

Katedra algebry
Matematicko-fyzikální fakulty Univerzity Karlovy v Praze

Vedoucí katedry: Doc. RNDr. Jan Trlifaj, CSc.

Teorie grup — základní aspekty

Aleš Drápal

Karolinum
PRAHA 2009

Tato kniha byla vysázena systémem $\text{\TeX}$.

© Aleš Drápal, Praha 2009
© Univerzita Karlova v Praze – Nakladatelství Karolinum

Obsah

I. Úvodní pojmy a vlastnosti	5
1 Operátorové grupy	5
2 Zassenhausovo lemma a jeho důsledky	16
3 Základní strukturní pojmy	21
4 Součiny	28
5 Sumy abelovských grup	31
6 Divisibilní grupy	38
7 Působení grupy na množině	43
8 Sylowovy věty	47
9 Nilpotentní grupy	50
10 Volné grupy a jejich podgrupy	54
11 Definující relace a volný součin grup	61
 Literatura	 67
 Seznam symbolů	 69

I. Úvodní pojmy a vlastnosti

1 Operátorové grupy

Množina G spolu s

- (i) binární operací $\cdot$,
- (ii) unární operací $^{-1}$,
- (iii) nulární operací 1 a
- (iv) unárními operacemi $\omega \in \Omega$

se nazývá Ω -grupou, jestliže

- (i) binární operace $\cdot$ je asociativní ($x \cdot yz = xy \cdot z$ pro všechna $x, y, z \in G$),
- (ii) prvek 1 je neutrální ($x \cdot 1 = 1 \cdot x = x$ pro všechna $x \in G$),
- (iii) prvky x^{-1} jsou vůči prvkům x inverzní ($x \cdot x^{-1} = 1 = x^{-1} \cdot x$ pro všechna $x \in G$) a
- (iv) působení operátorů Ω je slučitelné s binární operací $\cdot$ (vztah $\omega(x \cdot y) = \omega(x) \cdot \omega(y)$ platí pro všechna $x, y \in G, \omega \in \Omega$).

Jestliže množina Ω je prázdná, tak místo o Ω -grupě mluvíme jednoduše o grupě. Běžný pojem grupy je tedy speciálním případem Ω -grupy.

Je zřejmé, že v každé Ω -grupě platí $(x^{-1})^{-1} = x$, $x \cdot y = x \cdot z \Rightarrow y = z$ a $y \cdot x = z \cdot x \Rightarrow y = z$.

Mohutnost Ω -grupy G se značí $|G|$ a nazývá se její *řád*. V konečném případě tedy $|G|$ označuje počet prvků dané Ω -grupy.

Jsou-li G a H dvě Ω -grupy, nazveme zobrazení $f: G \rightarrow H$ *homomorfismem* Ω -grup, jestliže je splněno:

- (i) $f(x \cdot y) = f(x) \cdot f(y)$ pro všechna $x, y \in G$ a
- (ii) $f(\omega(x)) = \omega(f(x))$ pro všechna $x \in G$ a $\omega \in \Omega$.

Bijektivní homomorfismus se nazývá *izomorfismus*.

I.

Úvodní pojmy a vlastnosti

(Uvědomte si, že v poslední rovnosti vystupuje ω na levé straně v roli zobrazení $G \rightarrow G$ a na pravé straně jako zobrazení $H \rightarrow H$.)

1.1 Lemma. Je-li $f: G \rightarrow H$ homomorfismus Ω -grup G a H , tak platí $f(1) = 1$ a pro všechna $x \in G$ je splněno $f(x^{-1}) = (f(x))^{-1}$.

Důkaz. $f(1) = f(1 \cdot 1) = f(1) \cdot f(1)$ implikuje $f(1) = 1$, a zbytek plyne z $f(x) \cdot f(x^{-1}) = f(1) = 1$. $\square$

1.2 Lemma. Jsou-li $f: G \rightarrow H$ a $g: H \rightarrow K$ homomorfismy Ω -grup, tak $g \circ f: G \rightarrow K$ je rovněž homomorfismus Ω -grup. Je-li f izomorfismus, potom je zobrazení $f^{-1}: H \rightarrow G$ rovněž izomorfismus.

