24. GRUPY TRANSFORMÁCIÍ

V tejto kapitole si trochu bližšie všimneme niektoré typy grúp transformácií. Nebudeme sa však systematicky venovať ich štúdiu. Začneme dôkazom tzv. Cayleyho vety o reprezentácií, podľa ktorej je každá grupa izomorfná s nejakou grupou transformácií, a sústredíme sa najmä na využitie tohto faktu pri štúdiu abstraktných grúp. Uvidíme, že práve reprezentácie abstraktných grúp ako grúp transformácií konkrétnych množín, často vybavených dodatočnou štruktúrou, sú veľmi účinným nástrojom, ktorý nám umožňuje hlbšie preniknúť do štruktúry pôvodných grúp a jasnejšie osvetliť ich stavbu.

Ani v tomto smere však nebudeme postupovať príliš ďaleko. Uspokojíme sa s vybudovaním niekoľkých základných pojmov a techník, ktoré využijeme v nasledujúcej kapitole venovanej maticovým grupám, a týmito elementárnymi prostriedkami sa pokúsime zodpovedať niektoré prirodzené otázky, ktoré by pri štúdiu tejto a predchádzajúcej kapitoly mohli či – lepšie povedané – mali napadnúť zvedavého čitateľa.

24.1. Cayleyho veta o reprezentácii

Nech X je ľubovoľná množina. Každú podgrupu $G \subseteq \mathcal{S}(X)$ grupy všetkých permutácií množiny X nazývame *grupou transformácií množiny* X. Hovoríme, že G je *grupa transformácií*, ak G je grupou transformácií nejakej množiny.

Zrejme všetky prvky ľubovoľnej grupy transformácií sú *bijektívne* transformácie príslušnej množiny. Podľa uvedenej definície je množina $G \subseteq \mathcal{S}(X)$ grupou transformácií množiny X práve vtedy, keď $\mathrm{id}_X \in G$ a pre všetky $f, g \in G$ platí $f \circ g \in G$ a $f^{-1} \in G$, t. j. G je uzavretá vzhľadom na kompozíciu zobrazení a s každým zobrazením obsahuje aj k nemu inverzné zobrazenie.

Ukazuje sa, že grupy transformácií, až na izomorfizmus, zahŕňajú vôbec všetky grupy. Inak povedané, každú abstraktnú grupu $(G, \cdot)$ možno reprezentovať konkrétnym spôsobom ako grupu transformácií nejakej množiny X a jej grupovú operáciu skladaním zobrazení.

24.1.1. Veta. *(Cayley) Každá grupa je izomorfná s nejakou grupou transformácií.*

Dôkaz. Vlastne stačí k danej grupe G nájsť nejakú vhodnú množinu X a injektívny homomorfizmus grúp $\Phi\colon G \to \mathcal{S}(X)$. Podľa vety 23.5.4 o homomorfizme G je potom izomorfná s grupou transformácií $\mathrm{Im}\Phi \subseteq \mathcal{S}(X)$.

Zvoľme $X = G$ a pre $g \in G$, $x \in X$ položme $\Phi_g(x) = gx$. Inak povedané, pre $g \in G$ je $\Phi_g\colon X \to X$ zobrazenie dané priradením $x \mapsto gx$. Každé zobrazenie Φ_g je zrejme bijektívne, s inverzným zobrazením $\Phi_g^{-1} = \Phi_{g^{-1}}\colon x \mapsto g^{-1}x$, takže $\Phi\colon G \to \mathcal{S}(X)$.

Dokážeme, že Φ je homomorfizmus grúp, t. j. $\Phi_{gh} = \Phi_g \circ \Phi_h$ pre všetky $g, h \in G$. Nato stačí overiť, že uvedené dve zobrazenia dávajú rovnaké výsledky pre každé $x \in X$:

$$\Phi_{gh}(x) = (gh)x = g(hx) = \Phi_g(\Phi_h(x)) = (\Phi_g \circ \Phi_h)(x).$$

Na dôkaz injektívnosti homomorfizmu Φ sa stačí presvedčiť, že má triválne jadro. Ak $g \in \mathrm{Ker}\,\Phi$, tak $\Phi_g = \mathrm{id}_X$, preto $gx = \Phi_g(x) = \mathrm{id}_X(x) = x$ pre všetky $x \in X$. Voľbou $x = e$ dostávame $g = ge = e$, teda $\mathrm{Ker}\,\Phi = \{e\}$.

24.1.2. Príklad. Nech $(V,+)$ je aditívna grupa nejakého vektorového priestoru (nad ľubovoľným poľom K). Pre každé $\boldsymbol{u} \in V$ označme $\Phi_{\boldsymbol{u}}\colon V \to V$ zobrazenie dané priradením $\boldsymbol{x} \mapsto \boldsymbol{x}+\boldsymbol{u}$ pre $\boldsymbol{x} \in V$, t.j. posunutie (transláciu) o vektor $\boldsymbol{u}$. Zrejme každé posunutie $\Phi_{\boldsymbol{u}}$ je bijektívne zobrazenie (k nemu inverzné zobrazenie je posunutie o vektor $\Leftrightarrow\boldsymbol{u}$) a pre $\boldsymbol{u},\boldsymbol{v} \in V$ platí $\Phi_{\boldsymbol{u}+\boldsymbol{v}} = \Phi_{\boldsymbol{u}} \circ \Phi_{\boldsymbol{v}}$. Inak povedané, zložením posunutí o vektory $\boldsymbol{u}$ a $\boldsymbol{v}$ dostaneme posunutie o vektor $\boldsymbol{u}+\boldsymbol{v}$. Samozrejme, identickým zobrazením $\mathrm{id}_V : V \to V$ je jedine posunutie $\Phi_{\boldsymbol{0}}$ o nulový vektor $\boldsymbol{0}$. $\Phi\colon (V,+) \to (\mathcal{S}(V),\circ)$ je tak injektívny grupový homomorfizmus a $(V,+)$ je izomorfná s grupou $\mathrm{Im}\Phi \subseteq \mathcal{S}(V)$ všetkých posunutí priestoru V.

Výslovne upozorňujeme, že – napriek dojmu, ktorý by snáď mohol navodiť dôkaz vety 24.1.1 a príklad 24.1.2, – zďaleka nie pre každý injektívny homomorfizmus grúp $\Phi\colon G \to \mathcal{S}(X)$ musí množina X splývať so základnou množinou grupy G.

