23. ÚVOD DO TEÓRIE GRÚP

Pojem grupy hrá natoľko kľúčovú úlohu nielen v algebre, ale i v celej modernej matematike a jej početných aplikáciách, že ani v našom kurze lineárnej algebry a geometrie by už naďalej nebolo únosné sa mu vyhýbať.

Pri analýze akéhokoľvek (nie nevyhnutne matematického) štruktúrovaného oboru objektov hrá dôležitú úlohu otázka jeho *symetrie*. Znalosť transformácií, ktoré zachovávajú príslušnú štruktúru (t.j. jej symetrií), nám totiž neraz umožňuje výrazne sprehľadniť a zjednodušiť jej popis. Čím je takýchto transformácií viac, tým symetrickejšiu štruktúru nesie spomínaný obor, malé množstvo takýchto transformácií naopak svedčí o nízkom stupni symetrie.

Ukazuje sa, že (bijektívne) transformácie zachovávajúce danú štruktúru tvoria vždy *grupu*, t.j. množinu transformácií uzavretú vzhľadom na kompozíciu, obsahujúcu identickú transformáciu a spolu s každou transformáciou aj transformáciu k nej inverznú. Typickými príkladmi takýchto grúp sú kryštalografické grupy, alebo grupy transformácií euklidovských priestorov zachovávajúcich rôzne invarianty, ako napr. dĺžku, objem či uhol. Grupa transformácií daného štruktúrovaného oboru však v sebe nesie podstatne viac informácií o jeho symetrii, než len to, či je ich „veľa“ alebo „málo“. I „rovnako veľké“ grupy sa totiž môžu výrazne líšiť svojou vlastnou vnútornou štruktúrou, a tým spätne mnoho vypovedať o symetrii a štruktúre pôvodných oborov.

V tejto kapitole sa stručne oboznámime len s celkom základnými pojmami a výsledkami teórie grúp. V duchu modernej algebry ich však budeme študovať v abstraktnom poňatí, t.j. bez toho, aby sme predpokladali, že ide nutne o grupy transformácií. Tým sa budeme podrobnejšie venovať až v nasledujúcej kapitole.

23.1. Abstraktný pojem grupy

Grupou nazývame množinu G vybavenú binárnou operáciou $\cdot : G \times G \to G$, ktorá spĺňa nasledujúce podmienky, nazývané tiež *axiómami teórie grúp*:

(a) $(\forall\, a,b,c \in G)\big(a(bc) = (ab)c\big)$,
t.j. operácia $\cdot$ je asociatívna;

(b) $(\exists\, e \in G)(\forall\, a \in G)(ae = ea = a)$,
t.j. existuje neutrálny prvok $e \in G$ operácie $\cdot$;

(c) $(\forall\, a \in G)(\exists\, b \in G)(ab = ba = e)$,
t.j. ku každému $a \in G$ existuje inverzný prvok $b \in G$ vzhľadom na operáciu $\cdot$.

Ako už vieme z paragrafu 0.4, neutrálny prvok $e \in G$ je podmienkou (b) určený jednoznačne; podobne je podmienkou (c) jednoznačne určený inverzný prvok $b \in G$ k danému $a \in G$.

Hovoríme, že grupa G je *komutatívna*, alebo tiež *abelovská*, ak operácia $\cdot$ je komutatívna, t.j. platí $ab = ba$ pre všetky $a, b \in G$.

Uvedený spôsob zápisu, pri ktorom grupovú operáciu značíme $\cdot$ (a jej znak väčšinou vynechávame), prípadne $\circ$, nazývame *multiplikatívny zápis*. Grupovú operáciu vtedy nazývame *súčinom* alebo *násobením*, prípadne *skladaním* alebo *kompozíciou*.

Neutrálny prvok nazývame tiež *jednotkovým prvkom* alebo *jednotkou*, prípadne *identitou* a značíme ho väčšinou e, ε alebo 1, prípadne $\boldsymbol{I}$, id, ι a pod. Inverzný prvok k prvku $a \in G$ značíme a^{-1}, občas tiež a' alebo $\bar{a}$. Zrejmým spôsobom (porovnaj s paragrafom 1.2) zavádzame výrazy a^n pre $a \in G$, $n \in \mathbb{Z}$.

Grupovú operáciu, neutrálny prvok resp. inverzný prvok k danému môžeme, samozrejme, označiť hocako. Popri multiplikatívnom zápise sa však bežne používa už len tzv. *aditívny zápis*, pri ktorom grupovú operáciu značíme $+$ a nazývame *sčítaním*, neutrálny prvok značíme 0 a nazývame *nulou* alebo *nulovým prvkom* a inverzný prvok značíme $\Leftrightarrow a$ a nazývame *opačným prvkom* k prvku $a \in G$. Čitateľ by si mal samostane premyslieť, ako sa zmení formulácia grupových axióm (a), (b), (c) pri prechode k aditívnemu zápisu. Výrazy $a \Leftrightarrow b$, na, pre $a, b \in G$, $n \in \mathbb{Z}$, zavádzame obdobne ako v paragrafe 1.2.

Aditívny zápis je rezervovaný takmer výlučne pre abelovské grupy. To neznamená, že by sme sa s komutatívnou grupou nemohli stretnúť v multiplikatívnom zápise. No uvedením nejakej grupy v aditívnom zápise už vlastne dávame najavo (pokiaľ výslovne nezdôrazníme opak), že ide o abelovskú grupu.

Ako sme už naznačili, grupu väčšinou označujeme rovnakým znakom ako jej základnú množinu. Niekedy je však účelné zahrnúť do jej označenia i príslušnú grupovú operáciu, prípadne aj jej neutrálny prvok; vtedy hovoríme napr. o grupe $(G, \cdot)$, grupe $(A, +, 0)$ a pod.

Hovoríme, že *grupa* G je *konečná* resp. *nekonečná*, ak jej základná množina má príslušnú vlastnosť. *Rádom konečnej grupy* nazývame počet jej prvkov.

S niektorými jednoduchými príkladmi grúp sme sa už v našom kurze stretli.

23.1.1. Príklad. Množina $\mathbb{Z}$ všetkých celých čísel tvorí grupu vzhľadom na operáciu sčítania. Podobne, pre $n \geq 1$, tvorí grupu množina $\mathbb{Z}_n = \{0, 1, \ldots, n \Leftrightarrow 1\}$ všetkých zvyškových tried s operáciou sčítania modulo n (pozri paragraf 1.3). Zrejme $(\mathbb{Z}, +)$ aj všetky $(\mathbb{Z}_n, +)$ sú napospol abelovské grupy.

23.1.2. Príklad. Každé pole K určuje hneď dve komutatívne grupy. Je to jednak aditívna grupa $(K, +, 0)$, jednak multiplikatívna grupa $(K \setminus \{0\}, \cdot, 1)$ jeho nenulových prvkov, ktorú zvykneme tiež značiť $(K^\star, \cdot, 1)$ alebo len krátko $K^\star$. V prípade polí $\mathbb{Q}$ a $\mathbb{R}$ sa k nim pridružujú ešte multiplikatívne grupy $(\mathbb{Q}^+, \cdot, 1)$ resp. $(\mathbb{R}^+, \cdot, 1)$ kladných prvkov daného poľa.

Podobne určuje každý vektorový priestor V nad ľubovoľným poľom K abelovskú grupu $(V, +, \mathbf{0})$.

23.1.3. Príklad. Z úvah vykonaných v paragrafe 0.5 vyplýva, že množina $\mathcal{S}(X)$ všetkých permutácií ľubovoľnej množiny X tvorí grupu vzhľadom na operáciu $\circ$ skladania zobrazení, s jednotkou id_X. Táto grupa je pre $\# X \geq 3$ nekomutatívna. Pre konečnú množinu $X = \{1, \ldots, n\}$ nazývame grupu $\mathcal{S}(X) = \mathcal{S}_n$ *symetrickou grupou stupňa* n; jej rád je zrejme $n!$.

23.1.4. Príklad. Množinu všetkých regulárnych matíc rozmeru $n \times n$ nad poľom K budeme odteraz značiť $\mathrm{GL}(n, K)$. Z výsledkov paragrafu 7.2 vyplýva, že $\mathrm{GL}(n, K)$ tvorí grupu vzhľadom na operáciu násobenia matíc, s jednotkou $\boldsymbol{I}_n$; nazývame ju *všeobecná lineárna grupa (stupňa n nad poľom K)* (GL je skratka anglického *general linear*). Pre $n \geq 2$ je $\mathrm{GL}(n, K)$ nekomutatívna grupa.

Pri pohľade na pred chvíľou uvedenú definíciu a za ňou nasledujúce dôverne známe príklady hĺbavejšieho čitateľa asi nevdojak napadne otázka, prečo sme s definíciou grupy tak dlho otáľali. Pritom je to definícia – najmä v porovnaní s definíciami poľa a vektorového priestoru (pozri paragrafy 1.2 a 1.5) – veľmi jednoduchá. Vlastne už v paragrafe 0.4 sme mali pohromade všetky pojmy potrebné nato, aby sme ju mohli vysloviť. Navyše, keby sme vtedy boli tak učinili, mohli sme trochu neskôr definície poľa a vektorového priestoru sformulovať podstatne kratšie a jednoduchšie.

Napr. v definícii poľa (pozri paragraf 1.2) možno prvé štyri formuly ľavého stĺpca zhrnúť do podmienky, že množina K tvorí vzhľadom na sčítanie $+$ komutatívnu grupu s nulovým prvkom 0, a celý ľavý stĺpec zasa do podmienky, že množina $K^\star = K \setminus \{0\}$ tvorí komutatívnu grupu vzhľadom na násobenie s jednotkovým prvkom 1 (potom nutne $1 \in K^\star$, teda $0 \neq 1$). Zostáva už len jediná formula – distributívny zákon –, ktorá dáva do súvisu obe operácie. S istou dávkou zjednodušenia možno povedať, že pole pozostáva z dvoch komutatívnych grúp spojených distributívnym zákonom.

Podobne možno prvé štyri formuly v definícii vektorového priestoru (pozri paragraf 1.5) nahradiť požiadavkou, že $(V, +, \mathbf{0})$ je abelovská grupa.

To by však bol takmer celý zisk, ktorý by nám v našom doterajšom kurze lineárnej algebry a geometrie kynul z takého skorého zavedenia pojmu grupy. Navyše, pokiaľ by sme nechceli neorganicky odbočovať od témy, prípadne na prítomnosť grúp v našom výklade umelo upozorňovať, boli by sme obmedzení v podstate na grupy uvedené v príkladoch 23.1.1–4, v ktorých prevládajú abelovské grupy. Takéto obmedzenie by však zastieralo viaceré podstatné znaky sveta grúp, v ktorom naopak prevládajú grupy neabelovské. Práve stručnosť a jednoduchosť definície grupy má totiž za následok, že jej vyhovuje obrovské množstvo nesmierne rozmanitých matematických objektov, a tým aj prekvapivú zložitosť možnej štruktúry grúp. Abelovské grupy, a obzvlášť vektorové priestory patria práve k tým štruktúrne najjednoduchším predstaviteľom grúp.

Systematické štúdium teórie grúp nie je predmetom lineárnej algebry, teda ani tohto kurzu. Obmedzíme sa len na jej základné pojmy a výsledky v miere, ktorá nám umožní ich využitie pri hlbšom objasnení algebraickej a geometrickej štruktúry vektorových priestorov.

V nasledujúcom tvrdení, ktorého dôkaz prenechávame ako jednoduché cvičenie čitateľovi, je zhrnutých niekoľko najelementárnejších pravidiel pre počítanie v grupách.

23.1.5. Tvrdenie. *Nech $(G, \cdot, e)$ je grupa. Potom pre ľubovoľné prvky $a, b, c \in G$ a $m, n \in \mathbb{Z}$ platí*

$$e^{-1} = e, \qquad \left(a^{-1}\right)^{-1} = a, \qquad (ab)^{-1} = b^{-1}a^{-1},$$
$$a^0 = e, \qquad a^{m+n} = a^m a^n, \qquad a^{mn} = (a^m)^n,$$

v G sú splnené pravidlá o krátení zľava aj sprava, t.j.

$$ab = ac \;\Rightarrow\; b = c, \qquad ac = bc \;\Rightarrow\; a = b,$$

a každá z rovníc $ax = b$, resp. $ya = b$ má v G jediné riešenie $x = a^{-1}b$, resp. $y = ba^{-1}$.

23.2. Podgrupy, generujúce množiny, cyklické grupy

Nech $(G,\cdot,e)$ je grupa. Hovoríme, že podmnožina $S\subseteq G$ je *podgrupa* grupy G, ak $e\in S$ a pre ľubovoľné $a,b\in S$ platí $ab\in S$ aj $a^{-1}\in S$. Inak povedané, podgrupa grupy G je jej podmnožina, ktorá obsahuje neutrálny prvok a je uzavretá vzhľadom na operácie súčinu a inverzného prvku v G. Zrejme každá podgrupa grupy G je zároveň sama grupou vzhľadom na grupovú operáciu zdedenú z G.

Pri overovaní, či daná pomnožina grupy je jej podgrupou, býva niekedy užitočné nasledujúce tvrdenie.

