O grupách a svazech

1.6 Rozdělení prvků grupy do tříd dle podgrupy. Homomorfni zobrazení, normální podgrupa, podílová grupa. 1. a 2. věta o isomorfismu. Pojem jednoduché grupy

In: Ladislav Rieger (author): O grupách a svazech. (Czech). Praha: Přírodovědecké vydavatelství, 1952. pp. 53–80.

Persistent URL: http://dml.cz/dmlcz/403367

8. Ukažte, že násobící grupa všech komplexních čísel o absolutní hodnotě = 1 je isomorfní s grupou všech euklidovských otočení roviny (viz cvič. 1 k 1,4).

9.*Ukažte, že všechny regulární lomené transformace $T(a_1, b_1, a_2, b_2)$ jedné reálné (po př. komplexní) proměnné x tvaru

$$T(a_1, b_1, a_2, b_2) = \left\{ x' = \frac{a_1 x + b_1}{a_2 x + b_2} \right.$$

kde a_1, b_1, a_2, b_2 jsou reálná (komplexní) čísla, t. j. parametry transformace $T(a_1, b_1, a_2, b_2)$, která je jimi plně určena, a kde $a_1 b_2 - a_2 b_1 \neq 0$ (podmínka regulárnosti)) tvoří grupu (zvláštní případ t. zv. projektivní grupy).

Ukažte, že tato grupa (která jakožto grupa transformací jedné proměnné není lineární) je isomorfní s grupou všech lineárních homog. transformací dvou proměnných (čili je isomorfní s grupou všech regulárních matic stupně 2).

Ukažte, že t. zv. afinní transformace tvaru $x' = a_1 x + b_1$ tvoří podgrupu (zvl. případ t. zv. afinní grupy).

1,6. ROZDĚLENÍ PRVKŮ GRUPY DO TŘÍD DLE PODGRUPY. HOMOMORFNÍ ZOBRAZENÍ, NORMÁLNÍ PODGRUPA, PODÍLOVÁ 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 $x \,.\, h$, kde h probíhá celou podgrupu H. Souhrn těchto prvků si označíme jako $x \,.\, H$ 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 $x = x_1 \,.\, h_1 = x_2 \,.\, h_2$ při vhodných prvcích h_1 a h_2 z podgrupy

H. Libovolný prvek z levé třídy x_1H má tvar $x_1 \,.\, h$, kde h je prvek z podgrupy H. Dosazením z předchozího máme

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

Protože H je podgrupa, leží v ní s prvky h_1, h_2, h i součin $h_2 \,.\, h_1^{-1} \,.\, h$, takže libovolný prvek $x_1 \,.\, h$ 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. Tedy je 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, t. j. 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 $x \,.\, h_1 = x \,.\, h_2$ 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 „přihrádek", 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 (t. j. 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 odpustíme.

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

$$\ldots, a^{-2}, a^{-1}, a' = j, a^1, a^2, \ldots$$

Jestliže grupa G je konečná, nemohou být ani mocniny

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

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 t. zv. *řád prvku*. Je to zároveň i řád cyklické podgrupy, vytvořené prvkem a, protože prvky této cyklické podgrupy jsou mocniny $a, a^2, a^3, \ldots, a^{n-1}, a^n = j$ v počtu n. (Nepřekvapuje nás, že pak je třebas pro prvek a řádu 7

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

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

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

a tvoří t. zv. nekonečnou cyklickou grupu. Nekonečné cyklické grupy jsou zřejmě isomorfní se sečítací 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 t. zv. malá Fermatova[24] věta číselné theorie.

[24] Fermat byl veliký francouzský matematik ze 17. stol., jeden ze zakladatelů novověké matematiky. (Pojem grupy ovšem ještě neznal.)

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) — 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 t. zv. modulu ($0 = 0 \,.\, n$ je rovněž násobek čísla n). φ je t. zv. *Eulerova*[25] funkce číselné theorie.