24.2. Akcie a reprezentácie grúp

Niektoré metódy, ktoré sa vyskytli v dôkaze Cayleyho vety, stoja za podrobnejšie preskúmanie vo všeobecnej polohe.

Nech $(G,\cdot,e)$ je grupa a X je ľubovoľná množina.

(a) *Akciou grupy G na množine X* nazývame binárnu operáciu $\cdot\colon G \times X \to X$, ktorá spĺňa podmienky

$$ex = x \qquad \text{a} \qquad g(hx) = (gh)x$$

pre ľubovoľné $g,h \in G$, $x \in X$. Uvedený typ akcie presnejšie nazývame *ľavou akciou grupy G na množine X*. Analogicky možno definovať aj *pravú akciu* $\cdot\colon X \times G \to X$ *grupy G na množine X*; formuláciu príslušných podmienok prenechávame čitateľovi.

(b) *Reprezentáciou grupy G v množine X* nazývame ľubovoľný grupový homomorfizmus $\Phi\colon G \to \mathcal{S}(X)$. Keďže pre $g \in G$ je samotné $\Phi(g)\colon X \to X$ zobrazenie, budeme miesto $\Phi(g)$ dávať prednosť zápisu Φ_g; podmienka homomorfnosti Φ má potom tvar rovnosti $\Phi_{gh} = \Phi_g \circ \Phi_h$ pre všetky $g,h \in G$.

Rozdiel medzi pojmami akcie a reprezentácie je čisto formálny, sú to len dva mierne odlišné spôsoby ako hovoriť o tom istom. Ak je daná akcia $\cdot\colon G \times X \to X$, tak každé $g \in G$ určuje predpisom $\Phi_g(x) = gx$ bijekciu $\Phi_g \in \mathcal{S}(X)$; k nej inverzná bijekcia je daná prepisom $\Phi_{g^{-1}}(x) = g^{-1}x$. Zobrazenie $\Phi\colon G \to \mathcal{S}(X)$ je potom reprezentáciou grupy G v mmožine X. Z vlastností akcie totiž vyplýva podmienka homomorfnosti Φ:

$$\Phi_{gh}(x) = (gh)x = g(hx) = \Phi_g(\Phi_h(x)) = (\Phi_g \circ \Phi_h)(x),$$

pre všetky $g,h \in G$, $x \in X$. Naopak, každá reprezentácia $\Phi\colon G \to \mathcal{S}(X)$ určuje predpisom $gx = \Phi_g(x)$ akciu $\cdot\colon G \times X \to X$. Dôvody sú podobné: na dôkaz podmienky $g(hx) = (gh)x$ stačí prepísať uvedené rovnosti v mierne pozmenenom poradí; podmienka $ex = x$ vyplýva z vlastnosti reprezentácie $\Phi_e = \mathrm{id}_X$.

Nech grupa G má akciu na množine X. *Orbitou prvku $x \in X$* (vzhľadom na túto akciu) naývame množinu

$$Gx = \{gx;\, g \in G\}.$$

Podobne ako v paragrafe 23.4, i teraz možno ľahko nahliadnuť, že pre ľubovoľné $x,y \in X$ platí $x = ex \in Gx$ a

$$Gx \cap Gy \neq \emptyset \;\Leftrightarrow\; Gx = Gy.$$

Z toho vyplýva, že systém orbít všetkých prvkov grupy G tvorí rozklad množiny X; hovoríme mu *orbitálny rozklad množiny* X a značíme ho X/G. K nemu prislúchajúcu ekvivalenciu možno vyjadriť nasledujúcimi štyrmi ekvivalentnými spôsobmi:

$$x \equiv_G y \;\Leftrightarrow\; Gx = Gy \;\Leftrightarrow\; x \in Gy \;\Leftrightarrow\; y \in Gx \;\Leftrightarrow\; Gx \cap Gy \neq \emptyset.$$

Hovoríme, že *množina* $T \subseteq X$ je *transverzálna*, ak $\#\,(Gx \cap T) = 1$ pre každé $x \in X$, t.j. T obsahuje z každej orbity $Gx \in X/G$ práve jedného reprezentanta.

Stabilizátorom prvku $x \in X$ nazývame množinu

$$\mathrm{Stb}(x) = \{g \in G;\, gx = x\}.$$

Ľahko sa možno presvedčiť, že stabilizátor $\mathrm{Stb}(x)$ je dokonca podgrupou grupy G. Podobne nazývame

$$\mathrm{Fix}(g) = \{x \in G;\, gx = x\}$$

množinou pevných bodov, prípadne *množinou fixpunktov* prvku $g \in G$. Zrejme pre $g = e$ máme $\mathrm{Fix}(e) = X$.

Nasledujúce dva výsledky dávajú do súvisu práve zavedené pojmy.

24.2.1. Veta. *Nech grupa G má akciu na množine X. Potom pre každé $x \in X$ je predpisom $g\,\mathrm{Stb}(x) \mapsto gx$ korektne definované bijektívne zobrazenie $G/\mathrm{Stb}(x) \to Gx$ medzi množinou pravých tried rozkladu grupy G podľa stabilizátora $\mathrm{Stb}(x)$ a orbitou Gx. Ak G alebo X je konečná, tak to znamená, že*

$$\#\,Gx = [G : \mathrm{Stb}(x)].$$

Ak X je konečná, tak navyše pre každú transverzálnu množinu $T \subseteq X$ platí

$$\#X = \sum_{x \in T} [G : \mathrm{Stb}(x)].$$

Dôkaz. Označme $S = \mathrm{Stb}(x)$. Predpisom $g \mapsto gx$ je zrejme definované surjektívne zobrazenie $G \to Gx$. Pre všetky $g, h \in G$ pritom platí

$$gx = hx \;\Leftrightarrow\; x = g^{-1}hx \;\Leftrightarrow\; g^{-1}h \in S \;\Leftrightarrow\; gS = hS.$$

To znamená, že predpisom $gS \mapsto gx$ je naozaj korektne definované bijektívne zobrazenie $G/S \to Gx$. To dokazuje prvú rovnosť. Keďže množina X je zjednotením po dvoch disjunktných orbít Gx, $x \in T$, druhá rovnosť je dôsledkom prvej.