23.2.1. Tvrdenie. *Nech $(G,\cdot,e)$ je grupa a $S\subseteq G$. Potom S je podgrupa grupy G práve vtedy, keď $S\neq\emptyset$ a pre každé $a,b\in S$ platí $ab^{-1}\in S$.*

Dôkaz. Zrejme každá podgrupa grupy G je neprázdna a uzavretá vzhľadom na operáciu $(a,b)\mapsto ab^{-1}$. Naopak, nech $\emptyset\neq S\subseteq G$ je uzavretá na uvedenú operáciu a $s\in S$ je ľubovoľný prvok. Potom $e=ss^{-1}\in S$. Ďalej pre $a,b\in S$ platí $b^{-1}=eb^{-1}\in S$ a taktiež $ab=a(b^{-1})^{-1}\in S$. Teda S je podgrupa grupy G.

Pojem podgrupy danej grupy má niektoré spoločné črty s pojmom lineárneho podpriestoru daného vektorového priestoru: v oboch prípadoch ide o neprázdnu podmnožinu uzavretú vzhľadom na príslušné operácie. Navyše, lineárny podpriestor S vektorového priestoru V je zároveň aj podgrupou grupy $(V,+,\mathbf{0})$. Naopak, podgrupa S (aditívnej grupy) vektorového priestoru V je jeho lineárnym podpriestorom práve vtedy, keď je uzavretá aj vzhľadom na skalárne násobky.

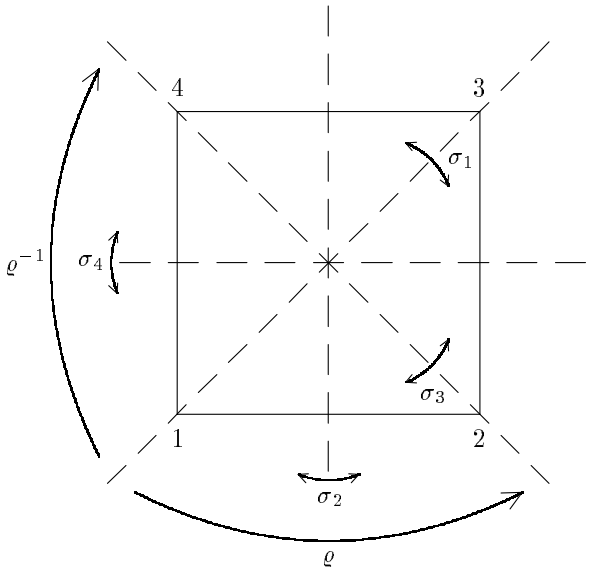
Každá grupa G obsahuje tzv. *triviálnu podgrupu* $\{e\}$ a *nevlastnú podgrupu* G. Pritom, okrem prípadu $G=\{e\}$, ide zrejme o dve rôzne podgrupy. V nasledujúcich príkladoch si ukážeme niekoľko dôležitých typov netriviálnych vlastných podgrúp, čím zároveň trochu rozšírime našu zatiaľ skromnú zbierku grúp.

23.2.2. Príklad. Nech $n\geq 3$ je prirodzené číslo. Označme ι identickú permutáciu množiny $\{1,\dots,n\}$ a ϱ cyklickú permutáciu $1\mapsto 2\mapsto\dots\mapsto n\mathop{\Leftrightarrow}1\mapsto n\mapsto 1$. Potom permutácie $\iota=\varrho^0$, $\varrho=\varrho^1$, $\dots$, ϱ^k, $\dots$, ϱ^{n-1} predstavujú otočenia (proti smeru hodinových ručičiek) pravidelného n-uholníka s vrcholmi $1,\dots,n$ o uhly $2k\pi/n$ pre $0\leq k\leq n\mathop{\Leftrightarrow}1$. Ak $n=2m$ je párne, tak pre $1\leq k\leq m$ označme σ_{2k-1} permutáciu n-uholníka zodpovedajúcu súmernosti podľa osi spájajúcej vrcholy k, $m+k$ a σ_{2k} permutáciu zodpovedajúcu súmernosti podľa osi strany $k\,k+1$ (a protiľahlej strany). Ak n je nepárne, tak σ_k pre $1\leq k\leq n$ označuje permutáciu zodpovedajúcu osovej súmernosti podľa spojnice vrchola k so stredom protiľahlej strany n-uholníka.

Prípad nepárneho $n=3$ je znázornený na obrázku v paragrafe 0.5 (kde zrejme $\varrho^{-1}=\varrho^2$). Obrázok na dalšej strane ukazuje situáciu pre párne $n=4$ (tentokrát $\varrho^{-1}=\varrho^3$).

Pre každé $n\geq 3$ tvorí množina $\{\iota,\varrho,\dots,\varrho^{n-1},\sigma_1,\dots,\sigma_n\}$ podgrupu symetrickej grupy $\mathcal{S}_n$. Označujeme ju Δ_n a nazývame *grupou symetrií pravidelného n-uholníka* alebo tiež *dihedrálnou grupou stupňa n*. Dihedrálna grupa Δ_n má rád $2n$ a okrem prípadu $n=3$, kedy $\Delta_3=\mathcal{S}_3$, je to netriválna vlastná podgrupa symetrickej grupy $\mathcal{S}_n$.

23.2.3. Príklad. Z vety 0.5.1 vyplýva, že množina všetkých párnych permutácií množiny $\{1,\dots,n\}$ tvorí podgrupu symetrickej grupy $\mathcal{S}_n$. Hovoríme jej *alternujúca grupa stupňa n* a značíme ju $\mathcal{A}_n$. Zrejme $\mathcal{A}_0=\mathcal{S}_0$, $\mathcal{A}_1=\mathcal{S}_1$, no pre $n\geq 2$ má $\mathcal{A}_n$ rád $n!/2$ (rozmyslite si prečo), teda je to vlastná (a pre $n\geq 3$ tiež netriviálna) podgrupa symetrickej grupy $\mathcal{S}_n$.



23.2.4. Príklad. Ako sme už spomínali, množina $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ tvorí grupu vzhľadom na násobenie. Z vlastností komplexných čísel možno ľahko nahliadnuť, že množina $\{z \in \mathbb{C};\ |z| = 1\}$ je jej podgrupou. Hovoríme jej *grupa komplexných jednotiek* (nepliesť si s jednotkou ako neutrálnym prvkom grupy) a z dôvodov, ktoré vysvitnú neskôr, ju značíme U(1). Zrejme U(1) je nekonečná vlastná podgrupa grupy $(\mathbb{C} \setminus \{0\}, \cdot)$.

Podobne ako vo vektorovom priestore V generuje ľubovoľná množina $X \subseteq V$ lineárny podpriestor $[X]$, každá podmnožina X grupy G generuje istú podgrupu grupy G, ktorú teraz opíšeme. Pre $X \subseteq G$ označme

$$\langle X \rangle = \left\{ x_1^{k_1} \dots x_n^{k_n};\ n \in \mathbb{N} \ \&\ k_1, \dots, k_n \in \mathbb{Z} \ \&\ x_1, \dots, x_n \in X \right\}.$$

Ak $X = \{x_1, \dots, x_m\}$ je konečná množina, tak miesto $\langle \{x_1, \dots, x_m\} \rangle$ píšeme len $\langle x_1, \dots, x_m \rangle$. Množinu $\langle X \rangle$ nazývame *podgrupa generovaná množinou* X. Tento názov je oprávnený nasledujúcim tvrdením.

23.2.5. Tvrdenie. *Nech X je podmnožina grupy G. Potom množina $\langle X \rangle$ je najmenšia podgrupa grupy G taká, že $X \subseteq \langle X \rangle$.*

Náčrt dôkazu. Podobne ako v tvrdení 4.2.1 pre vektorové priestory, možno i teraz ľahko dokázať, že

(a) $\langle X \rangle$ je podgrupa grupy G;

(b) pre každú podgrupu $S \subseteq G$ platí $X \subseteq S \Rightarrow \langle X \rangle \subseteq S$.

Ak $\langle X \rangle = G$, hovoríme, že *množina X generuje grupu G*, alebo, že X je *množinou generátorov grupy G*. Prvky množiny X potom nazývame *generátory grupy G*. *Grupa G* sa nazýva *konečne generovaná*, ak G má nejakú konečnú množinu generátorov.

Štruktúrne najjednoduchšími grupami sú tzv. *cyklické grupy*, t. j. grupy generované jediným generátorom. Príkladom cyklickej grupy je grupa $(\mathbb{Z}, +)$ všetkých celých čísel,

a taktiež grupy $(\mathbb{Z}_n, +)$ pre každé kladné celé číslo n. Každá z týchto grúp (okrem prípadu $n = 1$, kedy však $\mathbb{Z}_1 = \{0\} = \langle 0\rangle$) je totiž generovaná svojim prvkom 1.

Každý prvok x grupy G v nej generuje cyklickú podgrupu $\langle x\rangle$. Ak je konečná, tak jej rád $\#\langle x\rangle$ nazývame *rádom prvku* x v G; ak je nekonečná, hovoríme, že prvok $x \in G$ má *nekonečný rád*.

Nasledujúce tvrdenie by sme mohli dostať ako jednoduchý dôsledok našich neskorších úvah. Zámerne ho však dokážeme celkom elementárnymi, no o to názornejšími prostriedkami.

23.2.6. Tvrdenie. *Prvok x grupy G má konečný rád práve vtedy, keď existuje kladné celé číslo r také, že $x^r = e$. Rádom prvku x potom je najmenšie kladné celé číslo r s touto vlastnosťou a $\langle x\rangle = \{e, x, \dots, x^{r-1}\}$. Ak x má nekonečný rád, tak $\langle x\rangle = \{x^n;\ n \in \mathbb{Z}\}$, pričom $x^m \neq x^n$ pre všetky $m, n \in \mathbb{Z}$, $m \neq n$.*

Dôkaz. Vezmime $x \in G$ a uvažujme postupnosť mocnín $x^1 = x$, $x^2 = xx$, $x^3 = xxx$, atď. Všetky jej členy patria do podgrupy $\langle x\rangle$.

Pokiaľ x má konečný rád, t.j. $\langle x\rangle$ je konečná, musia sa v tejto postupnosti vyskytnúť aspoň dva rovnaké členy, napr. x^k a x^{k+r}, kde k a r sú kladné celé čísla. Potom však $x^k e = x^k = x^{k+r} = x^k x^r$, z čoho krátením zľava dostávame $e = x^r$. Ak r je najmenšie kladné celé číslo s touto vlastnosťou, tak všetky prvky $x^0 = e$, $x^1 = x$, $\dots$, x^{r-1} sú navzájom rôzne (rozmyliste si, prečo), a ďalšie mocniny sa už cyklicky opakujú: $x^r = e$, $x^{r+1} = x, \dots, x^{2r-1} = x^{r-1}$, atď. Ak si ešte uvedomíme, že pre $1 \leq k \leq r \Leftrightarrow 1$ potom platí $\left(x^k\right)^{-1} = x^{r-k}$, je jasné, že $\langle x\rangle = \{x^k;\ 0 \leq k \leq r \Leftrightarrow 1\}$.

Z prvej časti dôkazu je zrejmé, že ak $x \in G$ má nekonečný rád, tak všetky prvky uvažovanej nekonečnej postupnosti $x, x^2, \dots, x^n, \dots$ sú navzájom rôzne. Potom sa v nej nemôže vyskytnúť neutrálny prvok e. Navyše, žiadne dva z nich nemôžu byť navzájom inverzné. Teda $x^m \neq x^n$ pre navzájom rôzne $m, n \in \mathbb{Z}$ a $\langle x\rangle = \{x^n;\ n \in \mathbb{Z}\}$.

23.3. Homomorfizmy a izomorfizmy

Nech $(G, \cdot)$, $(H, \cdot)$ sú grupy. Zobrazenie $\varphi : G \to H$ sa nazýva *homomorfizmus grúp*, ak pre všetky $a, b \in G$ platí

$$\varphi(ab) = \varphi(a) \cdot \varphi(b).$$

Inak povedané, homomorfizmus je zobrazenie, ktoré zachováva operáciu súčinu v grupách. Nasledujúce tvrdenie ukazuje, že grupový homomorfizmus už nevyhnutne zachováva aj jednotku a operáciu inverzného prvku.

23.3.1. Tvrdenie. *Nech $\varphi : G \to H$ je homomorfizmus grúp. Potom $\varphi(e_G) = \varphi(e_H)$ a pre každé $a \in G$ platí $\varphi\left(a^{-1}\right) = \varphi(a)^{-1}$.*

Dôkaz. Čitateľ asi sám prišiel na to, že kvôli rozlíšeniu jednotiek v grupách G a H sme ich pre potreby tohto tvrdenia a jeho dôkazu označili e_G resp. e_H. S využitím vlastnosti homomorfizmu dostávame

$$\varphi(e_G) \cdot e_H = \varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G),$$

z čoho po krátení zľava vyplýva $e_H = \varphi(e_G)$.

Na dôkaz rovnosti $\varphi(a^{-1}) = \varphi(a)^{-1}$ stačí overiť, že $\varphi(a^{-1})$ sa správa ako inverzný prvok k prvku $\varphi(a)$, t.j. platí $\varphi(a) \cdot \varphi(a^{-1}) = e_H$. Vďaka vlastnosti homomorfizmu a už dokázanej prvej rovnosti nám vyjde

$$\varphi(a) \cdot \varphi(a^{-1}) = \varphi(aa^{-1}) = \varphi(e_G) = e_H.$$

Pre ľubovoľné dve grupy G, H je konštantné zobrazenie $x \mapsto e_H$, ktoré každému prvk $x \in G$ priradí jednotkový prvok grupy H, homomorfizmus grúp; nazývame ho *triválny homomorfizmus*. Čoskoro sa budeme mať možnosť zoznámiť aj s netriválnymi homomorfizmami.