Důkaz. Zobrazení $g \circ f$ splňuje $(g \circ f)(x \cdot y) = g(f(x) \cdot f(y)) = (g \circ f)(x) \cdot (g \circ f)(y)$ pro všechna $x, y \in G$. Pro každé $\omega \in \Omega$ a $x \in G$ máme $(f \circ g)(\omega(x)) = f(g(\omega(x))) = f(\omega(g(x))) = \omega((f \circ g)(x))$. Ať je f izomorfismus a ať h, k jsou libovolné prvky H . Pak h je rovno $f(x)$ a k je rovno $f(y)$ pro jednoznačně určené prvky $x, y \in G$. Platí jednak $f(f^{-1}(h) \cdot f^{-1}(k)) = f(x \cdot y) = f(x) \cdot f(y) = h \cdot k$, jednak $f(\omega(f^{-1}(h))) = f(\omega(x)) = \omega(f(x)) = \omega(h)$. $\square$

Je-li A podmnožina Ω -grupy G , tak A nazveme Ω -podgrupou, jestliže platí

- (i) $1 \in A$; $x \in A \Rightarrow x^{-1} \in A$; $x, y \in A \Rightarrow x \cdot y \in A$; a
- (ii) $x \in A, \omega \in \Omega \Rightarrow \omega(x) \in A$.

Jednou z nejčastěji používaných grup je *symetrická grupa* $S(X)$, kde X je nějaká množina. Tato grupa je tvořena všemi bijektivními zobrazeními (permutacemi) $f: X \rightarrow X$, přičemž binární operací je skládání zobrazení, inverzním prvkem je inverzní zobrazení a neutrálním prvkem je identické zobrazení (zapisuje se id_X nebo 1_X).

Homomorfismus $G \rightarrow H$ se nazývá *endomorfismus*, je-li $G = H$. Bijektivní endomorfismus se nazývá *automorfismus* (automorfismy jsou tedy homomorfismy, které jsou současně endomorfismy a izomorfismy).

Z 1.2 okamžitě plyne:

1.3 Důsledek. Množina všech automorfismů Ω -grupy tvoří podgrupu symetrické grupy $S(G)$. $\square$

Z definice Ω -grupy a z 1.1 dostáváme:

1.4 Důsledek. Ať G je Ω -grupa a $\omega \in \Omega$. Zobrazení $x \mapsto \omega(x)$ je endomorfismus grupy G (když G chápeme jako grupu bez Ω -operátorů) a pro všechna $x \in G$ platí $\omega(x^{-1}) = (\omega(x))^{-1}$. Rovněž je $\omega(1) = 1$. $\square$

1.5 Poznámka. Ω -grupa vlastně není nic jiného, než běžná grupa, u které je vyčleněna nějaká množina endomorfismů. Mluvíme-li o více Ω -grupách, tak ve všech těchto grupách jsou vybrány endomorfiny, které se identifikují pomocí množiny Ω . (Přitom je přípustné, aby v dané Ω -grupě dva různé symboly z Ω označovaly shodný endomorfismus.) Předpokládejme nyní, že $f: G \rightarrow H$ je homomorfismus (obyčejných) grup a že na G a H pohlížíme také jako na Ω -grupy. Pak $x \mapsto f(\omega(x))$ a $x \mapsto \omega(f(x))$ jsou podle 1.2 jistě homomorfiny $G \rightarrow H$. Homomorfismus $f: G \rightarrow H$ je Ω -homomorfismus, právě když uvedené dva homomorfiny jsou si rovny pro každé $\omega \in \Omega$.

1.6 Lemma. Bud' G grupa a g prvek G . Pak zobrazení $x \mapsto gxg^{-1}$ je automorfismem grupy G . Přitom $x \mapsto g^{-1}xg$ je inverzní automorfismus.