Podľa tejto vety sa počet prvkov orbity Gx ľubovoľného prvku $x \in X$ sa rovná indexu jeho stabilizátora $\mathrm{Stb}(x)$ v grupe G. Ak G je konečná, tak z toho podľa Lagrangeovej vety 23.4.2 vyplýva rovnosť $\mathrm{Stb}(x) = (\#\,G)/(\#\,Gx)$, v dôsledku čoho majú všetky stabilizátory prvkov tej istej orbity rovnaký rád. Neskôr uvidíme, že tieto stabilizátory sú dokonca izomorfné (pozri cvičenie...). Ešte poznamenajme, že druhá z rovností vety 24.2.1 sa občas zvykne nazývať *rovnosť tried*.

Ďalšia veta, známa pod názvom *Burnsideova lema*, vyjadruje počet orbít akcie ako aritmetický priemer počtov fixpunktov jednotlivých prvkov grupy. Ako vzápätí uvidíme Burnsideova lema je zovšeobecnením Lagrangeovej vety 23.4.2.

24.2.2. Veta. *Nech G je konečná grupa, ktorá má akciu na konečnej množine X. Potom*

$$\#\,(X/G) = \frac{1}{\#\,G}\sum_{g\in G} \#\,\mathrm{Fix}(g).$$

Dôkaz. Počet prvkov množiny $R = \{(g,x) \in G \times X;\, gx = x\}$ spočítame dvoma spôsobmi. Zrejme platí

$$\#R = \sum_{g\in G} \#\,\mathrm{Fix}(g) = \sum_{x\in X} \#\,\mathrm{Stb}(x).$$

S využitím predchádzajúceho tvrdenia a faktu, že X je zjednotením po dvoch disjunktných orbít $\omega \in X/G$, z toho dostaneme

$$\sum_{g\in G} \#\,\mathrm{Fix}(g) = \sum_{x\in X} \#\,\mathrm{Stb}(x) = \sum_{x\in X} \frac{\#\,G}{\#\,Gx} = \sum_{\omega\in X/G}\ \sum_{x\in\omega} \frac{\#\,G}{\#\,\omega} = \#\,(X/G)\cdot \#\,G.$$

S príkladom reprezentácie sme sa už stretli v predchádzajúcom paragrafe, v dôkaze vety 23.1.1. Tam zostrojené zobrazenie $\Phi : G \to \mathcal{S}(X)$ bolo injektívnou reprezentáciou grupy G v množine $X = G$. To je tiež dôvod, prečo uvedený výsledok nazývame Cayleyho veta *o reprezentácii*. Trochu všeobecnejšiu situáciu si teraz preberieme v reči akcií.

24.2.3. Príklad. Nech G je grupa a H je jej podgrupa. Potom grupa H má na množine G *ľavú akciu transláciou* $H\times G \to G$ danú priradením $(h,x) \mapsto hx$ pre $h \in H$, $x \in G$, ako aj *pravú akciu transláciou* $G \times H \to G$ danú priradením $(x,h) \mapsto xh$.

Orbitou prvku $x \in G$ v ľavej akcii transláciou je práve ľavá trieda rozkladu Hx prvku x podľa podgrupy H; jeho orbitou v pravej akcii transláciou je zasa pravá trieda rozkladu xH podľa podgrupy H. Označenie G/H množiny všetkých orbít (ľavej resp. pravej) akcie podgrupy H transláciou si tak zachováva svoj predošlý význam z paragrafu 23.4 množiny (ľavých resp. pravých) rozkladových tried grupy G podľa podgrupy H.

Ďalej sa sústreďme len na ľavú akciu podgrupy H na grupe G. Zrejme každé $x \in G$ má triviálny stabilizátor $\mathrm{Stb}(x) = \{e\}$, a taktiež množina pevných bodov každého $h \in H \setminus \{e\}$ je prázdna, čiže $\mathrm{Fix}(h) = \emptyset$; pre $h = e$ samozrejme $\mathrm{Fix}(e) = G$. Prvá časť vety 24.2.1 v tomto kontexte hovorí, že podgrupu $H \cong H/\{e\}$ možno prirodzeným spôsobom vzájomne jednoznačne zobraziť na každú orbitu (ľavú triedu rozkladu) Hx. Podobne, Burnsideova lema splýva v tomto prípade s Lagrangeovou vetou, podľa ktorej $\#(G/H) = (\#\,G)/(\#\,H)$.

Poznámka o značení. V literatúre sa možno stretnúť so značne rôznorodým označením akcií, orbít, stabilizátorov a pod. Napr. výsledok akcie prvku $g \in G$ na prvok $x \in X$ sa často značí ako „mocnina“ x^g a orbita prvku x ako $x^G = \{x^g;\, g \in G\}$. Tento zápis je vhodný najmä pre pravú akciu grupy $(G,\cdot,1)$ na množine X, kedy definujúce podmienky akcie nadobúdajú tvar $x^1 = x$ a $(x^g)^h = x^{gh}$. Bežné označenie stabilizátora prvku $x \in X$ v akcii grupy G je G_x. Orbita prvku x sa občas značí $\mathrm{Orb}(x)$.

24.3. Grupy automorfizmov a konjugácia

Niektoré reprezentácie Φ grupy G v množine X môžu mať isté vlastnosti navyše – jednotlivé zobrazenia Φ_g nemusia byť len bijekcie $X \to X$, ale môžu to byť zobrazenia zachovávajúce nejakú štruktúru na množine X. Potom reprezentáciu Φ možno chápať ako homomorfizmus $\Phi\colon G \to A$, kde A je nejaká podgrupa grupy $\mathcal{S}(X)$. Jedným takým prípadom sa budeme zaoberať v tomto paragrafe: množina X bude opäť splývať s grupou G a spomínaná podgrupa $A \subseteq \mathcal{S}(G)$ bude pozostávať z izomorfizmov $G \to G$.

Homomorfizmus $\varphi\colon G \to G$ grupy G do seba sa nazýva *endormorfizmus grupy* G. Množinu všetkých endomorfizmov grupy G značíme $\operatorname{End} G$. Zrejme $\mathrm{id}_G \in \operatorname{End} G$ a pre $\varphi, \psi \in \operatorname{End} G$ platí $\varphi \circ \psi \in \operatorname{End} G$, čiže množina $\operatorname{End} G$ obsahuje identické zobrazenie a je uzavretá vzhľadom na skladanie zobrazení. Taktiež obsahuje ďalší význačný prvok – je ním triviálny (konštantný) endomorfizmus $x \mapsto e$.