Odvození malé Fermatovy věty z našeho důsledku věty 5 bude ukázkou aplikace abstraktní poučky z theorie grup na konkretním matematickém materiálu. Proveďme 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 prvky naší grupy, a za druhé určit pro ně grupové násobení.

Prvky naší grupy budou nikoli snad jednotlivá čísla, nýbrž jisté celé t. zv. zbytkové třídy dle dělitele, t. zv. modulu n, t. j. 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 o rozdílu $b - a = -(a - b)$. (Na př. pro $n = 12$ patří $5^4 = 625 = 52 \,.\, 12 + 1$ do téže zbytkové třídy modulo 12

[25] L. Euler byl znamenitý německý matematik 18. stol., který prožil část života v Rusku v tehdejším Petrohradě (Leningradě).

jako 1; $-3 \equiv 9 \pmod{12}$ protože $-3-9=-12=-1 . 12$.)

Zbytkovou třídu, do níž patří číslo a, vyznačujeme někdy pomocí pruhu nahoře, tedy jako $\bar{a}$, takže $\bar{a}=\bar{b}$ 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 theorii 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 $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$.

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 $n=12$ na př. $\varphi(12)=4$. Zde je třeba si uvědomit dvojí věc. Předně zbytek 0 není nesoudělný (= je soudělný) s číslem n, neboť $0 = n . 0$ a $n = n . 1$, tedy čísla 0 a n mají za největší společný násobek číslo n, čili třída $\bar{0}$, t. j. 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

$$a = q . n + r_a$$

(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 $a - q . n = r_n$ 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 $\overline{a} \,.\, \overline{b}$ dvou zbytkových tříd rozumíme tu zbytkovou třídu, do níž náleží (obyčejný) součin ab. Můžeme tedy definici našeho násobení tříd psát rovností

$$\overline{a} \,.\, \overline{b} = \overline{ab}.$$

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

Jde již jen o to zjistit platnost grupových zákonů v naší, t. zv. násobící grupě modulo n.

Axiom (1) neomezenosti a jednoznačnosti bude splněn, jestliže předně — kvůli jednoznačnosti — výsledek násobení $\overline{ab}$ třídy $\overline{a}$ třídou $\overline{b}$ 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 $\overline{a}$ a b' do třídy $\overline{b}$, 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 dělitelny 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 s asociativity násobení čísel samých. Neboť jsou-li a, b, c tři libovolná celá čísla, pak platí

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

Axiom (3) jednotkového prvku je splněn pro zbytkovou třídu $\bar{1}$ (čísel, zanechávajících zbytek 1 při dělení modulem). Neboť nechť $i = q \,.\, n + 1$ je číslo z třídy $\bar{1}$ (t. j. $\bar{1} = \bar{i}$). Nechť 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 $x = p \,.\, n + r$ (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

$$\bar{x} \,.\, \bar{1} = \bar{1} \,.\, \bar{x} = \bar{x}.$$

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

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

(Na př. 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

$$\bar{x} \,.\, \bar{a} = \bar{a} \,.\, \bar{x} = \bar{1}$$

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, t. j. utvořme čísla

$$aa_1 = a, aa_2, aa_3, \ldots, aa_n.$$

(Na př. tedy třebas 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 $a, aa_1, \ldots, aa_{\varphi(n)}$ 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 $aa_1, aa_2, \ldots, aa_{\varphi(n)}$ 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 $t = 1, 2, \ldots, n$) dá nezáporný zbytek 1 při dělení číslem n, takže pak lze položit $x = a_t$ a je $\bar{x} \,.\, \bar{a} = \bar{a} \,.\, \bar{x} = \bar{1}$. (V našem příkladě mezi čísly 7, 35, 49, 77 nalézáme $49 = 4 \,.\, 12 + 1 \equiv 1 \pmod{12}$, 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 vytčeném 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, t. j. 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 $\varphi(n) = m \,.\, q$, 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 násobící grupy tříd celých čísel nesoudělných s modulem n, jichž jsme právě užili ke grupově theoretickému 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 t. zv. Fermatovu větu theorie grup, to jest tvrzení, že *v grupě řádu N je N-tá mocnina libovolného prvku rovna jednotce grupy, t. j.* $a^N = j$, kde a je libovolně zvolený prvek, j je jednotka dané grupy.