Důkaz. Z $g^{-1}gxg^{-1}g = x = gg^{-1}xgg^{-1}$ plyne, že skutečně běží o vzájemně inverzní zobrazení. Pro libovolné $x, y \in \Omega$ máme $xyg^{-1} = xg^{-1}gyg^{-1}$, takže jde i o homomorfiny. $\square$

Automorfiny grupy G , které lze vyjádřit ve tvaru $x \mapsto gxg^{-1}$, se nazývají *vnitřní*. Množina všech vnitřních automorfismů se značí $\text{Inn}(G)$. Množina všech automorfismů se značí $\text{Aut}(G)$ a množina všech endomorfismů $\text{End}(G)$.

Ať je pro grupu G vybrána nějaká podmnožina Ω množiny $\text{End}(G)$. Pak je jistě možné celou grupu G považovat za Ω -grupu, ale také všechny její Ω -podgrupy jsou Ω -grupy (říká se jim Ω -invariantní podgrupy grupy G).

Bud' H podgrupa grupy G .

- (i) H se nazývá *normální* $\iff H$ je $\text{Inn}(G)$ -invariantní.
- (ii) H se nazývá *charakteristická* $\iff H$ je $\text{Aut}(G)$ -invariantní.
- (iii) H se nazývá *úplně charakteristická* $\iff H$ je $\text{End}(G)$ -invariantní.

Je-li A podmnožina grupy G a $b \in G$, tak bA označuje množinu $\{ba; a \in A\}$ a Ab množinu $\{ab; a \in A\}$. Je zřejmé, že mohutnosti množin A , bA a Ab jsou shodné. Dále klademe $A^{-1} = \{a^{-1}; a \in A\}$.

1.7 Lemma. Nechť G je grupa, M její podmnožina a Ω taková podmnožina $\text{Aut}(G)$, že pro každé $\varphi \in \Omega$ je i $\varphi^{-1} \in \Omega$. Potom je ekvivalentní:

- (i) $\varphi(M) = M$ pro každé $\varphi \in \Omega$;
- (ii) $\varphi(M) \subseteq M$ pro každé $\varphi \in \Omega$; a
- (iii) $\varphi(M) \supseteq M$ pro každé $\varphi \in \Omega$.

Důkaz. Stačí si uvědomit, že $\varphi(M) \subseteq M$ nastane, právě když platí $M \subseteq \varphi^{-1}(M)$. $\square$

1.8 Lemma. Bud' G grupa a H její podgrupa. Definujme na G relace λ a ϱ tak, že $(a, b) \in \lambda \iff a^{-1}b \in H$ a $(a, b) \in \varrho \iff ab^{-1} \in H$.

- (i) Relace λ a ϱ jsou ekvivalence.
- (ii) Třída ekvivalence λ , která obsahuje prvek $a \in G$, je rovna aH .
- (iii) Třída ekvivalence ϱ , která obsahuje prvek $a \in G$, je rovna Ha .
- (iv) Pro všechna $a, b \in G$ platí $(a, b) \in \lambda \iff (a^{-1}, b^{-1}) \in \varrho$.

Důkaz.

- (i) Z $1 \in H$ plyne reflexivita obou relací. Symetrii dostaneme z $H^{-1} = H$. Je-li $(a, b) \in \lambda$ a $(b, c) \in \lambda$, jsou $a^{-1}b$ a $b^{-1}c$ prvky H , takže je i $a^{-1}c = a^{-1}b \cdot b^{-1}c \in H$, a tedy $(a, c) \in \lambda$. Podobně dokážeme i transitivitu ϱ .
- (ii) Je-li $(a, b) \in \lambda$, tak $b = a \cdot a^{-1}b \in aH$. Je-li $b = ah$, $h \in H$, tak $b^{-1}a = h^{-1} \in H$. U ekvivalence ϱ lze postupovat obdobně.
- (iii) Stačí si uvědomit, že $a^{-1}b \in H$ lze zapsat také jako $a^{-1}(b^{-1})^{-1} \in H$. $\square$

Třídy ekvivalence λ se nazývají *levé rozkladové třídy* G podle H a třídy ekvivalence ϱ jsou *pravé rozkladové třídy* G podle H .

