. homomorfismem zobrazením) dané grupy na jinou grupu  $H$ .

Normální podgrupy mají i jiné charakteristické vlastnosti, jimiž je možno je definovat. Hlubavý čtenář se rád přesvědčí, že:

a) Podgrupa  $U$  je normální tehdy a jen tehdy, když každá levá třída  $xU$  je rovna pravé třídě  $Ux$  téhož prvku  $x$  (všech pravých násobků  $ux$  prvků  $u$  podgrupy  $U$  násobených zprava prvkem  $x$ ).

b) Podgrupa  $U$  je normální tehdy a jen tehdy, když souhrn  $xUyU$  všech součinů násobků  $xu_1$  s násobky  $yu_2$  (kde  $u_1$  a  $u_2$  jsou libovolné prvky z podgrupy  $U$  a  $x$  a  $y$  jsou pevně zvolené prvky grupy) je vždy jistá levá třída podle  $U$ .

Na konec tohoto paragrafu si odvodíme důležitou tzv. druhou větu o isomorfismu teorie grup. Je to pomocná věta významu teoretického, jejíž užití si ukážeme v 6. kap.

### Věta 9

*Budiž  $G$  grupa,  $N$  její normální podgrupa a  $U$  její další podgrupa. Pak platí:*

1. *Souhrn  $UN$  všech součinů  $un$  prvků  $u$  z podgrupy  $U$  s prvky  $n$  z normální podgrupy  $N$  je opět z podgrupa grupy  $G$ . (Takový souhrn  $UN$  je tzv. spojení podgrup  $U$  a  $N$ .)*

2. *Souhrn označený jako  $U \cap N$  všech prvků grupy z  $G$ , které leží současně v podgrupě  $U$  i v normální podgrupě  $N$ , je rovněž podgrupou, a to dokonce podgrupou v grupě  $U$ . (Takovému souhrnu  $U \cap N$  říkáme průnik podgrup  $U$  a  $N$ .)*

3. *(Vlastní tvrzení věty):*

*Podgrupa  $N$  je normální podgrupou v grupě  $UN$ , podgrupa  $U \cap N$  je normální podgrupou v grupě  $U$  a faktorové grupy  $UN/N$  a  $U/(U \cap N)$  jsou navzájem isomorfní.*

**Důkaz:** Nejprve k bodu 1:

Máme ukázat především, že součin dvou násobků tvaru  $u_1n_1$  a  $u_2n_2$ , kde  $u_1, u_2$  jsou libovolné prvky z podgrupy  $U$  a  $n_1, n_2$  jsou libovolné prvky z normální podgrupy  $N$  (vše v  $G$ ) je opět prvek tvaru  $un$ , kde  $u$  je z  $U$  a  $n$  je z  $N$ . Skutečně je

$$(u_1n_1)(u_2n_2) = u_1u_2(u_2^{-1}n_1(u_2^{-1})^{-1}n_2)$$

Protože  $N$  je normální podgrupa, leží v ní s prvky  $n_1$  a  $n_2$  též i prvek  $n = u_2^{-1}n_1(u_2^{-1})^{-1}n_2$ . Prvek  $u = u_1u_2$  pak leží v  $U$ , protože  $U$  je podgrupa obsahující  $u_1$  i  $u_2$ . Z rovností  $(u_1n_1)^{-1} = n_1^{-1}u_1^{-1} = u_1^{-1}(u_1n_1^{-1}u_1u^{-1})$  je pak již snadno patrné, že  $UN$  je vskutku podgrupou v  $G$ .

Dále k bodu 2:

Je-li  $x$  i  $y$  jak v  $U$  tak i v  $N$ , pak platí totéž i o součinu  $xy$ , protože  $U, N$  jsou podgrupy. Jednotkový prvek  $j_G$  je ovšem jak v  $U$ , tak i v  $N$ . Je-li  $x$  v  $U$  i v  $N$ , pak ovšem totéž platí i o  $x^{-1}$ .

Konečně k hlavnímu bodu 3:

Předně je jasné, že  $N$  je podgrupou v grupě  $UN$ , neboť prvky  $n$  z  $N$  lze psát jako součiny  $jn$  kde  $j$  jednotka leží v  $U$  (jakožto v podgrupě). Je však samozřejmé, že  $N$  je normální podgrupou v grupě  $UN$ , neboť jestliže pro libovolný prvek  $z$  z  $G$  a kterýkoli prvek  $n$  z  $N$  je i konjugovaný prvek  $z n z^{-1}$  v  $N$ , pak to tím spíše platí pro prvek  $z$  ležící v podgrupě  $UN$ .

Nyní již řádně definovaná faktorová grupa  $UN/N$  tvoří zřejmě podgrupu faktorové grupy  $G/N$ , protože obsahuje ty levé třídy dle  $N$ , které mají nějaký prvek v podgrupě  $U$ . Při nám známém homomorfním zobrazení  $x \rightarrow xN$  celé grupy  $G$  na faktorovou grupu  $G/N$  zobrazíme tedy patrně podgrupu  $U$  (grupy  $G$ ) tímto homomorfním zobrazením na faktorovou podgrupu  $UN/N$ . Nyní užijeme hlavní části 1. věty o isomorfismu.