Opäť sa stretáme so zrejmou analógiou spájajúcou pojmy lineárneho zobrazenia medzi vektorovými priestormi a homomorfizmu grúp: sú to zobrazenia medzi ich základnými množinami, ktoré zachovávajú príslušné operácie. Navyše, lineárne zobrazenie $\varphi\colon V \to U$ je zároveň homomorfizmus grúp $\varphi\colon (V,+) \to (U,+)$. Naopak, homomorfizmus $\varphi\colon (V,+) \to (U,+)$ aditívnych grúp vektorových priestorov V a U je lineárnym zobrazením práve vtedy, keď φ zachováva aj skalárne násobky.

Z toho dôvodu nie je potrebné uvádzať dôkazy zostávajúcich tvrdení tohto paragrafu. Čitateľ by si však mal samostatne premyslieť, ako ich dostane malými obmenami dôkazov príslušných tvrdení o lineárnych zobrazeniach, ktorých čísla mu na uľahčenie zakaždým uvedieme.

23.3.2. Tvrdenie. *Nech $\psi\colon F \to G$, $\varphi\colon G \to H$ sú homomorfizmy grúp. Potom aj ich kompozícia $\varphi \circ \psi\colon F \to H$ je homomorfizmus grúp.*

Dôkaz. Pozri tvrdenie 6.1.2.

23.3.3. Tvrdenie. *Nech $\varphi\colon G \to H$ je homomorfizmus grúp, $S \subseteq G$ je podgrupa grupy G a $T \subseteq H$ je podgrupa grupy H. Potom aj $\varphi(S) \subseteq H$ je podgrupa grupy H a $\varphi^{-1}(T) \subseteq G$ je podgrupa grupy G.*

Dôkaz. Pozri tvrdenie 6.1.3.

Nech $\varphi\colon G \to H$ je homomorfizmus grúp. Jeho *jadrom* resp. *obrazom* nazývame množinu

$$\operatorname{Ker}\varphi = \varphi^{-1}\{e_H\} = \{x \in G;\, \varphi(x) = e_H\},$$

resp.

$$\operatorname{Im}\varphi = \varphi(G) = \{\varphi(x);\, x \in G\}.$$

Ako bezprostredný dôsledok tvrdenia 23.3.3 (pozri tiež tvrdenie 6.2.1) dostávame

23.3.4. Tvrdenie. *Nech $\varphi\colon G \to H$ je homomorfizmus grúp. Potom* $\operatorname{Ker}\varphi$ *je podgrupa grupy G a* $\operatorname{Im}\varphi$ *je podgrupa grupy H.*

Podobne ako vo vete 6.2.2 pre lineárne zobrazenia, možno pomocou jadra a obrazu charakterizovať aj injektívnosť resp. surjektívnosť grupových homomorfizmov.

23.3.5. Tvrdenie. *Nech $\varphi\colon G \to H$ je homomorfizmus grúp. Potom*

(a) φ je injektívny práve vtedy, keď $\operatorname{Ker}\varphi = \{e_G\}$;

(b) φ je surjektívny práve vtedy, keď $\operatorname{Im}\varphi = H$.

Bijektívny homomorfizmus grúp $\varphi\colon G \to H$ nazývame *izomorfizmus grúp*. Hovoríme, že grupy G, H sú *izomorfné*, označenie $G \cong H$, ak existuje nejaký izomorfizmus $\varphi\colon G \to H$.

Zrejme injektívny homomorfizmus $\varphi\colon G \to H$ je zároveň izomorfizmom grupy G na podgrupu $\operatorname{Im}\varphi$ grupy H.

Aj pre grupové izomorfizmy platí obdoba tvrdenia 6.3.1 pre lineárne izomorfizmy.

23.3.6. Tvrdenie. *Nech F, G, H sú grupy.*

(a) $\mathrm{id}_G\colon G \to G$ *je izomorfizmus grúp.*

(b) Ak $\varphi\colon G \to H$ *je izomorfizmus grúp, tak aj inverzné zobrazenie* $\varphi^{-1}\colon H \to G$ *je izomorfizmus grúp.*

(c) Ak $\psi\colon F \to G$, $\varphi\colon G \to H$ *sú izomorfizmy grúp, tak aj* $\varphi \circ \psi\colon F \to H$ *je izomorfizmus grúp.*

V dôsledku toho pre ľubovoľné grupy F, G, H platí

$$G \cong G,$$
$$G \cong H \;\Rightarrow\; H \cong G,$$
$$F \cong G \;\&\; G \cong H \;\Rightarrow\; F \cong H.$$

Inak povedané, vzťah $\cong$ izomorfnosti grúp je *reflexívny*, *symetrický* a *tranzitívny*, teda je to vzťah *ekvivalencie*. Izomorfné grupy môžeme z hľadiska ich štruktúry považovať za totožné.

23.3.7. Príklad. Nech $(G, \cdot)$ je ľubovoľná grupa, $a \in G$. Keďže pre všetky $m, n \in \mathbb{Z}$ platí $a^{m+n} = a^m a^n$, znamená to, že predpisom $\varphi(n) = a^n$ je definovaný homomorfizmus $\varphi\colon (\mathbb{Z}, +) \to (G, \cdot)$. Zrejme $\operatorname{Im}\varphi = \langle a \rangle$ je cyklická podgrupa grupy G generovaná prvkom a. Ak a má konečný rád r, tak $\operatorname{Ker}\varphi = r\mathbb{Z} = \{rn;\, n \in \mathbb{Z}\}$; ak x má nekonečný rád, tak $\operatorname{Ker}\varphi = \{0\}$. Teda φ je surjektívne práve vtedy, keď $G = \langle a \rangle$, t.j. keď a generuje grupu G, a φ je injektívne práve vtedy, keď a má nekonečný rád.

23.3.8. Príklad. Pripomeňme, že $\boldsymbol{R}_\alpha = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \in \mathrm{GL}(2, \mathbb{R})$ je matica otočenia euklidovskej roviny $\mathbb{R}^2$ okolo počiatku o uhol α (pozri príklad 6.4.3). Keďže pre $\alpha, \beta \in \mathbb{R}$ platí známy vzťah $\boldsymbol{R}_\alpha \cdot \boldsymbol{R}_\beta = \boldsymbol{R}_{\alpha+\beta}$, znamená to, že priradením $\alpha \mapsto \boldsymbol{R}_\alpha$ je definovaný homomorfizmus grúp $\boldsymbol{R}\colon (\mathbb{R}, +) \to (\mathrm{GL}(2, \mathbb{R}), \cdot)$. Zrejme jadro $\operatorname{Ker}\boldsymbol{R} = 2\pi\mathbb{Z} = \{2k\pi;\, k \in \mathbb{Z}\} \subseteq \mathbb{R}$ tvorí podgrupa všetkých celočíselných násobkov čísla 2π a obraz $\operatorname{Im}\boldsymbol{R} = \{\boldsymbol{R}_\alpha;\, \alpha \in \mathbb{R}\} \subseteq \mathrm{GL}(2, \mathbb{R})$ je práve podgrupa všetkých matíc otočení $\boldsymbol{R}_\alpha$.

23.3.9. Príklad. Nech $0 < a \in \mathbb{R}$. Keďže $a^x > 0$ a $a^{x+y} = a^x a^y$ pre všetky $x, y \in \mathbb{R}$, je predpisom $\varphi(x) = a^x$ definovaný homomorfizmus grúp $\varphi\colon (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$. Ak $a = 1$, ide o triviálny homomorfizmus $\varphi(x) = 1$ pre každé $x \in \mathbb{R}$, teda $\operatorname{Ker}\varphi = \mathbb{R}$ a $\operatorname{Im}\varphi = \{1\}$. Pre $a \neq 1$ je to však bijektívny homomorfizmus, teda izomorfizmus. Inverzný izomofizmus $\varphi^{-1}\colon (\mathbb{R}^+, \cdot) \to (\mathbb{R}, +)$ je daný predpisom $\varphi^{-1}(u) = \log_a u$ pre $u \in \mathbb{R}^+$. Známa formula $\log_a uv = \log_a u + \log_a v$ pre $u, v \in \mathbb{R}^+$ nie je vlastne nič iné než vlastnosť homomorfizmu zobrazenia $u \mapsto \log_a u$.

Okrem iného sme práve dokázali, že aditívna grupa $(\mathbb{R}, +)$ a multiplikatívna grupa $(\mathbb{R}^+, \cdot)$ sú izomorfné.

23.3.10. Príklad. Exponenciála rýdzo imaginárneho čísla $\mathrm{i}x$, kde $x \in \mathbb{R}$, je definovaná Eulerovým vzťahom $\mathrm{e}^{\mathrm{i}x} = \cos x + \mathrm{i}\sin x$. Opäť platí $\mathrm{e}^{\mathrm{i}(x+y)} = \mathrm{e}^{\mathrm{i}x}\,\mathrm{e}^{\mathrm{i}y}$ pre všetky $x, y \in \mathbb{R}$. To znamená, že priradením $x \mapsto \mathrm{e}^{\mathrm{i}x}$ je definovaný homomorfizmus grúp $\varphi\colon (\mathbb{R}, +) \to (\mathbb{C}^\star, \cdot)$. Ľahko možno nahliadnuť, že $\operatorname{Ker}\varphi = 2\pi\mathbb{Z}$ a $\operatorname{Im}\varphi = \mathrm{U}(1)$.

23.4. Rozklad grupy podľa podgrupy, normálne podgrupy

Skôr než čitateľ pristúpi k štúdiu tohto a nasledujúceho paragrafu, mal by si zopakovať základné fakty o ekvivalenciách a rozkladoch z paragrafu 0.6.

Pre ľubovoľné podmnožiny X, Y grupy $(G, \cdot)$ označíme

$$XY = \{xy;\ x \in X\ \&\ y \in Y\}.$$

Miesto $X\{y\}$ píšeme len krátko Xy a miesto $\{x\}Y$ iba xY. V aditívnom zápise používame označenie $X + Y = \{x + y;\ x \in X\ \&\ y \in Y\}$, $X + y$ a $x + Y$.

Nech S je podgrupa grupy $(G, \cdot, e)$. Potom zrejme $x = ex \in Sx$, lebo $e \in S$. Navyše pre ľubovoľné $x, y \in G$ platí

$$Sx \cap Sy \neq \emptyset \ \Rightarrow\ Sx = Sy;$$

inak povedané množiny, Sx, Sy sú disjunktné alebo sa rovnajú. Ak totiž $z \in Sx \cap Sy$, tak existujú $s_1, s_2 \in S$ také, že $z = s_1 x = s_2 y$. Potom $x = s_1^{-1} s_2 y$, a každý prvok množiny Sx má pre vhodné $s \in S$ tvar $sx = ss_1^{-1}s_2 y \in Sy$, lebo – keďže $S \subseteq G$ je podgrupa – platí $ss_1^{-1}s_2 \in S$. Teda $Sx \subseteq Sy$ a obrátenú inklúziu možno dostať rovnako, zámenou úloh x a y. Tým sme dokázali prvú časť nasledujúceho tvrdenia.

23.4.1. Tvrdenie. *Nech S je podgrupa grupy G. Potom systém množín $\{Sx;\ x \in G\}$ tvorí rozklad grupy G. Prvky $x, y \in G$ patria do tej istej triedy tohto rozkladu práve vtedy, keď $xy^{-1} \in S$.*

Dôkaz. Zostáva dokázať už len druhú časť. Keďže uvedený systém množín je rozklad a $y \in Sy$, tak x a y patria do tej istej triedy rozkladu práve vtedy, keď $x \in Sy$, t.j. $x = sy$ pre nejaké $s \in S$. To je zrejme ekvivalentné s podmienkou $xy^{-1} = s \in S$

Množiny Sx, $x \in G$, sa nazývajú *ľavé triedy rozkladu grupy G podľa podgrupy S*. Reláciu ekvivalencie zodpovedajúcu tomuto rozkladu značíme $\equiv_S$ a môžeme ju vyjadriť nasledujúcimi piatimi ekvivalentnými spôsobmi:

$$\begin{aligned} x \equiv_S y \ &\Leftrightarrow\ xy^{-1} \in S \ \Leftrightarrow\ Sx = Sy \\ &\Leftrightarrow\ x \in Sy \ \Leftrightarrow\ y \in Sx \ \Leftrightarrow\ Sx \cap Sy \neq \emptyset. \end{aligned}$$

Príslušnú faktorovú množinu (t.j. vlastne rozklad) značíme

$$G/S = G/{\equiv_S} = \{Sx;\ x \in G\}.$$

Počet prvkov $\#(G/S)$ faktorovej množiny G/S (ak je konečná) nazývame *indexom podgrupy S* v grupe G a značíme ho tiež $[G : S]$; ak G/S je nekonečná, kladieme $[G : S] = \infty$ a hovoríme, že S má v G *nekonečný index*. Rád $\#\,G$ samotnej grupy G zrejme splýva s indexom $[G : e]$ jej triviálnej podgrupy $\{e\}$.