Automorfizmom grupy G nazývame každý jej bijektívny endomorfizmus. Množinu všetkých automorfizmov grupy G značíme $\operatorname{Aut} G$.

24.3.1. Veta. *Nech $(G, \cdot)$ je grupa. Potom množina jej automorfizmov $\operatorname{Aut} G$ je podgrupou grupy $\mathcal{S}(G)$, teda je to grupa transformácií množiny G.*

Dôkaz. Zrejme $\operatorname{Aut} G \subseteq \mathcal{S}(G)$, $\mathrm{id}_G \in \operatorname{Aut} G$ a pre ľubovoľné $\varphi, \psi \in \operatorname{Aut} G$ platí $\varphi \circ \psi \in \operatorname{Aut} G$ a $\varphi^{-1} \in \operatorname{Aut} G$.

Dôležitým príkladom automorfizmov sú tzv. konjugácie. Ak g je prvok grupy G, tak zobrazenie $\Gamma_g\colon G \to G$ dané predpisom $\Gamma_g(x) = gxg^{-1}$ pre $x \in G$ nazývame *konjugáciou* prvkom $g \in G$.

24.3.2. Tvrdenie. *Nech G je grupa. Potom*

(a) pre každé $g \in G$ platí $\Gamma_g \in \operatorname{Aut} G$, t.j. zobrazenie Γ_g je automorfizmus grupy G;

(b) samotné zobrazenie $\Gamma\colon G \to \operatorname{Aut} G$ je reprezentácia grupy G v množine G.

Dôkaz. (a) Zrejme každé zobrazenie Γ_g je bijektívne – k nemu inverzným zobrazením je $\Gamma_g^{-1} = \Gamma_{g^{-1}}$. Ukážeme, že je to tiež homomorfizmus. Pre ľubovoľné $x, y \in G$ platí

$$\Gamma_g(xy) = g(xy)g^{-1} = \big(gxg^{-1}\big)\big(gyg^{-1}\big) = \Gamma_g(x)\Gamma_g(y).$$

(b) Treba overiť rovnosť $\Gamma_{gh} = \Gamma_g \circ \Gamma_h$ pre všetky $g, h \in G$. Zvoľme $x \in G$ a počítajme

$$\Gamma_{gh}(x) = (gh)x(gh)^{-1} = g\big(hxh^{-1}\big)g^{-1} = \Gamma_g(\Gamma_h(x)) = (\Gamma_g \circ \Gamma_h)(x).$$

Automorfizmy grupy G, ktoré majú tvar Γ_g pre nejaké $g \in G$, nazývame jej *vnútornými automorfizmami*. Podgrupu $\operatorname{Im}\Gamma \subseteq \operatorname{Aut} G$ značíme $\operatorname{In} G$ a nazývame *grupou vnútorných (interných) automorfizmov* grupy G.

Akciu grupy G na množine G konjugáciou budeme značiť $(g, x) \mapsto gxg^{-1}$; v predchádzajúcom paragrafe zavedené označenie $(g, x) \mapsto gx$ by v tomto prípade zrejme viedlo k nedorozumeniam.

Orbitou prvku $x \in G$ v tejto akcii je množina $\{gxg^{-1};\ g \in G\}$; prvky $x, y \in G$ sa nazývajú *konjugované*, označenie $x \sim_G y$, ak existuje $g \in G$ také, že $y = gxg^{-1}$, t.j. ak ležia v tej istej orbite. Zrejme relácia konjugovanosti $\sim_G$ je ekvivalencia na množine G. Orbitálny rozklad tvorí faktorová množina $G/\!\sim_G$, príslušné orbity sa

nazývajú *triedy konjugácie*. Výslovne upozorňujeme, že (s výnimkou komutatívnych grúp) ekvivalencia konjugovanosti $\sim_G$ *nie je kongruencia* na grupe G.

Stabilizátorom prvku $x \in G$ v akcii konjugáciou je podgrupa

$$C_G(x) = C(x) = \{g \in G;\, gxg^{-1} = x\} = \{g \in G;\, gx = xg\}$$

grupy G, nazývaná *centralizátor prvku* x; zrejme pre $g \in G$ platí $g \in C(x)$ práve vtedy, keď $gx = xg$, t.j. g *komutuje* s x. Podobne, množinou pevných bodov prvku $g \in G$ je opäť centralizátor

$$C_G(g) = C(g) = \{x \in G;\, gxg^{-1} = x\} = \{x \in G;\, gx = xg\}.$$

Jadrom reprezentácie $\Gamma : G \to \operatorname{Aut} G$ je množina

$$C(G) = \{g \in G;\, \Gamma_g = \mathrm{id}_G\} = \{g \in G;\, (\forall\, x \in G)(gx = xg)\}$$

nazývaná *centrum grupy* G, pozostávajúca zo všetkých prvkov grupy G, ktoré komutujú s každým jej prvkom. Zrejme $C(G)$ je abelovská grupa a G je abelovská práve vtedy, keď $C(G) = G$. Z vety 23.5.3 a vety 23.5.4 o homomorfizme okamžite vyplýva

24.3.3. Veta. *Centrum $C(G)$ grupy G je jej normálna podgrupa a faktorová grupa $G/C(G)$ je izomorfná s grupou $\operatorname{In} G$ vnútorných automorfimov grupy G; symbolicky $C(G) \lhd G$ a $G/C(G) \cong \operatorname{In} G$.*

Centrum hodne vypovedá o štruktúre pôvodnej grupy. Ako jednoduchú ukážku uvádzame nasledujúci zďaleka nie očividný výsledok.

24.3.4. Veta. *Nech G je ľubovoľná grupa. Ak faktorová grupa $G/C(G)$ je cyklická, tak G je komutatívna.*

Dôkaz. Označme $C = C(G)$ a predpokladajme, že G/C je cyklická rádu r, s generátorom Ca, kde $a \in G$. Potom množina $C \cup \{a\}$ generuje celú grupu G. Pre ľubovoľný prvok $x \in G$ totiž existuje $0 \le k < r$ také, že $Cx = (Ca)^k = Ca^k$. Preto $x \in Ca^k$, teda $x = ca^k \in \langle C \cup \{a\}\rangle$ pre nejaké $c \in C$. Ukážeme, že i samotná grupa G je komutatívna. Ľubovoľné $x, y \in G$ možno napísať v tvare $x = ca^k$, $y = da^l$ pre vhodné $c, d \in C$, $0 \le k, l < r$. V dôsledku toho platí $xy = ca^k \cdot da^l = da^l \cdot ca^k = yx$.