Uveďme 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, $n = r \,.\, s$, 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 $a^r, {}^{2r}, {}^{3r}, \ldots, a^{sr} = j$, 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

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

Potom však prvek a vytváří v G netriviální cyklickou podgrupu, takže možnost 2 dle předpokladu odpadá. Obráceně 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 t. zv. Fermatovy věty theorie 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 inversního prvku ke každému prvku v naší části, jež má být podgrupou, neboť přítomnost jednotky je již důsledkem.

Obraťme se k zásadně důležitému pojmu t. zv. 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 řekněme součást stroje školním modulem, který je sice z jiného materiálu (a po př. menších rozměrů), ale jehož tvar je přesně shodný s tvarem originálu.

Pro mnohé účely však stačí zmíněnou součást stroje kolmo *promítnout* (pomocí deskriptivní geometrie) 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 theorii 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.

Uveďme 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 prvém příkladě bude zobrazovanou grupou známá symetrická grupa $\mathfrak{S}_n$ všech permutací stupně n (z n předmětů). Přitom si zavedeme několik pojmů, které budeme potřebovat i později.

Říkáme, že permutace π provedená na n čísel $1, 2, \ldots, n$ je **sudá** anebo **lichá** podle toho, zda v pořadí čísel $\pi(1), \pi(2), \ldots, \pi(n)$ došlo k sudému či lichému počtu porušení přirozeného sledu dvou čísel, čili k sudému, či lichému počtu **inversí**. Na př. 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 inverse a permutace π je lichá. Permutace $\varrho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 4 & 3 & 1 \end{pmatrix}$ je sudá, protože má celkem 8 inversí.

Přiřaďme libovolně zvolené permutace π stupně n, jakožto prvku symetrické grupy $\mathfrak{S}_n$, číslo $+1$ anebo -1 podle toho, je-li tato permutace sudá či lichá. Takto přiřazené číslo k permutaci π označme jako $\varepsilon(\pi)$. Ukažme, že tím definované zobrazení je homomorfním zobrazením grupy $\mathfrak{S}_n$ na (násobící) grupu čísel $+1$ a -1, což patrně je cyklická grupa řádu 2. K tomu účelu vystihneme číslo $\varepsilon(\pi)$ (k dané permutaci π) takto: Znásobme si všechny rozdíly $\pi(h) - \pi(k)$, kde $h > k$. Pak součin (o zřejmém počtu $(n-1) + (n-2) + \ldots + 1 = \frac{(n-1) \cdot n}{2}$ činitelů) bude mít tolik záporných činitelů, kolikrát došlo k inversi při permutaci π, 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 $h, k = 1, 2, 3, \ldots, n$ a $h > k$, obdržíme právě číslo $\varepsilon(\pi)$. Krátce to lze vypsat 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 $\mathfrak{S}_n$ na grupu $(+1, -1)$. Protože zřejmě existují jak permutace sudé, tak i liché každého stupně n, 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

$$\varepsilon(\varrho\pi) = \varepsilon(\varrho) \,.\, \varepsilon(\pi).$$

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

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

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

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

Zde druhý součin je již číslo $\varepsilon(\pi)$. První součin však není nic jiného, než číslo $\varepsilon(\varrho)$. Neboť probíhají-li h, k čísla $1, 2, \ldots, n$, 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 $1, 2, \ldots, n$. Stane-li se však, že rozdíl $\pi(h) - \pi(k)$ je záporný (zatím co jsme předpokládali ve jmenovateli rozdíl kladný), pak to nevadí, neboť lze psát v takovém případě

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

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 $\varepsilon(\varrho)$. Máme tedy skutečně rovnost $\varepsilon(\varrho\pi) = \varepsilon(\varrho)\,\varepsilon(\pi)$ čili zobrazení ε je vskutku homomorfním zobrazením.