Analogicky možno zaviesť aj *pravé triedy rozkladu grupy G podľa podgrupy S*, t.j. množiny xS, $x \in G$, a dokázať pre ne obdobu tvrdenia 23.4.1.[1] Príslušnú reláciu ekvivalencie možno vyjadriť zodpovedajúcimi piatimi ekvivalentnými formulami:

$$\begin{aligned} x \,{}_S\!\equiv\, y \;&\Leftrightarrow\; x^{-1}y \in S \;\Leftrightarrow\; xS = yS \\ &\Leftrightarrow\; x \in yS \;\Leftrightarrow\; y \in xS \;\Leftrightarrow\; xS \cap yS \neq \emptyset. \end{aligned}$$

Taktiež rozklad grupy G na pravé triedy rozkladu podľa podgrupy S značíme rovnako

$$G/S = G/{}_S\!\equiv\, = \{xS;\, x \in G\};$$

ak je potrebné bližšie špecifikovať, či ide o rozklad na ľavé alebo pravé triedy, vyjadríme to väčšinou slovne.

Nech S je podgrupa grupy G a Sx, Sy sú ľubovoľné (nie nevyhnutne rôzne) ľavé triedy rozkladu G podľa S. Takpovediac na prstoch možno overiť, že predpisom $u \mapsto ux^{-1}y$ je definované bijektívne zobrazenie $Sx \to Sy$, ktoré prvok $u = sx \in Sx$ ($s \in S$) zobrazí na prvok $sy \in Sy$; k nemu inverzné zobrazenie $Sy \to Sx$ je dané predpisom $v \mapsto vy^{-1}x$, t.j. prvok $v = sy \in Sy$ ním prejde na prvok $sx \in Sx$. V prípade, že podgrupa S je konečná, to však znamená, že všetky ľavé (no rovnako aj pravé) triedy rozkladu G podľa S majú ten istý počet prvkov rovný rádu $\#S = [S : e]$ grupy $S = Se = eS$. Keďže G je zjednotením navzájom disjunktných, rovnako početných tried rozkladu $Sx \in G/S$ (prípadne xS), dokázali sme tým nasledujúcu vetu:

23.4.2. Veta. *(Lagrange) Nech S je podgrupa konečnej grupy G. Potom*

$$[G : e] = [G : S] \cdot [S : e],$$

teda rád aj index podgrupy S sú deliteľmi rádu grupy G.

Neskôr uvidíme, že pre daný deliteľ d rádu konečnej grupy G nemusí vždy existovať podgrupa grupy G rádu d (pozri cvičenie...).

23.4.3. Dôsledok. *(Malá veta Fermatova) Nech p je prvočíslo. Potom pre každé celé číslo x, ktoré nie je násobkom čísla p, platí*

$$x^{p-1} \equiv 1 \mod p,$$

t.j. číslo x^{p-1} dáva po delení číslom p zvyšok 1.

Dôkaz. Označme z zvyšok, ktorý dáva x po delení p. Keďže x nie je násobkom p, $z \in \mathbb{Z}_p^\star$, čo je multiplikatívna grupa (nenulových prvkov) poľa $\mathbb{Z}_p$ s rádom $p \Leftrightarrow 1$. Potom rád r jej cyklickej podgrupy $\langle z \rangle$ je deliteľom čísla $p \Leftrightarrow 1$, teda $p \Leftrightarrow 1 = rk$ pre nejaké kladné celé číslo k. Podľa tvrdenia 23.2.6 v grupe $(\mathbb{Z}_p^\star, \cdot, 1)$ platí $z^r = 1$, z čoho vyplýva

$$z^{p-1} = z^{rk} = (z^r)^k = 1^k = 1.$$

Teda z^{p-1} (teraz už ako prvok $\mathbb{Z}$) dáva po delení číslom p zvyšok 1. Avšak čísla z^{p-1} a x^{p-1} dávajú po delení číslom p rovnaký zvyšok (pozri cvičenie 16 z kapitoly 0).

[1] Používaná terminológia nie je v tomto smere jednotná. Niektorí autori nazývajú pravými triedami rozkladu grupy podľa podgrupy to, čo my nazývame ľavými triedami, a naopak.

Pre ľavú a pravú triedu rozkladu prvku x grupy G podľa jej podgrupy S môže vo všeobecnosti platiť $Sx \neq xS$. Napríklad rozklad dihedrálnej grupy $\Delta_3 = \mathcal{S}_3$ podľa cyklickej podgrupy $S = \langle \sigma_1 \rangle = \{\iota, \sigma_1\}$ na ľavé triedy tvoria množiny

$$S\iota = S\sigma_1 = \{\iota, \sigma_1\}, \qquad S\varrho = S\sigma_2 = \{\varrho, \sigma_2\}, \qquad S\varrho^{-1} = S\sigma_3 = \{\varrho^{-1}, \sigma_3\},$$

a rozklad na pravé triedy zasa množiny

$$\iota S = \sigma_1 S = \{\iota, \sigma_1\}, \qquad \varrho S = \sigma_3 S = \{\varrho, \sigma_3\}, \qquad \varrho^{-1} S = \sigma_2 S = \{\varrho^{-1}, \sigma_2\}.$$

(Overte pomocou multiplikatívnej tabuľky tejto grupy v paragrafe 0.5.)

Za istých dodatočných podmienok kladených na podgrupu S však ľavé a pravé triedy rozkladu G podľa S splývajú.

23.4.4. Tvrdenie. *Nech S je podgrupa grupy G. Potom nasledujúce podmienky sú ekvivalentné:*

(i) $(\forall\, x \in G)(\forall\, s \in S)\big(x^{-1}sx \in S\big)$;
(ii) $(\forall\, x \in G)\big(x^{-1}Sx = S\big)$;
(iii) $(\forall\, x \in G)(Sx = xS)$;
(iv) $(\forall\, x, y \in G)(x \equiv_S y \;\Leftrightarrow\; x \,{}_S\!\equiv y)$.

Dôkaz. (i) $\Rightarrow$ (ii) Z predpokladu (i) vyplýva inklúzia $x^{-1}Sx \subseteq S$. Jej prenásobením prvkom x zľava a prvkom x^{-1} sprava dostaneme inklúziu $S \subseteq xSx^{-1}$; keďže $x \in G$ je ľubovoľný prvok, substitúciou x^{-1} miesto x získame $S \subseteq x^{-1}Sx$. Teda $x^{-1}Sx = S$.

(ii) $\Rightarrow$ (iii) Stačí prenásobiť rovnosť $x^{-1}Sx = S$ prvkom x zľava.

(iii) $\Rightarrow$ (iv) Ak $Sx = xS$, tak

$$x \equiv_S y \;\Leftrightarrow\; y \in Sx \;\Leftrightarrow\; y \in xS \;\Leftrightarrow\; x \,{}_S\!\equiv y.$$

(iv) $\Rightarrow$ (i) Podľa predpokladu pre všetky $x, y \in G$ platí $xy^{-1} \in S \;\Leftrightarrow\; x^{-1}y \in S$. Keďže pre ľubovoľné $s \in S$ je $x(sx)^{-1} = s^{-1} \in S$, stačí položiť $y = sx$ a hneď máme $x^{-1}sx \in S$.

Hovoríme, že *podgrupa* S grupy G je *normálna* alebo tiež *invariantná*, označenie $S \lhd G$, ak spĺňa niektorú (teda všetky) z navzájom ekvivalentných podmienok tvrdenia 23.4.4. V prípade normálnych podgrúp teda nemusíme rozlišovať medzi ľavými a pravými triedami rozladu ani medzi ekvivalenciami $\equiv_S$ a ${}_S\!\equiv$.

V každej grupe G platí $\{e\} \lhd G$ a $G \lhd G$. Zrejme v abelovskej grupe G je každá podgrupa normálna. Ako sme však videli pred chvíľou, netriviálna vlastná podgrupa neabelovskej grupy už normálna byť nemusí.

Najdôležitejšími, a svojim spôsobom typickými príkladmi normálnych podgrúp sú jadrá grupových homomorfizmov.

23.4.5. Tvrdenie. *Nech $\varphi : G \to H$ je homomorfizmus grúp. Potom* $\operatorname{Ker}\varphi \lhd G$.

Dôkaz. Podľa tvrdenia 23.3.4 je $\operatorname{Ker}\varphi$ podgrupa grupy G. Overíme podmienku (i) tvrdenia 23.4.4, čím dokážeme jej normálnosť. Nech $a \in \operatorname{Ker}\varphi$, t. j. $\varphi(a) = e$, a $x \in G$ je ľubovoľný prvok. Potom

$$\varphi\big(x^{-1}ax\big) = \varphi\big(x^{-1}\big) \cdot \varphi(a) \cdot \varphi(x) = \varphi(x)^{-1} \cdot e \cdot \varphi(x) = e,$$

teda $x^{-1}ax \in \operatorname{Ker}\varphi$.

Každá podmnožina X grupy G generuje nielen najmenšiu podgrupu $\langle X\rangle \subseteq G$ takú, že $X \subseteq \langle X\rangle$, ale aj najmenšiu *normálnu* podgrupu $\langle\!\langle X\rangle\!\rangle \subseteq G$, ktorá obsahuje X. Množinu $\langle\!\langle X\rangle\!\rangle$ možno jednoducho popísať. Položme $X^{-1} = \{x^{-1};\, x \in X\}$, $\widehat{X} = \{gug^{-1};\, u \in X \cup X^{-1} \;\&\; g \in G\}$ a konečne

$$\langle\!\langle X\rangle\!\rangle = \langle \widehat{X}\rangle,$$

čiže $\langle\!\langle X\rangle\!\rangle$ je podgrupa generovaná množinou $\widehat{X}$. Jednoduchý dôkaz nasledujúceho tvrdenie prenechávame ako cvičenie čitateľovi.

23.4.6. Tvrdenie. *Nech G je grupa a $X \subseteq G$. Potom $\langle\!\langle X\rangle\!\rangle$ je najmenšia normálna podgrupa grupy G taká, že $X \subseteq \langle X\rangle\!\rangle$.*

Množinu $\langle\!\langle X\rangle\!\rangle$ teda môžeme oprávnene nazývať *normálna podgrupa grupy G generovaná množinou X*. Zrejme platí $\langle X\rangle \subseteq \langle\!\langle X\rangle\!\rangle$, a v abelovskej grupe G dokonca $\langle X\rangle = \langle\!\langle X\rangle\!\rangle$.

23.5. Faktorové grupy

V tomto paragrafe sa zoznámime s konštrukciou *faktorovej grupy*. Ide o dôležitý príklad všeobecnejšej konštrukcie *faktorovej štruktúry*, s ktorou sa možno stretnúť v najrôznejších oblastiach matematiky. S prvou základnou myšlienkou tejto konštrukcie sme sa už zbežne zoznámili v paragrafe 0.6 – spočíva v nazeraní prvkov faktorovej množiny $X/\!\sim$ množiny X podľa ekvivalencie $\sim$ nie ako množín (t.j. tried príslušného rozkladu) ale ako jednotlivých prvkov. Druhou kľúčovou myšlienkou spomínanej konštrukcie je *prenos štruktúry* z pôvodnej množiny X na faktorovú množinu $X/\!\sim$ pomocou kanonickej projekcie $X \to X/\!\sim$ danej priradením $x \mapsto \tilde{x}$. Túto všeobecnú myšlienku možno asi najjednoduchšie ilustrovať práve na konštrukcii faktorovej grupy.

Nech $(G, \cdot)$ je grupa a $\sim$ je ekvivalencia na množine G. Na faktorovej množine $G/\!\sim$ hodláme zaviesť binárnu operáciu $\cdot$ tak, aby $(G/\!\sim, \cdot)$ bola grupa a kanonická projekcia $G \to G/\!\sim$ homomorfizmus grúp. To znamená, že pre všetky $x, y \in G$ musí platiť

$$\tilde{x} \cdot \tilde{y} = \widetilde{xy},$$

Inak povedané, podmienka homomorfnosti kanonickej projekcie $x \mapsto \tilde{x}$ už jednoznačne určuje príslušnú binárnu operáciu na $G/\!\sim$.

Aby však takto bola *korektne* definovaná binárna operácia na množine $G/\!\sim$, jej výsledok nesmie závisieť na konkrétnych reprezentantoch x, y tried $\tilde{x}, \tilde{y} \in G/\!\sim$. Pre prvky $x_1, x_2, y_1, y_2 \in G$ také, že $\tilde{x}_1 = \tilde{x}_2$ a $\tilde{y}_1 = \tilde{y}_2$, t.j. $x_1 \sim x_2$ a $y_1 \sim y_2$, musí totiž platiť $\tilde{x}_1 \cdot \tilde{y}_1 = \tilde{x}_2 \cdot \tilde{y}_2$. Teda podľa našej definície

$$\widetilde{x_1y_1} = \tilde{x}_1 \cdot \tilde{y}_1 = \tilde{x}_2 \cdot \tilde{y}_2 = \widetilde{x_2y_2},$$

v dôsledku čoho $x_1y_1 \sim x_2y_2$.