Prvok $x \in C(G)$ je konjugovaný len sám so sebou, t.j. jeho orbitou je jednoprvková množina $\{x\}$, preto pre každú transverzálnu množinu T platí $C(G) \subseteq T$. Ak $x \notin C(G)$, tak jeho orbita obsahuje aspoň dva prvky. Centralizátor prvku $x \in C(G)$ je celá grupa, t.j. $C(x) = G$; pre $x \notin C(G)$ je $C(x)$ vlastná podgrupa grupy G.

Špecifikáciou viet 24.2.1 a 24.2.2 na akciu konjugáciou dostávame nasledujúce dve vety – rovnosť v prvej z nich sa opäť nazýva *rovnosť tried*, druhá je zvláštnym prípadom Burnsideovej lemy.

24.3.5. Veta. *Nech G je konečná grupa. Potom počet prvkov grupy G konjugovaných s prvkom $x \in G$ sa rovná indexu $[G : C(x)]$ jeho centralizátora. Ak $T \subseteq G$ je transverzálna množina vzhľadom na akciu konjugáciou, tak $C(G) \subseteq T$ a platí*

$$\#\, G = \sum_{x \in T} [G : C(x)] = \#\, C(G) + \sum_{x \in T \setminus C(G)} [G : C(x)].$$

24.3.6. Veta. *Nech G je konečná grupa. Potom počet tried konjugácie v grupe G je*

$$\#\,(G/\!\sim_G) = \frac{1}{\#\,G}\sum_{g\in G}\#\,C(g) = \#\,C(G) + \frac{1}{\#\,G}\sum_{g\in G\setminus C(G)}\#\,C(g)$$

a počet netriviálnych (t.j. aspoň dvojprvkových) tried konjugácie v G je

$$\#\,(G/\!\sim_G) \Leftrightarrow \#\,C(G) = \frac{1}{\#\,G}\sum_{g\in G\setminus C(G)}\#\,C(g).$$

Rovnosť tried ma celý rad zaujímavých dôsledkov. Jedným z nich je *Cauchyho veta*, ktorá je obrátením Lagrangeovej vety pre prvočíselné delitele rádu konečnej grupy.

24.3.7. Veta. *Nech G je konečná grupa a p je prvočíslo, ktoré delí jej rád. Potom G má podgrupu rádu p.*

Dôkaz. Najprv budeme predpokladať, že $G = \{x_1, \ldots, x_n\}$ je komutatívna rádu n, pričom prvok x_i má rád r_i. Vďaka komutatívnosti G ľahko nahliadneme, že priradením $(k_1, \ldots, k_n) \mapsto x_1^{k_1} \ldots x_n^{k_n}$ je definovaný surjektívny homomorfizmus grúp

$$\varphi : \mathbb{Z}_{r_1} \times \ldots \times \mathbb{Z}_{r_n} \to G.$$

Podľa vety o homomorfizme je $G \cong (\mathbb{Z}_{r_1} \times \ldots \times \mathbb{Z}_{r_n})/\operatorname{Ker}\varphi$ a z Lagrangeovej vety vyplýva, že rád n grupy G delí rád $r_1 \ldots r_n$ grupy $\mathbb{Z}_{r_1} \times \ldots \times \mathbb{Z}_{r_n}$. Potom aj prvočíslo p delí $r_1 \ldots r_n$, preto musí deliť niektorý z činiteľov r_i. Označme $k = r_i/p$. Prvok $y = x_i^k \in \langle x_i\rangle \subseteq G$ má zrejme rád p, teda $\langle y\rangle \subseteq G$ je cyklická podgrupa rádu p.

Predpokladajme teraz, že G je konečná grupa s najmenším možným rádom, ktorý je deliteľný číslom p, ale G nemá podgrupu rádu p. Potom G nie je komutatívna, takže centrum $C = C(G)$ je jej vlastná komutatívna podgrupa a z prvej časti dôkazu vyplýva, že p nemôže deliť ani rád centra C. Podľa rovnosti tried z vety 24.3.5 platí

$$\#\,G = \#\,C + \sum_{x\in T\setminus C}[G : C(x)],$$

kde $T \subseteq G$ je nejaká transverzálna množina vzhľadom na akciu konjugáciou grupy G na sebe samej. Keby p nedelilo rád žiadneho z centralizátorov $C(x)$, $x \in T \setminus C$, delilo by všetky ich indexy $[G : C(x)]$; potom by však muselo deliť aj rád $\#\,C$, čo je spor. Preto p delí rád $C(x)$ pre nejaké $x \notin C$, čo je vlastná podgrupa grupy G. Z minimality rádu G vyplýva, že $C(x)$, a tým aj G, obsahuje pogrupu rádu p, čo je opäť spor.

Pre konečné abelovské grupy je možné úplné obrátenie Lagrangeovej vety.

24.3.8. Veta. *Nech G je konečná abelovská grupa a d je prirodzené číslo, ktoré delí jej rád. Potom G má podgrupu rádu d.*

Dôkaz. Ak d je prvočíslo, tak potrebný záver vyplýva z predchádzajúcej vety. Predpokladajme, že d je najmenšie prirodzené číslo, pre ktoré existuje konečná abelovská grupa s rádom deliteľným číslom d, no bez podgrupy rádu d. Potom $d = pm$ pre nejaké prvočíslo p a prirodzené číslo $m > 1$. Nech G je spomínaná grupa. Keďže $m < d$ tiež delí rád grupy G, táto má podgrupu S rádu m. Faktorová grupa G/S má rád deliteľný číslom p, teda aj podgrupu H rádu p. Potom však $\zeta_S^{-1}(H)$ je podgrupa grupy G rádu $pm = d$, čo je spor. (Pripomíname, že $\zeta_S : G \to G/S$ označuje prirodzenú projekciu.)

Aj nasledujúci výsledok je jednoduchým dôsledkom rovnosti tried. Ide o slabšiu verziu výsledku dokázaného Burnsidom.