Je jasné, že zde homomorfní obraz, t. j. cyklická grupa řádu 2, je hrubý a vystihuje symetrickou grupu permutací velmi málo.[26]

2. V druhém příkladě bude homomorfní obraz věrnější.

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

$$(x_1 + i\,.\,y_1)(x_2 + i\,.\,y_2) = (x_1x_2 - y_1y_2) + \\ + i\,.\,(x_1y_2 + x_2y_1)$$

(kde $i = \sqrt{-1}$).

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

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

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

[26] Říká jen, že sudá kráte sudá a lichá kráte lichá permutace je sudá, lichá krát sudá a sudá krát lichá permutace je lichá permutace.

$$(x_1x_2 - y_1y_2)^2 + (x_1y_2 + x_2y_1)^2 = (x_1^2 + y_1^2)(x_2^2 + y_2^2)$$

(jestliže věc nezná ze školy).

Nyní je již na místě přesná abstraktní definice.

Definice.

Buďtež 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, t. zv. originálu, z grupy G.

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

$$f(x_1x_2) = f(x_1) \cdot f(x_2)$$

(jestliže tečkou . 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 k ničemu, protože naprosto deformuje zobrazovanou grupu.

Homomorfní zobrazení dává inversnímu prvku za obraz inversní 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

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

Nyní již není třeba zvláště podrobně vysvětlovat, co je to homomorfní representace dané grupy grupou permutací anebo grupou matic. Je to přirozené a důležité rozšíření pojmu isomorfní representace, s nímž jsme se již seznámili. Je zajímavé, že homomorfní representace 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", t. j. homomorfních representací (podobně jako si těleso zrekonstruujeme z jeho nárysu a půdorysu), jestliže známe t. zv. úplný systém homomorfních representací[27] dané grupy, z něhož lze sestrojit isomorfní obraz dané grupy. Vedlo by nás příliš daleko, kdybychom měli podat příklady na to; čtenář, který se odhodlá k hlubšímu studiu theorie grup je nalezne v obšírnějších učebnicích theorie grup.

Obrátíme se k dalšímu důležitému pojmu abstraktní theorie 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 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 prvém předchozím příkladě se symetrická grupa $\mathfrak{S}_n$ (všech permutací stupně n) rozpadá homomorfním zobrazením $f = \varepsilon$ (na cyklickou násobící grupu z čísel ± 1) ve dvě třídy, třídu sudých a třídu lichých permutací. V druhém předchozím příkladě se násobící grupa všech od nuly růz-

[27] Úplným nazýváme takový systém homomorfních representací, v němž každý nikoli jednotkový originál obdrží alespoň jednou nikoli jednotkový obraz.

ných komplexních čísel, znázorněných body komplexní roviny (mimo počátek) rozpadá 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 přesvědčíme, 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 inversního prvku je inversní prvek k obrazu původního prvku. Podgrupu (grupy G) originálů jednotky v našem homomorfním zobrazení grupy G na grupu H nazveme na příklad 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 týž 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

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

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}, t. zv. konjugovaný prvek k prvku x pomocí (libovolného) prvku z z grupy G.

Tak na př. ze dvou nám známých podgrup grupy euklidovských pohybů roviny (př. 2 v odst. 1,4) 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 $\mathfrak{S}_n$ tvoří t. zv. alternující grupu $\mathfrak{A}_n$ stupně n, která je normální podgrupou v grupě $\mathfrak{S}_n$. — V každé Abelově (komutativní) grupě je ovšem zřejmě každá podgrupa normální. (Obrácené tvrzení neplatí, viz cvič. 7 z odst. 1,5)*.