Zobrazení $a \mapsto a^{-1}$ je permutace G , která převádí levé rozkladové třídy podle H na pravé, a indukuje tak bijekci mezi množinou levých rozkladových tříd a množinou pravých rozkladových tříd. Společné mohutnosti těchto množin se říká *index* H v G a značí se $|G : H|$. Je-li levých (a tím i pravých) rozkladových tříd konečně mnoho, mluvíme o podgrupě *konečného indexu*.

Protože všechny levé rozkladové třídy (i všechny pravé rozkladové třídy) mají stejnou mohutnost rovnou řádu H , platí vztah

$$|G| = |H| \cdot |G : H|,$$

všeobecně známý jako Lagrangeova věta.

1.9 Lemma. Podgrupa H grupy G je normální, právě když levé rozkladové třídy podle H se shodují s pravými rozkladovými třídami podle H .

Důkaz. Ať je H normální a ať pro $a, b \in G$ platí $a^{-1}b \in H$. Potom je $i \cdot a \cdot a^{-1}b \cdot a^{-1} = ba^{-1} \in H$. Podobně z $ab^{-1} \in H$ plyne $a^{-1}b \in H$. Ekvivalence λ a ϱ (viz 1.8) jsou tedy shodné. Naopak, ať jsou tyto ekvivalence shodné a $h \in H$. Pak pro každé $a \in G$ je $(ah, a) \in \lambda = \varrho$, a tedy $aha^{-1} \in H$. $\square$

Ať je H podmnožina Ω -grupy G . Řekneme, že H je Ω -normální podgrupa G , jestliže je to Ω -grupa, která je současně invariantní vůči všem zobrazením $x \mapsto axa^{-1}$, $a \in G$. (Uvážíme-li G bez Ω -operátorů, tak Ω -normální podgrupy jsou prostě normální podgrupy, které jsou invariantní vůči všem endomorfismům indukovaným operátory z Ω .)

Ať H je Ω -normální podgrupa Ω -grupy G . Označme G/H množinu všech tříd G podle H a definujme na G/H následujícím způsobem veškeré operace Ω -grupy:

- (i) $aH \cdot bH = (ab)H$ pro všechna $a, b \in G$,
- (ii) $(aH)^{-1} = a^{-1}H$ pro všechna $a \in G$,
- (iii) $H = 1 \cdot H$ je neutrálním prvkem,
- (iv) $\omega(aH) = (\omega(a))H$ pro všechna $\omega \in \Omega$ a $a \in G$.

Je třeba ověřit, že tato definice je korektní. Ať $a', b' \in G$ splňují $aH = a'H$ a $bH = b'H$. Potom $abH = ab'H = aHb' = a'Hb' = a'b'H$ a $(a')^{-1}H = (Ha')^{-1} = (Ha)^{-1} = a^{-1}H$. Konečně $\omega(a)H = \omega(a')H$ plyne z Ω -invariance H .

Uvedené operace jsou tedy definovány korektně. Ověřit skutečnost, že splňují axiomy Ω -grupy, je nyní již snadné.

Zobrazení $a \mapsto aH$ nazýváme *přirozenou projekcí podle H* , případně též (přirozenou) projekcí G na faktorovou grupu G/H .

Je-li $\varphi: G \rightarrow H$ homomorfismus Ω -grup, tak *jádro* tohoto homomorfismu $\text{Ker } \varphi$ definujeme jako $\{g \in G; \varphi(g) = 1\}$. *Obraz* $\text{Im } \varphi$ se definuje jako $\{\varphi(g); g \in G\}$.

1.10 Lemma. Buď $\varphi: G \rightarrow H$ homomorfismus Ω -grup. Potom $\text{Ker } \varphi$ je Ω -normální podgrupa Ω -grupy G . Pro $a, b \in G$ platí $\varphi(a) = \varphi(b)$, právě když $a \text{ Ker } \varphi = b \text{ Ker } \varphi$.