V podgrupě  $U$  tvoří originály jednotky normální podgrupu  $N'$  tak, že faktorové grupy  $U/N$  a  $UN/N$  jsou navzájem isomorfní. Jednotkovým prvkem ve faktorové grupě  $UN/N$  je ovšem  $N$  (jakožto levá třída jednotky). Je zřejmo, že při homomorfním zobrazení  $x \rightarrow xN$ , omezeném na  $x$  z podgrupy  $U$ , budou mít  $N$  za obraz právě a jen ty prvky  $x$  z  $U$ , které současně leží v  $N$ , čili opravdu  $N' = U \cap N$  je průnik  $U$  s  $N$ , což bylo dokázat.

Než přikročíme k další kapitole, zavedme si ještě jeden základní pojem teorie grup: pojem jednoduché grupy.

Tak jako (vzhledem k dělitelnosti) hledíme celá (složená) čísla vystihovat čísly jednoduchými, tj. prvočíslly, z nichž se (násobením) každé celé číslo dá složit, tak i při zkoumání grup a toho, jak se „skládají“ ze svých podgrup a normálních podgrup nás zajímají nejprve podgrupy co možno „jednoduché“. Slova „skládají“ a „jednoduché“ byla dána do uvozovek proto, že obdoba skládání celého čísla jako součinu prvočísel se „skládáním“ grup z „jednoduchých“ podgrup je neurčitá a mnohoznačná: Jak obratu „skládat grupu“ tak výrazu z co možno „jednoduchých podgrup“ možno dávat různé přesné významy, při nichž zmíněná obdoba s čísly je při mnohem větší složitosti grup jednou větší, jednou menší. O tom více v 7. kap.

Za jednoduchou budeme jistě považovat např. každou cyklickou grupu prvočíselného řádu, poněvadž ta, jak víme z věty 6 nemá žádné netriviální podgrupy, podobně jako prvočíslo nemá jiné dělitele (celé kladné) než triviální dělitele (sebe sama a jedničku). Kdybychom však omezili pojem jednoduché grupy na cyklické grupy prvočíselného řádu, byl by takový pojem pro většinu účelů příliš úzký.

*Jako jednoduchou grupu definujeme raději grupu, která nemá žádné netriviální normální podgrupy.* Takové grupy mají tedy, obrazně řečeno, tu vlastnost, že si je již nemůžeme zjednodušit a zmenšit tím, že je „pozorujeme z dálky“ tvořením faktorové grupy. Jednoduché grupy jsou tedy jedním druhem základních stavebních kamenů obecných grup. Cyklické grupy prvočíselného řádu jsou zvláštním případem jednoduchých grup (které nemají vůbec netriviální podgrupy). Existují však také jednoduché nekonečné grupy (viz cvičení 7. za 7. kap. a při konečných grupách není jednoduchost grupy nikterak spojena s jednoduchostí jejího řádu (jak dále uvidíme).

Zvláštní a pro teorii rovnic důležitý druh konečných jednoduchých grup tvoří alternující grupy permutací stupně aspoň pátého. Těm se budeme věnovat v příští kapitole, čímž skončíme systematickou část výkladu základních pojmů teorie grup.

Mnohý z čtenářů bude snad ke své malé radosti konstatovat, že úvahy další kapitoly jsou obtížnější, než to, co předcházelo. Je to pochopitelné: prozatím jsme se omezovali na nezákladnější pojmy teorie grup a jejich vzájemné nejjednodušší souvislosti. V podstatě jsme tím jen třídili bohatý materiál jevů, ovládaných grupovou zákonitostí, aniž jsme se o mnoho povznesli nad zevšeobecněňování poznatků známých v matematice i bez teorie grup. Úsudky byly sice mnohde dosti abstraktní, zato však velmi prosté a průhledné. Tam, kde teorie grup skýtá hlubší a podstatně nové výsledky, jež (jako např. v následujícím) vedly k novým matematickým objevům, tam je již třeba vyvinout značně větší myšlenkové úsilí, abychom dobře pochopili základní myšlenku důkazu a její realizaci. Pokusím se čtenáři toto pochopení co nejvíce usnadnit, tj. provést důkaz do

podrobností, při tom ale nenechat v těchto podrobnostech zaniknout hlavní motiv celé úvahy, jehož rozvíjením a ověřováním právě důkaz je.

### Cvičení

1. Jaké jsou podgrupy v grupě  $S_3$  (sledujte v tabulce zákrytových pohybů rovnostranného trojúhelníka; tabulka podgrupy je obsažena v tabulce grupy při vhodném přerovnání jako její čtvercová část při levém horním rohu).