Důležitost normálních podgrup v grupě vyplývá z toho, že pomocí nich lze z dané grupy tvořit potřebné nové grupy, je-

*) V grupě základních kvaternionů ze cvič. 7 z odst. 1,5 je každá podgrupa normální podgrupou, ačkoli grupa není Abelova.

jímiž prvky se stávají celé (levé) třídy podle takové normální podgrupy. Násobení v takové grupě levých tříd dle normální podgrupy N grupy G je dáno takto: Jsou-li xN a yN dvě levé třídy (prvků x a y z G), potom za jejich součin $xN \,.\, yN$ položíme tu levou třídu, která obsahuje součin xy, to jest klademe

$$xN \,.\, yN = xyN.$$

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 $x' = xu_1$ 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

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

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): inversním prvkem k prvku (t. j ke třídě) xN je patrně třída $x^{-1}N$, protože součin $xN \,.\, x^{-1}N$ stejně jako $x^{-1}N \,.\, xN$ obsahuje jednotku j_G.

Grupě levých tříd v grupě G dle normální podgrupy N říkáme: Podílová grupa grupy G dle normální podgrupy N a značíme $\frac{G}{N}$; 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 podílové grupy $\frac{G}{N}$.

Jaký je zobrazovací vztah podílové grupy $\frac{G}{N}$ k původní grupě?

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

Vraťme se nyní k případu, že normální podgrupa N grupy G je souhrnem originálů jednotky v jakémsi homomorfním zobrazení f grupy G na grupu H. Jaký bude vztah podílové grupy $\frac{G}{N}$ ke grupě H?

Snadno nahlédneme, že tyto grupy jsou si 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 podílové grupy $\frac{G}{N}$ na grupu H je zřejmě homomorfní a kromě toho vzájemně jednoznačné. Shrňme si tedy výsledek předchozích úvah do následující t. zv. první věty o isomorfismu theorie 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 samy t. zv. podílovou grupu $\frac{G}{N}$ při násobení $xN \,.\, yN = xyN$. Podílová grupa $\frac{G}{N}$ je homomorfním obrazem grupy G při homomorfním zobrazení $x \to xN$ 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 podílová grupa $\frac{G}{N}$ je isomorfně zobrazena na grupu H zobrazením $\bar{f}$, daným rovností

$$\bar{f}(xN) = f(x).$$

Uvedená 1. věta o isomorfismu theorie 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:

Podílová grupa $\frac{\mathfrak{S}_n}{\mathfrak{A}_n}$ symetrické grupy stupně n podle její normální alternující podgrupy $\mathfrak{A}_n$ je isomorfní s kteroukoli cyklickou grupou řádu 2, na př. s podgrupou $(+1, -1)$ násobící grupy všech zlomků.

Násobící grupa kladných reálných čísel je isomorfní s podílovou grupou násobící grupy všech komplexních čísel o absolutní hodnotě 1.

Uveďme ještě jeden důležitý příklad na tvoření podílové grupy. Za grupu G vezměme sečítací 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, t. j. jež dávají při dělení modulem n týž nezáporný nejmenší zbytek. Podílová grupa $\frac{G}{N}$ je t. zv. sečítací grupa modulo n.

(Pozor, něco jiného byla t. zv. násobící grupa modulo n, která se skládala jen ze zbytkových tříd, naplněných vesměs čísly, nesoudělnými s modulem, kdežto sečítací grupa modulo n obsahuje všechny zbytkové třídy.) Je-li H jakákoli cyklická

grupa řádu n, na př. násobící grupa všech n n-tých odmocnin z 1, pak první věta o isomorfii nám zde říká, že sečítací grupa modulo n je isomorfní s touto cyklickou grupou.

Tvořením podílové grupy z grupy G podle normální podgrupy N ztotožňujeme vlastně prvky, patřící do téže levé třídy dle N v G. Zanedbávajíce rozdílnosti mezi prvky téže levé třídy, počínáme si obrazně řečeno asi tak, jako bychom se na naši grupu dívali (s 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" (t. j. homomorfním zobrazením) dané grupy na jinou grupu H.

Normální podgrupy mají i jiné charakteristické vlastnosti, jimiž je možno je definovat. Hloubavý 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 odvoďme důležitou t. zv. druhou větu o isomorfismu theorie grup. Je to pomocná věta významu theoretického, jejíž užití si ukážeme v par. 1,6.