Důkaz. Z $g, h \in \text{Ker } \varphi$ jistě plyne $gh \in \text{Ker } \varphi$ a $g^{-1} \in \text{Ker } \varphi$. Pro $\omega \in \Omega$ a $g \in \text{Ker } \varphi$ také máme $\varphi(\omega(g)) = \omega(\varphi(g)) = \omega(1) = 1$, takže $\text{Ker } \varphi$ je Ω -podgrupa. Konečně ať je $g \in \text{Ker } \varphi$ a $a \in G$. Pak $\varphi(aga^{-1}) = \varphi(a)\varphi(g)\varphi(a)^{-1} = \varphi(a)\varphi(a)^{-1} = 1$, takže je i $aga^{-1} \in \text{Ker } \varphi$. Zbytek je snadný. $\square$

1.11 Lemma. Ať H je Ω -normální podgrupa Ω -grupy G . Potom přirozená projekce $\pi: G \rightarrow G/H$ je Ω -homomorfismus s jádrem H .

Důkaz. Je zřejmé, že operace v G/H jsou definovány právě takovým (jediným možným) způsobem, aby přirozená projekce byla homomorfismus. Přitom $aH = H$ platí právě pro $a \in H$. $\square$

Surjektivní homomorfismus Ω -grup se nazývá *epimorfismus* a injektivní homomorfismus Ω -grup sluje *monomorfismus*. Je zřejmé, že homomorfismus φ je injektivní, právě když $\text{Ker } \varphi = \{1\}$, a že φ je izomorfismem, právě když je současně epimorfismem a monomorfismem.

1.12 Tvzení (Věta o homomorfismu). Buď $\varphi: G \rightarrow H$ homomorfismus Ω -grup a ať N je Ω -normální podgrupa G a $\pi: G \rightarrow G/N$ přirozená projekce. Homomorfismus Ω -grup $\psi: G/N \rightarrow H$ takový, že platí $\varphi = \psi\pi$, lze sestavit, právě když je $N \subseteq \text{Ker } \varphi$. V takovém případě je homomorfismus ψ určen jednoznačně, jeho jádrem je $\text{Ker } \varphi/N$ a pro každé $a \in G$ je $\psi(aN) = \varphi(a)$. Přitom $\text{Im } \psi = \text{Im } \varphi$.

Důkaz. Platí-li $\varphi = \psi\pi$, tak pro každé $h \in N$ je $\varphi(h) = \psi\pi(h) = \psi(1) = 1$, a tedy je $N \subseteq \text{Ker } \varphi$. Předpokládejme, že tato inkluze platí. Pak pro každou třídu aN musí být $\psi(aN) = \varphi(a)$. Z $N \subseteq \text{Ker } \varphi$ plyne, že zobrazení $\psi: G/N \rightarrow H$ je takto definováno korektně. Zbývá ověřit, že ψ je homomorfismus Ω -grup. Ovšem $\psi(aN \cdot bN) = \psi(abN) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(aN) \cdot \psi(bN)$ a $\psi(\omega(aN)) = \psi(\omega(a)N) = \varphi(\omega(a)) = \omega(\varphi(a)) = \omega(\psi(aN))$ pro všechna $a, b \in G$ a $\omega \in \Omega$. $\square$

Je-li N normální podgrupa grupy G a $A \subseteq G$ je taková podmnožina G , že pro všechna $a \in A$ je $aN \subseteq A$, tak je A sjednocením určité množiny rozkladových tříd G podle N . Množinu těchto rozkladových tříd je přirozené označovat jako A/N .

Jsou-li A, B podmnožiny grupy G , tak součinem AB se rozumí množina $\{ab; a \in A, b \in B\}$.

Uvědomte si, že pro $\pi: G \rightarrow G/N$ přirozenou projekci a $A \subseteq G$ je $\pi(A)$ rovno AN/N .