Hovoríme, že ekvivalencia $\sim$ na grupe G je *kongruencia*, ak pre ľubovoľné prvky $x_1, x_2, y_1, y_2 \in G$ platí

$$x_1 \sim x_2 \;\&\; y_1 \sim y_2 \;\;\Rightarrow\;\; x_1y_1 \sim x_2y_2.$$

Krátko povedané, aby rovnosťou $\tilde{x} \cdot \tilde{y} = \widetilde{xy}$ bola korektne definovaná binárna operácia na faktorovej množine $G/\!\sim$, ekvivalencia $\sim$ musí byť *kongruenciou* na grupe G. Táto nevyhnutná podmienka je aj postačujúca na dosiahnutie nášho vopred stanoveného cieľa.

23.5.1. Veta. *Nech $\sim$ je kongruencia na grupe $(G,\cdot)$. Potom faktorová množina $G/\!\sim$ s binárnou operáciou $\tilde{x}\cdot\tilde{y}=\widetilde{xy}$ tvorí grupu, ktorej jednotkovým prvkom je $\tilde{e}$ a inverzným prvkom k prvku $\tilde{x}\in G/\!\sim$ je prvok $\tilde{x}^{-1}=\widetilde{x^{-1}}$. Navyše, prirodzená projekcia $G\to G/\!\sim$ je surjektívny homomorfizmus grúp.*

Dôkaz. Na dôkaz prvej časti tvrdenia stačí overiť, že pre ľubovoľné prvky $x,y,z\in G$ platí

$$\tilde{x}\cdot(\tilde{y}\cdot\tilde{z})=(\tilde{x}\cdot\tilde{y})\cdot\tilde{z},\qquad \tilde{e}\cdot\tilde{x}=\tilde{x}\cdot\tilde{e}=\tilde{x},\qquad \tilde{x}\cdot\widetilde{x^{-1}}=\widetilde{x^{-1}}\cdot\tilde{x}=\tilde{e}.$$

Príslušné jednoduché výpočty prenechávame ako cvičenie čitateľovi.

Zrejme prirodzená projekcia $G\to G/\!\sim$ je surjekcia. Už len stačí pripomenúť, že násobenie na množine $G/\!\sim$ bolo definované práve tak, aby zobrazenie $x\mapsto\tilde{x}$ bolo homomorfizmom.

Ukazuje sa, že kongruencie na grupách úzko súvisia s normálnymi podgrupami.

23.5.2. Tvrdenie. *Nech $(G,\cdot,e)$ je grupa.*

(a) Ak N je normálna podgrupa grupy G, tak ekvivalencia $\equiv_N$ je kongruenciou na grupe G.

(b) Ak $\sim$ je kongruencia na grupe G, tak $N=\tilde{e}$ je normálna podgrupa grupy G a pre všetky $x,y\in G$ platí

$$x\sim y\ \Leftrightarrow\ xy^{-1}\in N,$$

t.j. $\sim$ splýva s ekvivalenciou $\equiv_N$ rozkladu grupy G podľa N a pre $x\in G$ platí $\tilde{x}=Nx=xN$.

Inými slovami, kongruencie na grupách sú práve ekvivalenciami rozkladu podľa ich *normálnych podgrúp*.

Dôkaz. (a) Nech $N\lhd G$. Už vieme, že $\equiv_N$ je ekvivalencia na G. Zvoľme v G prvky $x_1\equiv_N x_2$, $y_1\equiv_N y_2$; ukážeme, že platí $x_1y_1\equiv_N x_2y_2$. Podľa predpokladu $x_1x_2^{-1}\in N$ a $y_1y_2^{-1}\in N$. Keďže N je normálna, platí $x_2\big(y_1y_2^{-1}\big)x_2^{-1}\in N$. Preto tiež

$$(x_1y_1)(x_2y_2)^{-1}=x_1\big(y_1y_2^{-1}\big)x_2^{-1}=\big(x_1x_2^{-1}\big)\big(x_2\big(y_1y_2^{-1}\big)x_2^{-1}\big)\in N,$$

teda $x_1y_1\equiv_N x_2y_2$, takže $\equiv_N$ je kongruencia na G.

(b) Nech $\sim$ je kongruencia na G. Podľa tvrdenia 23.5.1 je $x\mapsto\tilde{x}$ homomorfizmus grúp $G\to G/\!\sim$. Jeho jadrom je zrejme $N=\tilde{e}$. Podľa tvrdenia 23.4.5 potom $N\lhd G$.

Keďže $(G/\!\sim,\cdot)$ je grupa, pre $x,y\in G$ máme

$$x\sim y\ \Leftrightarrow\ \tilde{x}=\tilde{y}\ \Leftrightarrow\ \tilde{x}\cdot\tilde{y}^{-1}=\tilde{e}.$$

Nakoľko $x\mapsto\tilde{x}$ je homomorfizmus, platí $\tilde{x}\cdot\tilde{y}^{-1}=\big(xy^{-1}\big)^{\sim}$, preto tretia podmienka je zrejme ekvivalentná so vzťahom $xy^{-1}\in N$. Zvyšok je dôsledkom tvrdenia 23.4.4.

Grupu $G/\!\equiv_N$ nazývame *faktorovou grupou* grupy G podľa jej normálnej podgrupy N a značíme ju G/N. Násobenie v G/N je definované rovnosťou

$$Nx\cdot Ny=Nxy,$$

jednotkovým prvkom v G/N je $N=Ne$ a inverzným prvkom k $Nx\in G/N$ je $(Nx)^{-1}=Nx^{-1}$.

Prirodzená projekcia $\zeta_N\colon G\to G/N$, daná predpisom $\zeta_N(x)=Nx$ pre $x\in G$, je surjektívny homomorfizmus s jadrom $\operatorname{Ker}\zeta_N=N$. To dokazuje platnosť aj obrátenej implikácie k tvrdeniu 23.4.5.

23.5.3. Veta. *Podgrupa N grupy G je normálna práve vtedy, keď existuje homomorfizmus grúp $\varphi: G \to H$ taký, že $N = \operatorname{Ker}\varphi$.*

23.5.4. Veta. *(O homomorfizme) Nech $\varphi: G \to H$ je homomorfizmus grúp; označme $N = \operatorname{Ker}\varphi$. Potom predpisom $\varphi_*(Nx) = \varphi(x)$ je definovaný injektívny homomorfizmus grúp $\varphi_*: G/N \to H$. V dôsledku toho*

$$\operatorname{Im}\varphi \cong G/\operatorname{Ker}\varphi;$$

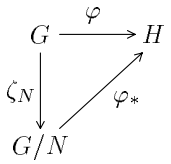
ak φ je navyše surjektívny homomorfizmus, tak $H \cong G/\operatorname{Ker}\varphi$.

Dôkaz. Pre $x, y \in G$ platí $Nx = Ny \Leftrightarrow \varphi(x) = \varphi(y)$. Implikácia $\Rightarrow$ zaručuje, že priradením $Nx \mapsto \varphi(x)$ je korektne definované zobrazenie $\varphi_*: G/N \to H$. Obrátená implikácia $\Leftarrow$ vyjadruje injektívnosť tohto zobrazenia. Priamočiary výpočet

$$\varphi_*(Nx \cdot Ny) = \varphi_*(Nxy) = \varphi(xy) = \varphi(x) \cdot \varphi(y) = \varphi_*(Nx) \cdot \varphi_*(Ny)$$

ukazuje, že ide o homomorfizmus. Druhá časť vety je bezprostredným dôsledkom prvej.

Uvedený homomorfizmus φ_* spĺňa podmienku $\varphi = \varphi_* \circ \zeta_N$, t.j. zabezpečuje komutatívnosť diagramu



Naopak, pokiaľ má zobrazenie $\varphi_*: G/N \to H$ vyhovovať tejto podmienke, musí byť nevyhnutne definované rovnosťou $\varphi_*(Nx) = \varphi(x)$.

Grupa H sa nazýva *homomorfným obrazom grupy* G, ak existuje surjektívny homomorfizmus $\varphi: G \to H$. Zrejme každá faktorová grupa grupy G je jej homomorfným obrazom. Ako vyplýva z vety o homomorfizme, tiež naopak, každý homomorfný obraz grupy G je izomorfný s faktorovou grupou G/N grupy G podľa niektorej jej normálnej podgrupy N. To znamená, že všetky homomorfné obrazy grupy G sú (až na izomorfizmus) skryte prítomné už v samotnej grupe G.

23.5.5. Príklad. Nech n je kladné celé číslo. Označme $\zeta_n(x)$ zvyšok po delení celého čísla x číslom n. Potom $\zeta_n: \mathbb{Z} \to \mathbb{Z}_n$ je homomorfizmus grúp (s operáciou $+$). Keďže ζ_n je surjektívny a $\operatorname{Ker}\zeta_n = n\mathbb{Z}$, podľa vety o homomorfizme platí $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Po stotožnení faktorovej grupy $\mathbb{Z}/n\mathbb{Z}$ s homomorfným obrazom $\mathbb{Z}_n = \zeta_n(\mathbb{Z})$ grupy $\mathbb{Z}$, danom uvedeným izomorfizmom, je každý prvok $x + n\mathbb{Z} = \{x + nk;\, k \in \mathbb{Z}\}$ faktorovej grupy $\mathbb{Z}/n\mathbb{Z}$, t.j. vlastne nekonečná trieda rozkladu podľa podgrupy $n\mathbb{Z} \subseteq \mathbb{Z}$, reprezentovaný ako *jediný prvok* $\zeta_n(x) \in \mathbb{Z}_n = \{0, 1, \ldots, n \Leftrightarrow 1\}$. Príslušná kongruencia $\equiv_{n\mathbb{Z}}$ zrejme splýva s kongruenciou $\equiv_n$ modulo n z cvičenia 16 z kapitoly 0.

23.5.6. Príklad. Z príkladu 23.3.8 vieme, že zobrazenie $\boldsymbol{R}: (\mathbb{R}, +) \to (\mathrm{GL}(2, \mathbb{R}), \cdot)$ je homomorfizmus grúp s jadrom $\operatorname{Ker}\boldsymbol{R} = 2\pi\mathbb{Z}$ a obrazom $\operatorname{Im}\boldsymbol{R} = \{\boldsymbol{R}_\alpha;\, \alpha \in \mathbb{R}\}$. Z príkladu 23.3.10 zasa vieme, že priradením $x \mapsto \mathrm{e}^{\mathrm{i}x}$ je definovaný homomorfizmus

grúp $(\mathbb{R},+) \to (\mathbb{C}^\star,\cdot)$ s rovnakým jadrom $2\pi\mathbb{Z}$ a s obrazom $\mathrm{U}(1) = \{\mathrm{e}^{\mathrm{i}x};\, x \in \mathbb{R}\} = \{z \in \mathbb{C};\, |z| = 1\}$. Z vety 23.5.4 tak okamžite vyplýva $\mathrm{Im}\,\boldsymbol{R} \cong \mathbb{R}/2\pi\mathbb{Z} \cong \mathrm{U}(1)$.

Práve izomorfizmus aditívnej faktorovej grupy $\mathbb{R}/2\pi\mathbb{Z}$ a jej homomorfného obrazu, multiplikatívnej grupy $\mathrm{U}(1)$, je pre pochopenie všeobecnej konštrukcie faktorovej grupy veľmi poučný. Faktorová množina $\mathbb{R}/2\pi\mathbb{Z}$ je ním reprezentovaná ako jednotková kružnica – názorne si môžeme predstaviť, že vznikla priložením bodu 0 reálnej osi $\mathbb{R}$ na bod 1 jednotkovej kružnice $\mathrm{U}(1) \subseteq \mathbb{C}$ a následným namotaním kladnej polosi proti a zápornej v smere hodinových ručičiek. Body $x, y \in \mathbb{R}$ sa pritom ocitnú v tom istom bode kružnice $\mathrm{U}(1)$ práve vtedy keď $x \Leftrightarrow y \in 2\pi\mathbb{Z}$, t.j. práve vtedy, keď $(x \Leftrightarrow y)/2\pi$ je celé číslo. Celá nekonečná trieda rozkladu $x + 2\pi\mathbb{Z} \in \mathbb{R}/2\pi\mathbb{Z}$ prvku $x \in \mathbb{R}$ podľa podgrupy $2\pi\mathbb{Z} \subseteq \mathbb{R}$ je tak reprezentovaná *jediným bodom* $\mathrm{e}^{\mathrm{i}x} = \cos x + \mathrm{i}\sin x$ kružnice $\mathrm{U}(1)$.

Konštrukcia faktorovej grupy pripúšťa tiež abstraktnejší popis pomocou tzv. krátkych exaktných postupností. Hovoríme že *postupnosť*

$$G_0 \overset{\varphi_1}{\leftrightarrows} G_1 \overset{\varphi_2}{\leftrightarrows} \quad \cdots \quad \overset{\varphi_{n-1}}{\leftrightarrows} G_{n-1} \overset{\varphi_n}{\leftrightarrows} G_n$$

grupových homomorfizmov je *exaktná*, ak pre každé $1 \le i < n$ platí

$$\mathrm{Im}\,\varphi_i = \mathrm{Ker}\,\varphi_{i+1}.$$

Podobne možno definovať pojem exaktnosti aj pre (na jednu či na obe strany) nekonečné postupnosti na seba nadväzujúcich grupových homomorfizmov. *Krátkou exaktnou postupnosťou* nazývame exaktnú postupnosť tvaru

$$\{e\} \overset{\eta}{\leftrightarrows} F \overset{\varphi}{\leftrightarrows} G \overset{\psi}{\leftrightarrows} H \overset{\tau}{\leftrightarrows} \{e\},$$

kde $\eta\colon \{e\} \to F$ a $\tau\colon H \to \{e\}$ sú triviálne homomorfizmy. Exaktnosť v člene F znamená, že $\mathrm{Ker}\,\varphi = \mathrm{Im}\,\eta = \{e_F\}$, čiže injektívnosť φ. Podobne, exaktnosť v člene H znamená, že $\mathrm{Im}\,\psi = \mathrm{Ker}\,\tau = H$, čiže surjektívnosť ψ. Konečne exaktnosť v strednom člene G znamená, že platí $\mathrm{Im}\,\varphi = \mathrm{Ker}\,\psi \lhd G$, z čoho vzhľadom na vetu o homomorfizme a surjektívnosť ψ vyplýva $G/\,\mathrm{Im}\,\varphi \cong H$.