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 podgrupa v grupě G.* (Takový souhrn UN je t. zv. spojení podgrup U a N.)

2. *Souhrn označený jako $U \cap N$ všech prvků z grupy 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 podílové grupy $\frac{UN}{N}$ *a* $\frac{U}{U \cap N}$ *jsou navzájem isomorfní.*

Důkaz:

Nejprve k bodu 1:

Máme ukázat především, že součin dvou násobků tvaru $u_1 n_1$ a $u_2 n_2$, 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

$$(u_1 n_1)(u_2 n_2) = u_1 u_2 (u_2^{-1} n_1 (u_2^{-1})^{-1} n_2).$$

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 $u = u_1 u_2$ pak leží v U, protože U je podgrupa obsahující u_1 i u_2. Z rovností $(u_1 n_1)^{-1} = n_1^{-1} u_1^{-1} = u_1^{-1} (u_1 n_1^{-1} u_1^{-1})$ je pak již snadno patrno, že UN je vskutku podgrupou v A.

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 znz^{-1} v N, pak to tím spíše platí pro prvek z ležící v podgrupě UN.

Nyní již řádně definovaná podílová grupa $\frac{UN}{N}$ tvoří

zřejmě podgrupu podílové grupy $\frac{G}{N}$, protože obsahuje ty levé třídy dle N, které mají nějaký prvek v podgrupě U. Při námi známém homomorfním zobrazení $x \to xN$ celé grupy G na podílovou grupu $\frac{G}{N}$ zobrazíme tedy patrně podgrupu U (grupy G) tímto homomorfním zobrazením na podílovou podgrupu $\frac{UN}{N}$. Nyní užijeme hlavní části 1. věty o isomorfismu. V podgrupě U tvoří originály jednotky normální podgrupu N' tak, že podílové grupy $\frac{U}{N'}$ a $\frac{UN}{N}$ jsou navzájem isomorfní. Jednotkovým prvkem v podílové grupě $\frac{UN}{N}$ je ovšem N (jakožto levá třída jednotky). Je zřejmo, že při homomorfním zobrazení $x \to xN$, 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 dalšímu paragrafu, zaveďme si ještě jeden základní pojem theorie grup: pojem jednoduché grupy.

Tak jako (vzhledem k dělitelnosti) hledíme celá (složená) čísla vystihovat čísly jednoduchými, t. j. prvočísly, 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 par. 1,7.

Za jednoduchou budeme jistě považovat na př. 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 podílové 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. po 1,7) a při konečných grupách není jednoduchost grupy nikterak spojena s jednoduchostí jejího řádu (jak dále uvidíme).

Zvláštní a pro theorii rovnic důležitý druh konečných jednoduchých grup tvoří alternující grupy permutací stupně aspoň pátého. Těm se budeme věnovat v příštím paragrafu, čímž skončíme systematickou část výkladu základních pojmů theorie grup.

Mnohý z čtenářů bude snad ke své malé radosti konstatovat, že úvahy dalšího paragrafu jsou obtížnější, než to, co předcházelo. Je to pochopitelné: prozatím jsme se omezovali na nejzákladnější pojmy theorie grup a jejich vzájemné nejjednodušší souvislosti. V podstatě jsme tím jen třídili bohatý materiál zjevů, ovládaných grupovou zákonitostí, aniž jsme se o mnoho povznesli nad zevšeobecňování poznatků známých v matematice i bez theorie grup. Úsudky byly sice mnohde dosti abstraktní, zato však velmi prosté a průhledné. Tam, kde theorie grup skýtá hlubší a podstatně nové výsledky, jež (jako na př. v následujícím) vedly k novým

matematickým objevům, tam je již třeba vyvinout značně větší myšlenkové úsilí, abychom dobře pochopili základní myšlenku důkazu a její realisaci. Pokusím se čtenáři toto pochopení co nejvíce usnadnit, t. j. provést důkaz do podrobností, při tom ale nenechat v těchto podrobnostech zaniknout hlavní motiv celé úvahy, jehož rozvíjením a ověřováním právě důkaz je.