Doporučuji se smířit s tím, že neutrální prvek G/N může být označen několika způsoby — buď přímo genericky jako 1, nebo jako N , nebo jako N/N .

1.13 Tvzení (První věta o izomorfismu). *Buď $\varphi: G \rightarrow H$ epimorfismus Ω -grup a ať je $N = \text{Ker } \varphi$. Potom zobrazení $aN \mapsto \varphi(a)$ je Ω -izomorfismus G/N na H .*

Důkaz. Přímou aplikací 1.12. $\square$

1.14 Tvzení. *Buď $\varphi: G \rightarrow H$ homomorfismus Ω -grup. Obrazem každé Ω -podgrupy G je Ω -podgrupa H . Ať $N \subseteq M$ jsou Ω -podgrupy G , přičemž N je Ω -normální podgrupa M . Potom $\varphi(N)$ je rovněž Ω -normální podgrupou $\varphi(M)$.*

Důkaz. Jsou-li $a, b \in \varphi(M)$, je $a = \varphi(c)$ a $b = \varphi(d)$ pro nějaká $c, d \in M$. Tudíž $a \cdot b = \varphi(c) \cdot \varphi(d) = \varphi(c \cdot d) \in \varphi(M)$, $a^{-1} = (\varphi(c))^{-1} = \varphi(c^{-1}) \in \varphi(M)$ a pro libovolné $\omega \in \Omega$ je $\omega(a) = \omega(\varphi(c)) = \varphi(\omega(c)) \in \varphi(M)$. Ať N je Ω -normální podgrupa M . Pak pro $a = \varphi(c) \in \varphi(M)$ a $b = \varphi(d) \in \varphi(N)$ je aba^{-1} rovno $\varphi(cdc^{-1}) \in \varphi(N)$. $\square$

1.15 Lemma. *Buď $\varphi: G \rightarrow H$ homomorfismus Ω -grup. Vzor každé Ω -podgrupy H je Ω -podgrupou G . Ať $N \subseteq M$ jsou Ω -podgrupy H , přičemž N je Ω -normální podgrupa M . Potom $\varphi^{-1}(N)$ je Ω -normální podgrupou $\varphi^{-1}(M)$.*

Důkaz. Jsou-li $a, b \in \varphi^{-1}(M)$, je $\varphi(ab) = \varphi(a)\varphi(b) \in M$, $\varphi(a^{-1}) = (\varphi(a))^{-1} \in M$ a pro $\omega \in \Omega$ je $\varphi(\omega(a)) = \omega(\varphi(a)) \in M$. To znamená, že $\varphi^{-1}(M)$ je Ω -podgrupa G . Ať N je Ω -normální podgrupa M a ať je $a \in \varphi^{-1}(N)$ a $b \in \varphi^{-1}(M)$. Potom $\varphi(bab^{-1}) = \varphi(b)\varphi(a)\varphi(b)^{-1} \in N$, takže $\varphi^{-1}(N)$ je ve $\varphi^{-1}(M)$ vskutku Ω -normální. $\square$

Připomeňme, že soustava podmnožin $\mathcal{A}$ množiny M se nazývá *uzávěrový systém*, jestliže je $M \in \mathcal{A}$ a pro libovolné neprázdné $\mathcal{B} \subseteq \mathcal{A}$ průnik $\bigcap(B; B \in \mathcal{B})$ patří do $\mathcal{A}$ (tedy $\mathcal{A}$ je systém podmnožin M , který je uzavřený na průniky a obsahuje M).

Chápeme-li $\mathcal{A}$ jako množinu částečně uspořádanou inkluzí, tak $\mathcal{A}$ je úplný svaz s nejmenším prvkem $\bigcap(A; A \in \mathcal{A})$ a největším prvkem M . Průsek v tomto svazu je roven průniku, a spojení množin $A_i \in \mathcal{A}$, $i \in I$, je rovno nejmenší množině $A \in \mathcal{A}$, která obsahuje $\bigcup(A_i; i \in I)$.