Triviálna grupa $\{e\}$ na okrajoch, ako aj triviálne homomorfizmy η, τ sa zvyknú pri zápise krátkej exaktnej postupnosti vynechávať. Ak teda hovoríme o krátkej exaktnej postupnosti

$$F \overset{\varphi}{\rightarrowtail} G \overset{\psi}{\twoheadrightarrow} H,$$

znamená to, že φ je injektívny a ψ je surjektívny homomorfizmus grúp, pričom platí $\mathrm{Im}\,\varphi = \mathrm{Ker}\,\psi$. Injektívnosť φ resp. surjektívnosť ψ sa vyznačuje modifikovanými šípkami $\rightarrowtail$ resp. $\twoheadrightarrow$. Ak existuje krátka exaktná postupnosť $F \overset{\varphi}{\rightarrowtail} G \overset{\psi}{\twoheadrightarrow} H$, hovoríme, že stredná grupa G je *rozšírením grupy H pomocou grupy F*.

Paragraf uzatvárame zhrnutím úvah o krátkych exaktných postupnostiach a vety o homomorfizme do jedného celku.

23.5.7. Veta. *(a) Nech G je grupa a $N \lhd G$ je jej normálna podgrupa. Označme $\iota\colon N \to G$ vnorenie, t.j. identické zobrazenie N do G a $\zeta\colon G \to G/N$ kanonickú projekciu G na faktorovú grupu G/N. Potom $N \overset{\iota}{\rightarrowtail} G \overset{\zeta}{\twoheadrightarrow} G/N$ je krátka exaktná postupnosť homomorfizmov grúp.*

(b) Nech naopak $F \overset{\varphi}{\rightarrowtail} G \overset{\psi}{\twoheadrightarrow} H$ je krátka exaktná postupnosť homomorfizmov grúp. Označme $N = \mathrm{Im}\,\varphi = \mathrm{Ker}\,\psi$. Potom $F \cong N \lhd G$ a $H \cong G/N$.

23.6. Priamy súčin grúp

Konštrukcia priameho súčinu nám, spolu s konštrukciami podgrúp a faktorových grúp, umožňuje vytvárať z daných grúp nové. Taktiež naopak, niekedy nám umožňuje reprezentovať danú grupu v tvare priameho súčinu jednoduchších grúp, a tým sprehľadniť jej štruktúru. Opäť ide o špeciálny prípad veľmi dôležitej všeobecnej konštrukcie, ktorej pôsobnosť sa neobmedzuje len na teóriu grúp.

Priamym súčinom grúp $(G_1, \cdot, e_1)$, $(G_2, \cdot, e_2)$ nazývame karteziánsky súčin

$$G_1 \times G_2 = \{(x_1, x_2);\, x_1 \in G_1 \ \&\ x_2 \in G_2\},$$

množín G_1, G_2, s binárnou operáciou definovanou po zložkách, t.j.

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2)$$

pre $x_1, y_1 \in G_1$, $x_2, y_2 \in G_2$. Roznásobením zvlášť v každej zložke sa možno ľahko presvedčiť, že táto operácia na množine $G_1 \times G_2$ je asociatívna, má (e_1, e_2) za neutrálny prvok a inverzným prvkom k prvku $(x_1, x_2) \in G_1 \times G_2$ je $(x_1, x_2)^{-1} = \left(x_1^{-1}, x_2^{-1}\right)$. Tým sme vlastne dokázali nasledujúcu vetu.

23.6.1. Veta. *Priamy súčin $G_1 \times G_2$ grúp G_1, G_2 je grupa.*

Zovšeobecnenie konštrukcie priameho súčinu, ako aj vety 23.6.1 na ľubovoľný konečný počet grúp prenechávame čitateľovi.

Reprezentácia danej grupy G v tvare priameho súčinu $G \cong G_1 \times G_2$ prináša niečo nové, len ak sú obe grupy G_1, G_2 netriviálne. To nastoluje zaujímavý problém: rozložiť danú grupu G na priamy súčin dvoch netriviálnych grúp, t.j. nájsť netriválne grupy G_1 a G_2 tak, že platí $G \cong G_1 \times G_2$, prípadne ukázať, že také grupy neexistujú – v tom prípade hovoríme, že *grupa G* je *priamo nerozložiteľná*. Rozumnú charakterizáciu priamo nerozložiteľných grúp nemáme naporúdzi. Jednako uvedieme niekoľko jednoduchých podmienok, ktoré nám umožnia rozložiť niektoré známe grupy na priamy súčin v istom zmysle jednoduchších faktorov.

Najprv si všimnime, že projekcie $\pi_1 \colon G_1 \times G_2 \to G_1$, $\pi_2 \colon G_1 \times G_2 \to G_2$, dané predpismi $\pi_1(x_1, x_2) = x_1$, $\pi_2(x_1, x_2) = x_2$, sú surjektívne grupové homomorfizmy a pre ich jadrá platí

$$\operatorname{Ker} \pi_1 = \{e_1\} \times G_2 \cong G_2, \qquad \operatorname{Ker} \pi_2 = G_1 \times \{e_2\} \cong G_1;$$

príslušné izomorfizmy sú dané priradeniami $(e_1, x_2) \mapsto x_2$ resp. $(x_1, e_2) \mapsto x_1$. To znamená, že grupa $G_1 \times G_2$ obsahuje dve normálne podgrupy $N_1 \cong G_1$ a $N_2 \cong G_2$. Navyše $N_1 \cap N_2 = \{(e_1, e_2)\}$ a pre ľubovoľný prvok $(x_1, x_2) \in G_1 \times G_2$ platí

$$(x_1, x_2) = (x_1, e_2) \cdot (e_1, x_2) = (e_1, x_2) \cdot (x_1, e_2),$$

z čoho vyplývajú rovnosti $G = N_1 N_2 = N_2 N_1$.

23.6.2. Tvrdenie. *Nech $(G, \cdot)$ je grupa a $S, T \subseteq G$ sú jej podgrupy. Označme $\varphi \colon S \times T \to G$ zobrazenie dané predpisom $\varphi(x, y) = xy$ pre $x \in S$, $y \in T$. Potom*

(a) φ je homomorfizmus grúp práve vtedy, keď pre všetky $x \in S$, $y \in T$ platí $xy = yx$;

(b) φ *je injektívne práve vtedy, keď* $S \cap T = \{e\}$*;*
(c) φ *je surjektívne práve vtedy, keď* $G = ST$*.*

Dôkaz. (a) Predpokladajme, že φ je homomorfizmus. Potom pre ľubovoľné $x \in S$, $y \in T$ platí

$$xy = \varphi(x,y) = \varphi\big((e,y)\cdot(x,e)\big) = \varphi(e,y)\cdot\varphi(x,e) = (ey)(xe) = yx.$$

Nech naopak pre všetky $x \in S$, $y \in T$ platí $xy = yx$. Zvoľme $x_1, x_2 \in S$, $y_1, y_2 \in T$. Potom

$$\begin{aligned}\varphi\big((x_1,y_1)\cdot(x_2,y_2)\big) &= \varphi(x_1x_2, y_1y_2) = (x_1x_2)(y_1y_2)\\ &= (x_1y_1)(x_2y_2) = \varphi(x_1,y_1)\cdot\varphi(x_2,y_2),\end{aligned}$$

čo znamená, že φ je homomorfizmus.

(b) Predpokladajme, že platí $S \cap T = \{e\}$. Nech $(x_1,y_1),(x_2,y_2) \in S \times T$ sú také, že $\varphi(x_1,y_1) = \varphi(x_2,y_2)$. Potom $x_1y_1 = x_2y_2$, a keďže S, T sú podgrupy a $x_1, x_2 \in S$, $y_1, y_2 \in T$, platí $x_2^{-1}x_1 = y_2y_1^{-1} \in S \cap T$. Z toho vyplýva $x_2^{-1}x_1 = y_2y_1^{-1} = e$, teda $(x_1,y_1) = (x_2,y_2)$, čo dokazuje injektívnosť zobrazenia φ.

Nech naopak φ je injektívne. Potom pre $x \in S \cap T$ platí tiež $x^{-1} \in S \cap T$, lebo $S \cap T$ je podgrupa grupy G. Preto $\big(x, x^{-1}\big) \in S \times T$ a

$$\varphi\big(x, x^{-1}\big) = xx^{-1} = e = \varphi(e,e).$$

Vďaka injektívnosti φ z toho vyplýva $x = e = x^{-1}$. Teda $S \cap T = \{e\}$.

(c) platí triviálne.

23.6.3. Dôsledok. *Nech* G *je grupa a* S, $T \lhd G$ *sú jej dve normálne podgrupy také, že* $S \cap T = \{e\}$ *a* $G = ST$*. Potom* $G \cong S \times T$*.*

Dôkaz. Stačí overiť, že za uvedených predpokladov je splnená aj podmienka (a) predchádzajúceho tvrdenia, čiže pre všetky $x \in S$, $y \in T$ platí $xy = yx$. Potom totiž priradenie $(x,y) \mapsto xy$ bude izomorfizmus grúp $S \times T \cong G$. Keďže S, $T \lhd G$, platí $yx^{-1}y^{-1} \in S$, $xyx^{-1} \in T$ a

$$x \cdot yx^{-1}y^{-1} = xyx^{-1}\cdot y^{-1} \in S \cap T,$$

teda $xyx^{-1}y^{-1} = e$, z čoho už vyplýva požadovaná rovnosť.

Nasleduje niekoľko aplikácií čerstvo dokázaných výsledkov.

23.6.4. Tvrdenie. *Nech* m, n *sú kladné celé čísla. Potom cyklická aditívna grupa* $\mathbb{Z}_{mn}$ *je izomorfná s priamym súčinom* $\mathbb{Z}_m \times \mathbb{Z}_n$ *cyklických aditívych grúp* $\mathbb{Z}_m$ *a* $\mathbb{Z}_n$ *práve vtedy, keď* m *a* n *sú nesúdeliteľné.*

Dôkaz. Nech m, n sú nesúdeliteľné. Označme S, T podmnožiny množiny $\mathbb{Z}_{mn}$ pozostávajúce z čísel deliteľných číslom n resp. m. Zrejme S aj T sú podgrupy grupy $\mathbb{Z}_{mn}$ a platí $\mathbb{Z}_m \cong S = \{0, n, 2n, \ldots, (m \Leftrightarrow 1)n\}$, $\mathbb{Z}_n \cong T = \{0, m, 2m \ldots, (n \Leftrightarrow 1)m\}$. Keďže grupa $\mathbb{Z}_{mn}$ je komutatívna, rovnosť $x + y = y + x$ platí pre všetky $x, y \in \mathbb{Z}_{mn}$, a nielen pre $x \in S$, $y \in T$. Z nesúdeliteľnosti m a n vyplýva $S \cap T = \{0\}$. Podľa

častí (a), (b) tvrdenia 23.6.2 je predpisom $(x,y) \mapsto x+y$ definovaný injektívny homomorfizmus grúp $S \times T \to \mathbb{Z}_{mn}$. Keďže množina S má m prvkov a množina T má n prvkov, je to injekcia mn-prvkovej množiny $S \times T$ do množiny $\mathbb{Z}_{mn}$ s rovnakým počtom prvkov, teda zároveň surjekcia. Môžeme uzavrieť, že uvedené zobrazenie je izomorfizmus grúp, preto platí

$$\mathbb{Z}_{mn} \cong S \times T \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Nech naopak m, n sú súdeliteľné s najväčším spoločným deliteľom $d > 1$. Potom m/d, n/d aj $k = mn/d < mn$ sú celé čísla. Pre každý prvok (x,y) grupy $\mathbb{Z}_m \times \mathbb{Z}_n$ platí

$$k(x,y) = (kx, ky) = \left(\frac{n}{d}\, mx, \frac{m}{d}\, ny\right) = (0,0),$$

lebo $mx = 0$ v $\mathbb{Z}_m$ a $ny = 0$ v $\mathbb{Z}_n$ (výrazy ako kz označujú súčet k exemplárov prvku z v príslušnej grupe). To znamená, že rád každého prvku tejto grupy je nanajvýš k, teda ostro menší než mn. Z toho dôvodu, podľa tvrdenia 23.2.6, $\mathbb{Z}_m \times \mathbb{Z}_n$ nemôže byť izomorfná s cyklickou grupou rádu mn.