2. Jaké jsou levé třídy dle podgrupy všech násobků čísla 3 (celých čísel tvaru  $3k$ ,  $k = \pm 1, \pm 2, \dots$ ) v aditivní grupě celých čísel. Totéž pro násobky čísel 2, 4, 5. Jaké jsou vůbec všechny podgrupy aditivní grupy celých čísel?

3. Ukažte, že v symetrické grupě  $S_n$  (všech permutací z  $n$  čísel), všechny permutace, nechávající stát pevně různá daná čísla  $k_1, k_2, \dots, k_r$ , tvoří podgrupu, isomorfní s grupou  $S_{n-r}$ . Ukažte, že takové podgrupy jsou při stejném počtu  $r$  pevných čísel vzájemně isomorfní.

Jaké jsou levé třídy dle takové podgrupy pro  $n = 3, 4$ ;  $r = 1$ ;  $k_1 = n$ ? (Udejte je výslovně.)

4. Proveďte tytéž úvahy, které v textu jsou provedeny pro levé třídy — i pro pravé třídy v grupě dle dané podgrupy.

Sledujte v grupě  $S_3$  levé i pravé třídy dle téže podgrupy.

5. Ukažte, že každá podgrupa, dávající jen dvě levé třídy, je normální (v dané grupě).

6. Ukažte, že zobrazení  $f(x) = |x|$  (absolutní hodnota z  $x$ ) je homomorfní zobrazení multiplikativní grupy všech reálných čísel  $\neq 0$  na multiplikativní grupu všech kladných čísel reálných.

7. Ukažte, že přiřadíme-li komplexnímu číslu  $\alpha = x + iy$  jeho reálnou část  $x = R(\alpha)$ , pak  $R$  je homomorfní zobrazení aditivní grupy komplexních čísel  $\alpha$  na aditivní grupu reálných čísel  $x$ . Totéž pro imaginární část  $I(\alpha) = y$ .

8. \*Dokažte, že zobrazení

$$f \left\{ \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix} \right\} = a_1 b_2 - a_2 b_1$$

( $a_{1,2}, b_{1,2}$  reálná anebo komplexní čísla) je homomorfní zobrazení grupy všech regulárních matic stupně 2 na multiplikativní grupu všech reálných (komplexních) čísel  $\neq 0$ . Jaká je tu odpovídající grupa originálů jednotky (čísla 1)? (Dle 1. věty o isomorfismu.)

9. Přesvědčte se, že matice tvaru

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$$

( $a \neq 0$ , tzv. diagonální matice) tvoří normální podgrupu v grupě všech regulárních matic stupně 2. Dokažte, že diagonální matice jsou komutativní s každou maticí stupně 2.

10. \*Ukažte, se faktorová grupa dle normální podgrupy dle cvič. 9 je isomorfní s podgrupou všech matic  $\begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \end{pmatrix}$  splňujících

$$a_1 b_2 - a_2 b_1 = 1$$

(Návod: Ve třídě, která je prvkem faktorové grupy, vyhledejte k libovolné tam ležící matici

$$\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix}$$

matici

$$\begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ x_1 y_2 - x_2 y_1 & 1 \end{pmatrix}$$

kteřá v této třídě leží rovněž. Ukažte, že pro libovolnou matici téže třídy je tento součin též matice a že tyto matice tvoří hledanou grupu tzv. grupu reprezentantů tříd, která je isomorfní s uvedenou faktorovou grupou.)

11. Co je dle 1. věty o isomorfii normální podgrupou originálů jednotky při homomorfním zobrazení  $f(n) = i^n$  ( $i$  je imaginární jednotka) aditivní grupy celých čísel na multiplikativní grupu všech čtvrtých odmocnin z čísla  $+1$ ?

12. Budiž  $G$  grupa,  $N$  její normální podgrupa,  $H$  její podgrupa. Jestliže podgrupy  $N$  a  $H$  nemají jiných společných prvků, než jednotku grupy, je faktorová grupa  $\overline{HN}/N$  isomorfní s podgrupou  $H$ . Jestliže ještě každý prvek grupy  $G$  se dá psát jako součin prvku z  $H$  s prvkem z  $N$ , pak faktorová grupa  $G/N$  je isomorfní s podgrupou  $H$ . (Jako ve cvič. 10 je  $H$  pak grupou reprezentantů k faktorové grupě  $G/N$ .) Dokažte.

13. \*Budiž  $G$  aditivní grupa všech celých čísel,  $U$  její podgrupa všech celých násobků čísla 4 a  $N$  její (normální) podgrupa všech násobků čísla 6. Pak grupa  $UN$  je podgrupa všech sudých čísel, průnik  $U \cap N$  je podgrupa všech násobků čísla 12.

(Návod: 2 je největší společný dělitel čísel 4, 6; 12 je jejich nejmenší společný násobek.)

14. \*Ukažte, že v př. 13 nám 2. věta o isomorfismu říká, že sečítání a odčítání sudých čísel modulo 6 je isomorfní se sečítáním a odčítáním všech celých čísel dělitelných čtyřmi, ale modulo 12.