Cvičení k 1,6.

1. Jaké jsou podgrupy v grupě $\mathfrak{S}_3$ (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 $3k$, $k = \pm 1, \pm 2, \ldots$) v sečítací grupě celých čísel. Totéž pro násobky čísel 2, 4, 5. Jaké jsou vůbec všechny podgrupy sečítací grupy celých čísel?

3. Ukažte, že v symetrické grupě $\mathfrak{S}_n$ (všech permutací z n čísel), všechny permutace, nechávající stát pevně různá daná čísla $k_1, k_2, \ldots k_r$, tvoří podgrupu, isomorfní s grupou $\mathfrak{S}_{n-r}$. 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 $\mathfrak{S}_3$ 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 násobící grupy všech reálných čísel $\neq 0$ na násobící grupu všech kladných čísel reálných.

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

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 násobící 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

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

($a \neq 0$, t. zv. 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, že podílová 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 podílové grupy, vyhledejte k libovolné tam ležící matici

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

matici

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

která v této třídě leží rovněž. Ukažte, že pro libovolnou matici téže třídy je tento součin táž matice a že tyto matice tvoří hledanou grupu t. zv. grupu representantů tříd, která je isomorfní s uvedenou podílovou grupou.)

11. Co je dle 1. věty o isomorfii normální podgrupou originálů jednotky při homomorfním zobrazení $f(n) = i^n$ ($i = \sqrt[+]{-1}$) sečítací grupy celých čísel na násobící 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, pak je podílová grupa $\frac{HN}{N}$ isomorfní s podgrupou H. Jestliže ještě každý prvek grupy G se dá psát jako součin prvku z H s prvkem z N, pak podílová grupa $\frac{G}{N}$ je isomorfní s podgrupou H. (Jako ve cvič. 10 je H pak grupou representantů k podílové grupě $\frac{G}{N}$.) — Dokažte.

13.* Budiž G sečítací 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.

1,7. TŘÍDA KONJUGOVANÝCH PRVKŮ. NORMALISÁTOR PRVKU. TŘÍDOVÁ ROVNICE. KONJUGOVANÉ PERMUTACE. JEDNODUCHOST ALTERNUJÍCÍ GRUPY $\mathfrak{A}_n$ PRO $n > 4$.

Při pojmu normální grupy jsme narazili na pojem konjugovaných prvků v grupě (prvek y byl nazván konjugovaným s prvkem x pomocí prvku z, jestliže platilo

$$y = zxz^{-1}).$$

Vzájemná konjugovanost prvků je jakási příbuznost, která dovoluje rozdělit důležitým způsobem prvky grupy do oddělených tříd vzájemně konjugovaných prvků (dle zcela jiného hlediska než rozdělení do levých tříd dle podgrupy).

Utvoříme-li totiž v grupě skupiny vzájemně konjugovaných prvků, pak zřejmě každý prvek grupy leží v (alespoň) jedné skupině a žádný neleží ve dvou či více skupinách současně. Neboť jakmile by prvek z byl konjugován jednak s prvkem x, jednak s prvkem y, čili jakmile by $z_1 x z_1^{-1} = z_2 y z_2^{-1}$, pak by

$$y = z_2^{-1} z_1 x z_1^{-1} z_2 = z_2^{-1} z_1 x (z_2^{-1} z_1)^{-1},$$

takže x by bylo konjugováno s y. Každá grupa G se tedy skutečně rozpadá ve třídy vzájemně konjugovaných prvků.

Některé třídy mohou ovšem obsahovat jen jediný prvek. Především je jednotkový prvek j (v grupě G) konjugován sám se sebou, protože $xjx^{-1} = j$. V Abelových grupách je rozdělení do tříd konjugovaných prvků zřejmě nezajímavé, každá třída vzájemně konjugovaných prvků se tam skládá z jediného prvku.