Poznámka. Metódami do istej miery podobnými niektorým metódam z kapitoly 21 možno dokázať, že každá konečne generovaná abelovská grupa je izomorfná s priamym súčinom konečného počtu cyklických grúp. V dôsledku toho je každá konečná abelovská grupa izomorfná s priamym súčinom $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_k}$ pre vhodné kladné celé čísla $n_1, \ldots, n_k$. Čísla $n_1, \ldots, n_k$ možno navyše vybrať tak, že každé z nich je mocninou nejakého prvočísla (primárny kanonický tvar), prípadne tak, že každé z nich je násobkom nasledujúceho (racionálny kanonický tvar). Tieto výsledky však už výrazne presahujú rámec nášho kurzu.

Nasledujúce jednoduché dôsledky vety 23.6.4 nám poslúžia pri dôkaze záverečného tvrdenia.

23.6.5. Dôsledok. *V ľubovoľnej grupe $(G,\cdot)$ platí:*

(a) Ak prvky $x, y \in G$ komutujú, t.j. $xy = yx$, a majú konečné po dvoch nesúdeliteľné rády m resp. n, tak prvok xy má rád mn.

(b) Ak prvok $x \in G$ má konečný rád mn, kde m, n sú navzájom nesúdeliteľné kladné celé čísla, tak existujú prvky $u, v \in \langle x\rangle$ rádov m resp. n také, že $x = uv$.

(c) Ak prvky $x, y \in G$ komutujú a majú konečné rády m resp. n, tak existuje prvok $z \in \langle x, y\rangle$, ktorého rád je najmenším spoločným násobkom čísel m a n.

Dôkaz. (a) Rád prvku $xy \in \langle x,y\rangle \cong \langle x\rangle \times \langle y\rangle$ je zrejme rovnaký ako rád prvku $(1,1) \in \mathbb{Z}_m \times \mathbb{Z}_n$.

(b) Cyklická podgrupa $\langle x\rangle$ grupy G je izomorfná s priamym súčinom $\mathbb{Z}_m \times \mathbb{Z}_n$; nech $\varphi\colon \mathbb{Z}_m \times \mathbb{Z}_n \to \langle x\rangle$ je nejaký izomorfizmus a $(a,b) = \varphi^{-1}(x)$. Potom rád prvku $a \in \mathbb{Z}_m$ je m a rád prvku $b \in \mathbb{Z}_n$ je n (rozmyslite si prečo). Stačí položiť $u = \varphi(a,0)$, $v = \varphi(0,b)$.

(c) Nech $m = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, $n = p_1^{\beta_1} \ldots p_k^{\beta_k}$, kde $p_1, \ldots, p_k$ sú navzájom rôzne prvočísla a $\alpha_i, \beta_i \in \mathbb{N}$. Keďže pre $i \neq j$ sú čísla $p_i^{\alpha_i}$, $p_j^{\alpha_j}$ navzájom nesúdeliteľné, podľa (b) (ktoré možno indukciou zovšeobecniť na ľubovoľný konečný počet činiteľov) existujú prvky $u_1, \ldots, u_k \in \langle x\rangle$ také, že $x = u_1 \ldots u_k$ a u_i má rád $p_i^{\alpha_i}$. Z rovnakého dôvodu existujú prvky $v_1, \ldots, v_k \in \langle y\rangle$ také, že $y = v_1 \ldots v_k$ a v_i má rád $p_i^{\beta_i}$. Zrejme ľubovoľné

dva z prvkov $u_1, \ldots, u_k, v_1, \ldots, v_k$ komutujú. Položme $w_i = u_i$, ak $\alpha_i \geq \beta_i$ a $w_i = v_i$, ak $\alpha_i < \beta_i$. Podľa (a) (ktoré možno takisto zovšeobecniť indukciou na ľubovoľný konečný počet činiteľov) rád prvku $z = w_1 \ldots w_k$ je $p_1^{\gamma_1} \ldots p_k^{\gamma_k}$, kde $\gamma_i = \max(\alpha_i, \beta_i)$, čiže najmenší spoločný násobok čísel m a n.

Taktiež časť (c) uvedeného dôsledku možno indukciou zovšeobecniť na ľubovoľný konečný počet po dvoch komutujúcich prvkov grupy. Jeden špeciálny prípad tohto zovšeobecnenia si zaslúži našu pozornosť.

23.6.6. Dôsledok. *Nech G je konečná abelovská grupa. Potom existuje prvok $z \in G$, ktorého rád je násobkom rádu každého prvku grupy G.*

Nasledujúca veta odhaľuje zaujímavú súvislosť medzi štruktúrou polí a konečných cyklických grúp.

23.6.7. Veta. *Nech K je ľubovoľné pole. Potom každá konečná podgrupa multiplikatívnej grupy $K^\star$ jeho nenulových prvkov je cyklická.*

Dôkaz. Nech G je konečná podgrupa grupy $K^\star$. Podľa dôsledku 23.6.6 existuje prvok $z \in G$, ktorého rád $n = \# \langle z \rangle$ je násobkom rádu každého prvku grupy G. Potom n delí rád $\# G$, teda $n \leq \# G$, a pre každé $a \in G$ platí $a^n = 1$. Inak povedané, každý prvok grupy G je koreňom polynómu $x^n \Leftrightarrow 1 \in K[x]$. Ale, ako sme sa už zmienili v úvode paragrafu 19.1, polynóm n-tého stupňa má v poli K najviac n koreňov (dokonca vrátane násobnosti). Preto musí platiť $\# G \leq n$, teda $\# G = n$ a $G = \langle z \rangle$ je cyklická.

23.6.8. Dôsledok. *Nech K je konečné pole. Potom multiplikatívna grupa $K^\star$ jeho nenulových prvkov je cyklická.*

Ešte poznamenajme, že generátor cyklickej multiplikatívnej grupy $K^\star$ konečného q-prvkového poľa K sa nazýva $(q \Leftrightarrow 1)$*-á primitívna odmocnina z jednotky.* Takýto prvok má totiž rád $q \Leftrightarrow 1$, t.j. vyhovuje rovnici $x^{q-1} = 1$, ale žiadnej z rovníc $x^k = 1$ pre $1 \leq k < q \Leftrightarrow 1$.

23.7. Voľné a konečne prezentované grupy

Nech X je ľubovoľná množina. Zamyslime sa nad otázkou, ako vyzerá „najvšeobecnejšia“ grupa generovaná množinou X. Predovšetkým treba upresniť, čo vlastne znamená ono „najvšeobecnejšia“. Označme F túto zatiaľ bližšie neurčenú grupu. Vieme, že $X \subseteq F = \langle X \rangle$. Podľa našich predstáv by v grupe F nemali platiť „žiadne vzťahy navyše“ okrem tých, ktoré sú nevyhnutnými logickými dôsledkami axióm (a), (b), (c) teórie grúp, uvedených na začiatku paragrafu 23.1.

Grupa F by teda okrem prvkov množiny X mala obsahovať aj nejaký (jediný) neutrálny prvok e, a keďže nás nič nenúti, aby pre nejaké $x \in X$ platilo $x = e$, tento prvok by mal byť rôzny od každého prvku $x \in X$. S každým prvkom $x \in X$ by F mala obsahovať aj k nemu inverzný prvok x^{-1}, ktorý by mal byť z rovnakého dôvodu rôzny od každého prvku $y \in X$ aj od prvku e. Na druhej strane, axiómy teórie grúp nás nútia položiť $e^{-1} = e$ a $(x^{-1})^{-1} = x$. Pôvodná množina X sa nám tak rozrástla do zjednotenia po dvoch disjunktných množín X, $\{e\}$ a $X^{-1} = \{x^{-1}; x \in X\}$.

Grupa F však musí byť uzavretá aj vzhľadom na súčiny, teda musí popri prvku e obsahovať aj všetky výrazu tvaru $s_1 s_2 \ldots s_n$, kde $1 \leq n \in \mathbb{N}$ a $s_1, \ldots, s_n \in X \cup X^{-1}$. Zátvorky si môžeme dovoliť vynechať, lebo v dôsledku asociatívnosti grupy F ich

umiestnenie nemá vplyv na výsledok. Keď sa však v takomto „slove“ vyskytnú vedľa seba „písmená“ x a x^{-1}, je nevyhnutné ich navzájom vykrátiť a takto pokračovať, pokiaľ sa to len dá. Napr. zo slova $u^{-1}uxxyz^{-1}zy^{-1}zu^{-1}$, kde $x, y, z, u \in X$, tak najprv dostaneme $xxyy^{-1}zu^{-1}$ a potom $xxzu^{-1}$.

Ukážeme, že do množiny F netreba ďalej nič pridávať. Ak sa navyše dohodneme, že prvok e stotožníme s prázdnou postupnosťou prvkov množiny $X \cup X^{-1}$, máme

$$F = \big\{s_1 \dots s_n;\, n \in \mathbb{N} \,\&\, s_1, \dots, s_n \in X \cup X^{-1} \,\&\, (\forall\, i < n)(s_i^{-1} \neq s_{i+1})\big\}.$$

Prvky množiny F nazývame *redukované grupové slová nad abecedou* X.

Súčin redukovaných slov $r_1 \dots r_m$, $s_1 \dots s_n$ definujeme v dvoch krokoch: Najprv ich jednoducho napíšeme za sebou, t.j. utvoríme slovo $r_1 \dots r_m s_1 \dots s_n$, a potom ho zredukujeme podľa skôr spomínaného receptu.

Ľahko nahliadneme, že takto definovaná operácia násobenia je asociatívna. Prázdne slovo e je naozaj redukované a je jej neutrálnym prvkom. Inverzným prvkom k redukovanému slovu $s_1 \dots s_n$ je redukované slovo $s_n^{-1} \dots s_1^{-1}$, lebo redukciou zloženého slova $s_1 \dots s_n s_n^{-1} \dots s_1^{-1}$ zrejme dostaneme prázdne slovo e. Krátko povedané, množina F s práve definovanou operáciou tvorí grupu. Nazývame ju *voľná grupa* nad množinou generátorov X a prvkom množiny X hovoríme *voľné generátory*. Aby sme zvýraznili ich úlohu, používame označenie $F = \mathrm{FG}(X)$ (z anglického *free group*).

Voľné grupy však možno charakterizovať aj iným, abstraktným spôsobom.

23.7.1. Veta. *Nech X je množina a G je ľubovoľná grupa. Potom ku každému zobrazeniu $f\colon X \to G$ existuje práve jeden homomorfizmus $\varphi\colon \mathrm{FG}(X) \to G$ taký, že $\varphi \restriction X = f$, t.j. $\varphi(x) = f(x)$ pre každé $x \in X$. Naopak, ak nejaká grupa F má tiež uvedenú vlastnosť, t.j. $X \subseteq F$ a ku každému zobrazeniu $g\colon X \to G$ existuje jediný homomorfizmus grúp $\psi\colon F \to G$ taký, že $\psi \restriction X = g$, tak $F \cong \mathrm{FG}(X)$.*

Dôkaz. Nech $f\colon X \to G$ je nejaké zobrazenie z množiny X do grupy G. Ak má byť $\varphi\colon \mathrm{FG}(X) \to G$ homomorfizmus rozširujúci f, tak pre každé (redukované) slovo $x_1^{\alpha_1} \dots x_n^{\alpha_n} \in \mathrm{FG}(X)$, kde $x_1, \dots, x_n \in X$ a $\alpha_i \in \{1, \Leftrightarrow 1\}$, musí platiť

$$\varphi\big(x_1^{\alpha_1} \dots x_n^{\alpha_n}\big) = \varphi(x_1)^{\alpha_1} \dots \varphi(x_n)^{\alpha_n} = f(x_1)^{\alpha_1} \dots f(x_n)^{\alpha_n},$$

teda φ možno definovať len jediným spôsobom. Naopak, ľahko nahliadneme, že uvedeným predpisom je naozaj definovaný homomorfizmus grúp rozširujúci f.

Predpokladajme, že $F \supseteq X$ je grupa a ku každému zobrazeniu $g\colon X \to G$ do ľubovoľnej grupy G existuje jediný homomorfizmus $\psi\colon X \to G$ rozširujúci g. Uvažujme identitu id_X ako zobrazenie $X \to F$ aj ako zobrazenie $X \to \mathrm{FG}(X)$. Existuje jediný homomorfizmus $\varphi\colon \mathrm{FG}(X) \to F$ rozširujúci id_X a taktiež jediný taký homomorfizmus $\psi\colon F \to \mathrm{FG}(X)$. Potom aj $\varphi \circ \psi\colon F \to F$ je homomorfizmus rozširujúci id_X, rovnako ako $\psi \circ \varphi\colon \mathrm{FG}(X) \to \mathrm{FG}(X)$. Preto nevyhnutne $\varphi \circ \psi = \mathrm{id}_F$ a $\psi \circ \varphi = \mathrm{id}_{\mathrm{FG}(X)}$, teda φ, ψ sú navzájom inverzné izomorfizmy.