24.3.9. Veta. *Nech rád grupy G je kladnou mocninou prvočísla p. Potom G má netriviálne centrum.*

Dôkaz. Nech $T \subseteq G$ je transverzálna množina vzhľadom na akciu konjugáciou. Pre každé $x \in T \setminus C(G)$ je centralizátor $C(x)$ vlastnou podgrupou grupy G, teda jeho index $[G : C(x)]$ je deliteľný číslom p. Potom však aj rád centra

$$\#\,C(G) = \#\,G \Leftrightarrow \sum_{x \in T \setminus C(G)} [G : C(x)]$$

je deliteľný číslom p.

24.3.10. Dôsledok. *Nech G je grupa rádu p^2, kde p prvočíslo. Potom G je komutatívna.*

Dôkaz. Podľa predošlej vety G má netriviálne centrum; toto môže mať len p alebo p^2 prvkov. Prvý prípad však nemôže nastať, lebo potom by faktorová grupa $G/C(G)$ bola rádu p, teda cyklická. Podľa vety 24.3.4 by G bola komutatívna, čiže $C(G) = G$.

24.4. Polopriamy súčin grúp

Reprezentácie jednej grupy automorfizmami inej grupy umožňujú zaujímavé zovšeobecnenie konštrukcie priameho súčinu grúp. Zatiaľ čo priamy súčin abelovských grúp je abelovská grupa, pomocou tzv. polopriameho súčinu možno i z abelovských grúp vytvoriť grupy neabelovské. Naopak, rozkladom nejakej grupy na polopriamy súčin v istom zmysle jednoduchších grúp možno získať hlbší vhľad do jej štruktúry.

Nech G a X sú grupy a $\Phi\colon G \to \operatorname{Aut} X$ je homomorfizmus grúp, teda vlastne reprezentácia grupy G v množine X *automorfizmami grupy* X. *Polopriamym súčinom grúp* G a X vzhľadom na reprezentáciu Φ nazývame množinu $G \times X$ s binárnou operáciou definovanou predpisom

$$(g, x) \cdot (h, y) = (gh, x\Phi_g(y))$$

pre $g, h \in G$, $x, y \in X$. Polopriamy súčin grúp G, X budeme značiť $G \ltimes_\Phi X$, prípadne len $G \ltimes X$, ak reprezentácia Φ bude zrejmá z kontextu.

24.4.1. Veta. *Nech $(G, \cdot, e)$ a $(X, \cdot, \varepsilon)$ sú grupy $\Phi : G \to \operatorname{Aut} X$ je reprezentácia grupy G. Potom polopriamy súčin $G \ltimes_\Phi X$ grúp G a X je grupa.*

Dôkaz. Na základe definície operácie na polopriamom súčine $G \ltimes_\Phi X$ a vlastností homomorfizmov pre ľubovoľné $(g, x), (h, y), (f, z) \in G \times X$ platí

$$\begin{aligned}
(g, x) \cdot \big((h, y) \cdot (f, z)\big) &= (g, x) \cdot (hf, y\,\Phi_h(z)) = \big(g(hf), x\,\Phi_g(y\,\Phi_h(z))\big) \\
&= \big((gh)f, x\,\Phi_g(y)\,\Phi_{gh}(z)\big) = (gh, x\,\Phi_g(y)) \cdot (f, z) \\
&= \big((g, x) \cdot (h, y)\big) \cdot (f, z), \\
(e, \varepsilon) \cdot (g, x) &= (eg, \varepsilon\,\Phi_e(x)) = (g, x) \\
&= (ge, x\,\Phi_g(\varepsilon)) = (g, x) \cdot (e, \varepsilon), \\
(g, x) \cdot \big(g^{-1}, \Phi_{g^{-1}}(x^{-1})\big) &= \big(gg^{-1}, x\,\Phi_{gg^{-1}}(x^{-1})\big) = \big(e, xx^{-1}\big) = (e, \varepsilon) \\
&= \big(g^{-1}g, \Phi_{g^{-1}}(x)^{-1}\Phi_{g^{-1}}(x)\big) = \big(g^{-1}, \Phi_{g^{-1}}(x)^{-1}\big) \cdot (g, x).
\end{aligned}$$

To znamená, že príslušná binárna operácia je asociatívna, jej neutrálnym prvkom je (e,ε) a inverzným prvok k prvku (g,x) je

$$(g,x)^{-1} = \big(g^{-1}, \Phi_{g^{-1}}\big(x^{-1}\big)\big) = \big(g^{-1}, \Phi_{g^{-1}}(x)^{-1}\big),$$

teda $G \ltimes_\Phi X$ je grupa.

Ak $\Phi : G \to \operatorname{Aut} X$ je triviálny automorfizmus, čiže $\Phi_g = \mathrm{id}_X$ pre všetky $g \in G$, tak uvedená definícia operácie na množine $G \times X$ nadobúda tvar $(g,x)\cdot(h,y) = (gh, xy)$, teda polopriamy súčin $G \ltimes_\Phi X$ splýva s priamym súčinom $G \times X$ grúp G, X.

Iný dôležitý špeciálny prípad polopriameho súčinu dostaneme tak, že za grupu G vezmeme priamo grupu $\operatorname{Aut} X$ všetkých automorfizmov grupy X a za homomorfizmus Φ identické zobrazenie $\mathrm{id}_G : G \to \operatorname{Aut} X$. Príslušný polopriamy súčin značíme $\operatorname{Aut} X \ltimes X = \operatorname{Hol}(X)$ a nazývame *holomorf grupy* X. Bližší pohľad na holomorf nájde čitateľ v cvičeniach. Trochu všeobecnejšie možno za G vziať akúkoľvek podgrupu grupy automorfizmov $\operatorname{Aut} X$. Násobenie v takomto polopriamom súčine $G \ltimes X$ je dané formulou

$$(g,x)\cdot(h,y) = (g\circ h, xg(y)).$$

Konečne tretí špeciálny prípad možno dostať ako polopriamy súčin grupy G samej so sebou vzhľadom na reprezentáciu konjugáciou $\Gamma : G \to \operatorname{Aut} G$. I táto konštrukcia funguje za trochu všeobecnejších podmienok. Ak H a N sú podgrupy grupy G, pričom $N \lhd G$ (dokonca stačí, aby platilo $hxh^{-1} \in N$ pre všetky $h \in H$, $x \in N$), tak H má reprezentáciu $\Gamma : H \to \operatorname{Aut} N$ konjugáciou na grupe N. Násobenie na polopriamom súčine $H \ltimes N = H \ltimes_\Gamma N$ je dané predpisom

$$(g,x)\cdot(h,y) = \big(gh, xgyg^{-1}\big),$$

pre $g,h \in H$, $x,y \in N$. Pre tento polopriamy súčin nezavádzame osobitný názov práve preto, že – ako hneď uvidíme – ide svojim spôsobom o prípad typický.

Podobne ako v prípade priameho súčinu, aj v súvislosti s polopriamym súčinom prirodzene vzniká otázka rozložiteľnosti danej grupy na polopriamy súčin netriválnych, v istom zmysle jednoduchších faktorov. Tieto, ak existujú, možno opäť nájsť medzi jej vhodnými podgrupami.

Ľahko možno overiť, že s každým polopriamym súčinom $G \ltimes_\Phi X$ grúp $(G,\cdot,e)$, $(X,\cdot,\varepsilon)$ sú zviazané tri grupové homomorfizmy

$$X \xrightarrow{\ \xi\ } G \ltimes_\Phi X \underset{\gamma}{\overset{\pi}{\rightleftarrows}} G,$$

dané predpismi

$$\xi(x) = (e,x), \qquad \pi(g,x) = g, \qquad \gamma(g) = (g,\varepsilon),$$

pre $g \in G$, $x \in X$. Pritom ξ je injektívny, π je surjektívny a platí $\operatorname{Im}\xi = \operatorname{Ker}\pi$, teda $X \overset{\xi}{\rightarrowtail} G \ltimes X \overset{\pi}{\twoheadrightarrow} G$ je krátka exaktná postupnosť. Taktiež $\gamma : G \to G \ltimes X$ je injektívny a spĺňa podmienku $\pi\circ\gamma = \mathrm{id}_G$. Podotýkame, že ani jedno z ponúkajúcich sa zobrazení $(g,x) \mapsto x$ resp. $(g,x) \mapsto \Phi_g(x)$ vo všeobecnosti *nie je homomorfizmom* $G \ltimes_\Phi X \to X$.

V polopriamom súčine $G \ltimes_\Phi X$ sme tak identifikovali dve podgrupy

$$H = \operatorname{Im}\gamma = \{(g,\varepsilon);\, g \in G\} \cong G,$$
$$N = \operatorname{Im}\xi = \operatorname{Ker}\pi = \{(e,x);\, x \in X\} \cong X$$

také, že $N \lhd G \ltimes_\Phi X$ a $H \cap N = \{(e,\varepsilon)\}$. Navyše každý prvok $(g,x) \in G \ltimes X$ možno písať v tvare $(g,x) = (e,x)\cdot(g,\varepsilon) \in NH$, ako aj $(g,x) = (g,\varepsilon)\cdot(e,\Phi_{g^{-1}}(x)) \in HN$, teda $G = NH = HN$. Ukazuje sa, že prítomnosť takýchto podgrúp v danej grupe už zabezpečuje jej rozklad na ich polopriamy súčin.

24.4.2. Veta. *Nech $(G,\cdot,e)$ je grupa a H, N sú jej podgrupy také, že $N \lhd G$, $H \cap N = \{e\}$ a $G = NH$. Potom G je izomorfná s polopriamym súčinom $H \ltimes_\Gamma N$ grúp H, N vzhľadom na reprezentáciu konjugáciou $\Gamma\colon H \to \operatorname{Aut} N$.*

Dôkaz. Ukážeme, že zobrazenie $\varphi(g,x) = xg$ je homomorfizmus grúp $\varphi\colon H \ltimes N \to G$. Pre $g,h \in H$, $x,y \in N$ jednoduchým výpočtom dostávame

$$\varphi\big((g,x)\cdot(h,y)\big) = \varphi(gh, xgyg^{-1}) = (xgyg^{-1})(gh) = (xg)(yh) = \varphi(g,x)\varphi(h,y).$$

Keďže $H \cap N = \{e\}$, z tvrdenia 23.6.2(b) vyplýva, že φ je injekcia. Surjektívnosť φ je dôsledkom rovností $\operatorname{Im}\varphi = NH = G$. Teda $G \cong H \ltimes N$.

24.4.3. Príklad. Nech m, n sú prirodzené čísla. Keďže $\mathbb{Z}_n \cong \langle x \mid x^n\rangle$, každý endomorfizmus $\varphi\colon \mathbb{Z}_n \to \mathbb{Z}_n$ je jednoznačne určený jediným prvkom $k \in \mathbb{Z}_n$, totiž obrazom $k = \varphi(1)$ generátora $1 \in \mathbb{Z}_n$. Pre $b \in \mathbb{Z}_n$ potom platí $\varphi(b) = kb$. Samostatne si rozmyslite, že $\varphi \in \operatorname{Aut}\mathbb{Z}_n$ práve vtedy, keď $k = \varphi(1)$ je nesúdeliteľné s n. Podobne, z dôvodu $\mathbb{Z}_m \cong \langle x \mid x^m\rangle$ je každý homomorfizmus $\Phi\colon \mathbb{Z}_m \to \operatorname{Aut}\mathbb{Z}_n$ jednoznačne určený jediným automorfizmom φ grupy $\mathbb{Z}_n$, totiž obrazom $\varphi = \Phi_1$ generátora $1 \in \mathbb{Z}_m$, ktorý však musí vyhovovať podmienke $\varphi^m = \mathrm{id}_{\mathbb{Z}_n}$ (pozri vetu 23.7.3). V konečnom dôsledku je tak každý homomorfizmus $\Phi\colon \mathbb{Z}_m \to \operatorname{Aut}\mathbb{Z}_n$ jednoznačne určený jediným prvkom $k = \Phi_1(1) \in \mathbb{Z}_n$, ktorý je nesúdeliteľný s n a vyhovuje podmienke $k^m \equiv_n 1$. Potom pre $a \in \mathbb{Z}_m$, $b \in \mathbb{Z}_n$ platí $\Phi_a(b) = k^a b$.