Uvedená vlastnosť voľných grúp pripomína vektorové priestory. Aj tie sú „voľné nad svojimi bázami“. Ak totiž X je (neusporiadaná) báza vektorového priestoru V nad poľom K, tak každé zobrazenie $f\colon X \to U$ do nejakého vektorového priestoru U možno jediným spôsobom rozšíriť do lineárneho zobrazenia $\varphi\colon V \to U$. Zrejme φ

zobrazí lineárnu kombináciu $c_1x_1 + \ldots + c_nx_n$, kde $x_1, \ldots, x_n \in X$, $c_1, \ldots, c_n \in K$ do lineárnej kombinácie

$$\varphi(c_1x_1 + \ldots + c_nx_n) = c_1f(x_1) + \ldots + c_nf(x_n).$$

No na rozdiel od vektorových priestorov, zďaleka nie všetky grupy, dokonca ani tie konečne generované, nie sú voľné. Jednako – ako ukazuje nasledujúca veta – voľné grupy sú v istom zmysle predobrazmi všetkých grúp.

23.7.2. Veta. *Každá grupa je homomorfným obrazom nejakej voľnej grupy.*

Dôkaz. Nech G je ľubovovoľná grupa a $X \subseteq G$ je nejaká množina jej generátorov (vždy môžeme položiť napr. $X = G$). Nech $F = \mathrm{FG}(X)$ je voľná grupa nad množinou X. Uvažujme identitu id_X ako zobrazenie $\mathrm{id}_X : X \to G$. Podľa predchádzajúcej vety existuje (dokonca jediný) homomorfizmus grúp $\varphi : F \to G$ taký, že $\varphi(x) = x$ pre všetky $x \in X$. Keďže X generuje G, φ je zrejme surjekcia.

Napríklad voľná grupa s jedným generátorom x je zrejme nekonečná cyklická grupa, teda $(\mathrm{FG}(x), \cdot) \cong (\mathbb{Z}, +)$. Podľa vety 23.3.1 je každý homormofizmus $\mathbb{Z} \to G$ jednoznačne určený obrazom jej generátora $1 \in \mathbb{Z}$, ktorým môže byť každý prvok grupy G. Homomorfné obrazy grupy $\mathbb{Z}$ – grupy $\mathbb{Z}_n$, kde $2 \leq n \in \mathbb{N}$, – však voľné nie sú. Voľné grupy s viac než jedným generátorom už nie sú komutatívne a majú podstatne zložitejšiu štruktúru.

Nech $X \subseteq G$ je nejaká množina, ktorá generuje grupu G. Uvažujme (jednoznačne určený) surjektívny homomorfizmus $\varphi : \mathrm{FG}(X) \to G$ rozširujúci identické zobrazenie $\mathrm{id}_X : X \to G$. Potom jeho jadro $N = \mathrm{Ker}\,\varphi$ je normálna podgrupa voľnej grupy $\mathrm{FG}(X)$. Ľubovoľný prvok $s_1 \ldots s_n \in N$ predpisuje rovnosť $s_1 \ldots s_n = e$, ktorá musí platiť v grupe G. Ak napr. $xyx^{-1}y^{-1} \in N$, znamená to v G platí $xyx^{-1}y^{-1} = e$, t.j. generátory $x, y \in X$ komutujú. Podobne, ak $xxx \in N$, tak v G platí $x^3 = e$, t.j. generátor x má rád 3, prípadne 1. Keby sme vypísali všetky slová, ktoré sú prvkami grupy N, dostali by sme tak zoznam všetkých redukovaných grupových slov nad abecedou X, ktoré sa v grupe G rovnajú neutrálnemu prvku e. Keďže každú rovnosť medzi slovami $r_1 \ldots r_m = s_1 \ldots s_n$ možno prepísať na ekvivalentný tvar $r_1 \ldots r_m s_n^{-1} \ldots s_1^{-1} = e$, grupa N tak v sebe skrýva všetky možné rovnosti medzi (redukovanými) grupovými slovami nad abecedou X ktoré platia v G.

Aby sme však mohli popísať grupu $G \cong \mathrm{FG}(X)/N$, nepotrebujeme explicitne poznať všetky rovnosti $s_1 \ldots s_n = e$ spomínaného tvaru, ktoré platia v G. Stačí mať k dispozícii nejaký menší zoznam takých rovností, z ktorých všetky ostatné rovnosti v G logicky vyplývajú. Inak povedané, nepotrebujeme zoznam všetkých prvkov grupy $N \lhd \mathrm{FG}(X)$, stačí nejaká jej podmnožina $E \subseteq N$, taká, že $\langle\!\langle E \rangle\!\rangle = N$. Potom rovnosť $r_1 \ldots r_m = s_1 \ldots s_n$ platí v G práve vtedy, keď vyplýva z množiny rovností E, t.j. práve vtedy, keď $r_1 \ldots r_m s_n^{-1} \ldots s_1^{-1} \in \langle\!\langle E \rangle\!\rangle$.

Faktorovú grupu $\mathrm{FG}(X)/\langle\!\langle E \rangle\!\rangle$ značíme $\langle X \mid E \rangle$ a nazývame ju *grupa prezentovaná množinou generátorov X a množinou slov E*. $\langle X \mid E \rangle$ tak predstavuje "najvšeobecnejšiu" grupu generovanú množinou X, v ktorej platia rovnosti $s_1 \ldots s_n = e$, kde $s_1 \ldots s_n \in E$. Akákoľvek iná rovnosť medzi slovami zostavenými z generátorov (t.j. z prvkov množiny X) v nej platí, len ak je logickým dôsledkom rovností z E a axióm teórie grúp – inak nie. Špeciálne $\mathrm{FG}(X) = \langle X \mid \emptyset \rangle$.

Niekedy slová $w \in E$ zapisujeme ako rovnosti $w = e$, prípadne slová tvaru $uv^{-1} \in E$ ako rovnosti $u = v$. Napr.

$$\langle x \mid x^n \rangle = \langle x \mid x^n = e \rangle,$$

predstavuje cyklickú grupu rádu n, teda izomorfnú s aditívnou grupou $\mathbb{Z}_n$. Podobne

$$\langle x, y \mid xyx^{-1}y^{-1} \rangle = \langle x, y \mid xy = yx \rangle$$

predstavuje "voľnú abelovskú grupu" s dvoma generátormi. Možno ukázať, že je izomorfná s priamym súčinom $\mathbb{Z} \times \mathbb{Z}$.

Grupy tvaru $\langle X \mid E \rangle$, kde X aj $E \subseteq \mathrm{FG}(X)$ sú *konečné* množiny, nazývame *konečne prezentované grupy*. Ak $X = \{x_1, \ldots, x_n\}$, $E = \{w_1, \ldots, w_k\}$, píšeme

$$\langle X \mid E \rangle = \langle x_1, \ldots, x_n \mid w_1, \ldots, w_k \rangle.$$

Zrejme každá konečná grupa je konečne prezentovaná (rozmyslite si prečo). Ako sme však videli pred chvíľou, konečne prezentovaná grupa môže byť nekonečná.

Prezentácie grúp hrajú dôležitú úlohu pri popise na nich definovaných homomorfizmov.

23.7.3. Veta. *Nech $\langle X \mid E \rangle$ je prezentácia grupy G a H je ľubovoľná grupa. Potom zobrazenie $f : X \to H$ možno rozšíriť do homomorfizmu $\varphi : G \to H$ práve vtedy, keď pre každé $s_1 \ldots s_n \in E$ platí $f(s_1) \ldots f(s_n) = e_H$. V tom prípade je homomorfizmus φ rozširujúci f určený jednoznačne.*

Dôkaz. Zrejme jediný možný spôsob ako definovať φ, je položiť

$$\varphi\big(x_1^{k_1} \ldots x_n^{k_n}\big) = \varphi(x_1)^{k_1} \ldots \varphi(x_n)^{k_n} = f(x_1)^{k_1} \ldots f(x_n)^{k_n}$$

pre $x_1, \ldots, x_n \in X$, $k_1, \ldots, k_n \in \mathbb{Z}$. Ľahko možno overiť, že takto definované zobrazenie je homomorfizmus grúp práve vtedy, keď $f(s_1) \ldots f(s_n) = e_H$ pre každé $s_1 \ldots s_n \in E$.

Ak si napríklad uvedomíme, že $\mathbb{Z}_n \cong \langle x \mid x^n \rangle$, pričom úlohu generátora x hrá prvok $1 \in \mathbb{Z}_n$, hneď vidíme, že priradenie $1 \mapsto a \in H$ možno rozšíriť do homomorfizmu grúp $\varphi : \mathbb{Z}_n \to H$ práve vtedy, keď v H platí $a^n = e$, čiže rád prvku a je deliteľom čísla n. Taktiež naopak, každý homomorfizmus $\varphi : \mathbb{Z}_n \to H$ je jednoznačne určený obrazom $a = \varphi(1)$ jediného prvku $1 \in \mathbb{Z}_n$. Úlohu prvku 1 môže samozrejme zohrať ľubovoľný generátor cyklickej grupy $\mathbb{Z}_n$, t. j. ľubovoľný prvok $k \in \mathbb{Z}_n$ nesúdeliteľný s n.

23.7.4. Príklad. *Metacyklickou grupou* nazývame konečne prezentovanú grupu tvaru

$$F_{mn}^k = \langle x, y \mid x^m = y^n = e,\ xyx^{-1} = y^k \rangle,$$

kde m, n sú prirodzené čísla a $k \in \mathbb{Z}_n$ je nesúdeliteľné s n také, že $k^m \equiv_n 1$. Pripúšťame aj prípady $m = 0$ alebo $n = 0$; vtedy kladieme $\mathbb{Z}_0 = \mathbb{Z}$, navyše podmienka nesúdeliteľnosti $k \in \mathbb{Z}$ s $n = 0$ znamená $k = \pm 1$. Grupy F_{mn}^k patria do širšej triedy grúp nazývaných *Frobeniovými grupami*.

Ukážeme, že každý prvok grupy F_{mn}^k má tvar $y^b x^a$ pre jednoznačne určené $a \in \mathbb{Z}_m$, $b \in \mathbb{Z}_n$. Uvedená prezentácia totiž umožňuje vypočítať všetky súčiny $y^b x^a \cdot y^d x^c$ a previesť ich na súčin vhodných mocnín generátorov y a x. Ak si totiž uvedomíme, že pre

prvky ľubovoľnej grupy platí $gug^{-1}\cdot gvg^{-1}=guvg^{-1}$ a $(gh)u(gh)^{-1}=g(huh^{-1})g^{-1}$, môžeme počítať

$$y^bx^a\cdot y^dx^c=y^b\cdot x^ay^dx^{-a}\cdot x^{a+c}=y^b(x^ayx^{-a})^dx^{a+c}=y^by^{k^ad}x^{a+c}=y^{b+k^ad}x^{a+c},$$

lebo $xyx^{-1}=y^k$, $x^2yx^{-2}=xy^kx^{-1}=(xyx^{-1})^k=(y^k)^k=y^{k^2}$, ..., $x^ayx^{-a}=y^{k^a}$.

Pre $m=2$, $k=n\Leftrightarrow 1$ dostávame dihedrálnu grupu Δ_n z príkladu 23.2.2. Keďže pre generátor y rádu n je $y^{n-1}=y^{-1}$, môžeme jej prezentáciu prepísať do obvyklej podoby

$$\Delta_n\cong\langle x,y\mid x^2=y^n=e,\ xyx^{-1}=y^{-1}\rangle.$$

Zrejme v uvedenej prezentácii zodpovedá generátor x osovej súmernosti podľa niektorej z osí pravidelného n-uholníka a y otočeniu okolo jeho stredu o uhol $2\pi/n$.

23.7.5. Príklad. Nech p, q sú ľubovoľné prvočísla. Keďže podľa dôsledku 23.6.8 multiplikatívna grupa $\mathbb{Z}_q^\star$ poľa $\mathbb{Z}_q$ je cyklická rádu $q\Leftrightarrow 1$, prvok $k\in\mathbb{Z}_q^\star$ rádu p (t.j. $k\in\mathbb{Z}_q$, $k^p\equiv_q 1$ a $k\neq 1$) existuje práve vtedy, keď p delí $q\Leftrightarrow 1$. V takom prípade $p<q$ a

$$F_{pq}^k=\langle x,y\mid x^p=y^q=e,\ xyx^{-1}=y^k\rangle$$

je nekomutatívna grupa rádu pq. Ukážeme, že metacyklická grupa F_{pq}^k nezávisí na k; presnejšie, ak $l\in\mathbb{Z}_q^\star$ je iný prvok rádu p, tak $F_{pq}^k\cong F_{pq}^l$.

Množina $A=\{a\in\mathbb{Z}_q^\star;\ a^p=1\}$ tvorí cyklickú podgrupu grupy $\mathbb{Z}_q^\star$ rádu p, preto $l\in A=\langle k\rangle$. Teda existuje $1\leq r\leq p\Leftrightarrow 1$ také, že v $\mathbb{Z}_q$ platí $l=k^r$, čiže $l\equiv_q k^r$. Potom pre $z=x^r\in F_{pq}^k$ máme $\langle z\rangle=\langle x\rangle$, $z^p=e$ a

$$zyz^{-1}=x^ryx^{-r}=y^{k^r}=y^l.$$

To však podľa vety 23.7.3 znamená, že priradenie $x\mapsto x^r$, $y\mapsto y$ možno rozšíriť do homomorfizmu grupy

$$F_{pq}^l=\langle x,y\mid x^p=y^q=e,\ xyx^{-1}=y^l\rangle$$

do grupy F_{pq}^k. Čitateľ by si mal samostatne premyslieť, že ide naozaj o izomorfizmus.