Nech teda $\Phi\colon \mathbb{Z}_m \to \operatorname{Aut}\mathbb{Z}_n$ je reprezentácia grupy $\mathbb{Z}_m$ automorfizmami grupy $\mathbb{Z}_n$ a $k = \Phi_1(1)$. Polopriamy súčin $\mathbb{Z}_m \ltimes_\Phi \mathbb{Z}_n$ budeme značiť $\mathbb{Z}_m \ltimes_k \mathbb{Z}_n$. Operácia v grupe $\mathbb{Z}_m \ltimes_k \mathbb{Z}_n$ je daná formulou

$$(a,b) * (c,d) = (a + c, b + k^a d),$$

pre $a,c \in \mathbb{Z}_m$, $b,d \in \mathbb{Z}_n$. Pri porovnaní s príkladom 23.7.4 vidíme, že priradením $(a,b) \mapsto y^b x^a$ je definovaný homomorfizmus grúp $\mathbb{Z}_m \ltimes_k \mathbb{Z}_n \to F^k_{mn}$. Čitateľ by si mal samostatne premyslieť, že ide dokonca o izomorfizmus. Teda

$$\mathbb{Z}_m \ltimes_k \mathbb{Z}_n \cong F^k_{mn} = \langle x,y \mid x^m = y^n = e,\ xyx^{-1} = y^k\rangle,$$

čím sme metacyklické grupy predstavili v tvare polopriamych súčinov cyklických grúp.

24.5. Štruktúra grúp jednoduchých rádov

Ako naznačuje naše doterajšie krátke zoznámenie so svetom grúp, štruktúra konečnej grupy do značnej miery závisí od jej rádu, presnejšie od štruktúry deliteľov tohto čísla. Jednako rád grupy (okrem istých singulárnych prípadov) ani zďaleka neurčuje jej štruktúru jednoznačne. Štruktúrou deliteľov rádu grupy je však daný akýsi predbežný rozvrh možností, ktoré u grúp daného rádu vôbec prichádzajú do úvahy. Naopak, ak je štruktúra deliteľov niektorého prirodzeného čísla dostatočne jednoduchá, umožňuje to popísať štruktúru všetkých grúp daného rádu.

Pomocou doteraz dokázaných výsledkov sme schopní jednoznačne až na izomorfizmus popísať všetky grupy rádov p, p^2 a pq, kde p, q sú rôzne prvočísla. Skúsme si najprv zosumarizovať to málo, čo už vieme:

1. Každá grupa G rádu p je cyklická, teda izomorfná s aditívnou grupou $\mathbb{Z}_p$.
2. Každá grupa G rádu p^2 je podľa dôsledku 24.3.10 komutatívna. Ak obsahuje prvok rádu p^2, tak je cyklická, teda izomorfná s grupou $\mathbb{Z}_{p^2}$. V opačnom prípade musí obsahovať aspoň dva prvky a, b rádu p také, že $b \notin \langle a\rangle$. Ľahko možno overiť, že potom $\langle a\rangle \cap \langle b\rangle = \{e\}$ a $\langle a\rangle\langle b\rangle = G$ (skúste sami). Z tvrdenia 23.6.2 tak vyplýva izomorfizmus grúp $G \cong \langle a\rangle \times \langle b\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$.

Štruktúru všetkých grúp rádu pq popisuje nasledujúca veta.

24.5.1. Veta. *Nech $p < q$ sú dve prvočísla. Potom*

(a) každá komutatívna grupa rádu pq je cyklická, teda izomorfná s grupou $\mathbb{Z}_{pq}$;

(b) nekomutatívna grupa rádu pq existuje práve vtedy, keď p delí $q \Leftrightarrow 1$, a v tom prípade je izomorfná s metacyklickou grupou F^k_{pq}, kde $k \in \mathbb{Z}^\star_q$ je prvok rádu p.

Dôkaz. Nech G je grupa rádu pq. Podľa Cauchyho vety G obsahuje podgrupu A rádu p aj podgrupu B rádu q. Obe sú zrejme cyklické, teda $A = \langle a\rangle$, $B = \langle b\rangle$ pre nejaké prvky $a, b \in G$ rádov p resp. q. Keďže rád podgrupy $A \cap B$ musí deliť rád každej z grúp A, B, nevyhnutne $A \cap B = \{e\}$. Podľa tvrdenia 23.6.2(b) je predpisom $(x, y) \mapsto yx$ definované injektívne zobrazenie $A \times B \to G$. Keďže obe množiny $A \times B$ aj G majú zhodne pq prvkov, je to dokonca bijekcia, teda $G = BA$.

Podobným spôsobom ukážeme, že B je normálna podgrupa v G. Keby pre niektoré $g \in G$ platilo $gBg^{-1} \neq B$, podgrupa $B \cap gBg^{-1}$ by bola triviálna, teda predpisom $(x, y) \mapsto xy$ by bolo definované prosté zobrazenie $B \times gBg^{-1} \to G$. Ale množina $B \times gBg^{-1}$ má q^2 kým množina G len pq prvkov, čo je spor, teda $B \lhd G$.

Podľa vety 24.4.2 grupa G je izomorfná s polopriamym súčinom $A \ltimes B$ vzhľadom na reprezentáciu konjugáciou $\Gamma\colon A \to \mathrm{Aut}\, B$ grupy A automorfizmami grupy B. Nech $\Gamma_a(b) = aba^{-1} = b^k$, kde $k \in \mathbb{Z}^\star_q$. Z úvah vykonaných v príkladoch 23.7.4–5 a 24.4.3 je jasné, že G je izomorfná s metacyklickou grupou F^k_{pq}.

Ak $k = 1$, tak generátory a, b komutujú, teda i G je komutatívna a podľa tvrdenia 23.6.2 izomorfná s priamym súčinom svojich cyklických podgrúp $A \cong \mathbb{Z}_p$, $B \cong \mathbb{Z}_q$. Z tvrdenia 23.6.4 potom vyplýva, že $G \cong \mathbb{Z}_{pq}$ je cyklická grupa.

Ak $k \neq 1$, tak k je prvok rádu p multiplikatívnej grupy $\mathbb{Z}^\star_q$ poľa $\mathbb{Z}_q$. Keďže $\mathbb{Z}^\star_q$ má rád $q \Leftrightarrow 1$, takéto k existuje vtedy a len vtedy, keď p delí $q \Leftrightarrow 1$. Navyše, ako sme dokázali v príklade 23.7.5, metacyklická grupa $F^k_{pq} \cong G$ je nezávisle na $k \neq 1$ určená jednoznačne až na izomorfizmus.