1.16 Lemma. *Buď dána Ω -grupa G . Pak všechny Ω -podgrupy tvoří uzávěrový systém a všechny Ω -normální podgrupy G tvoří také uzávěrový systém. Přitom svaz Ω -normálních podgrup je podsvazem svazu všech Ω -podgrup.*

Důkaz. Uzavřenost na průniky je zřejmá, je tedy pouze třeba ukázat, že Ω -normální podgrupy tvoří podsvaz. Průseky se v obou svazech shodují, takže jde jen o spojení Ω -normálních podgrup N_i , $i \in I$, $I \neq \emptyset$. Buď M nejmenší Ω -podgrupa G , která obsahuje $\bigcup(N_i; i \in I)$. Pro každé $h \in G$ a každé $i \in I$ je $hMh^{-1} \supseteq hN_ih^{-1} = N_i$, takže hMh^{-1} obsahuje $\bigcup(N_i; i \in I)$. Pokud víme, že hMh^{-1} je Ω -grupa (a tak tomu například bude, když $\Omega = \emptyset$), tak musí platit $hMh^{-1} \supseteq M$, a tedy $hMh^{-1} = M$ podle 1.7.

Obecně ovšem nemůžeme předpokládat, že hMh^{-1} je Ω -grupa. Vztah $hMh^{-1} \supseteq M$ dokážeme pro obecný případ jinou metodou, která je velmi jednoduchá, ale přeci jen se odlišuje od postupů používaných na jiných místech této kapitoly. Ať N je množina všech prvků G , které lze vyjádřit jako $g_1g_2 \cdots g_r$, kde každé g_j , $1 \leq j \leq r$, padne do $\bigcup(N_i; i \in I)$. Prázdný součin (případ $r = 0$) ať vyjadřuje neutrální prvek. Okamžitě vidíme, že N je Ω -podgrupa G , která obsahuje každé N_i , $i \in I$. Navíc N leží v každé podgrupě této vlastnosti, a proto $N \subseteq M$. Ovšem M je nejmenší podgrupa, která obsahuje $\bigcup(N_i; i \in I)$. Proto $N = M$. Zbývá dokázat, že $hNh^{-1} \subseteq N$ pro každé $h \in G$. Máme $hg_1g_2 \cdots g_rg^{-1} = g'_1g'_2 \cdots g'_r$, kde $g'_j = hg_jh^{-1} \in N$, pokud $g_j \in N_i$, $1 \leq j \leq r$ a $i \in I$. $\square$

Nejmenším prvkem svazu Ω -podgrup Ω -grupy G je $\{1\}$. Této grupě se říká *triviální* podgrupa a formální rozdíl mezi $\{1\}$ a 1 se ve značení často zanedbává. Největším prvkem svazu Ω -podgrup Ω -grupy G je přímo G . O G a o 1 se mluví jako o *nevlastních* Ω -podgrupách, ostatní Ω -podgrupy jsou *vlastní*.

Připomeňme, že pro prvky $a \leq b$ svazu L se množina $[a; b] = \{c \in L; a \leq c \leq b\}$ nazývá interval, přičemž každý interval je podsvazem daného svazu. Připomeňme dále, že bijekce $f: L \rightarrow M$ dvou svazů je svazový izomorfismus,

právě když pro všechna $c, d \in L$ je splněna ekvivalence $c \leq d \Leftrightarrow f(c) \leq f(d)$.

1.17 Tvzení. At $\varphi: G \rightarrow H$ je epimorfismus Ω -grup a $N = \text{Ker } \varphi$. Pak jsou zobrazení $L \mapsto \varphi(L)$ a $K \mapsto \varphi^{-1}(K)$ vzájemně inverzními svazovými izomorfismy intervalu $[N; G]$ obsaženého ve svazu Ω -podgrup Ω -grupy G se svazem všech Ω -podgrup Ω -grupy H . Tyto svazové izomorfismy zachovávají vztah Ω -normality.

Důkaz. Z $L \supseteq N$ plyne $\varphi^{-1}\varphi(L) = L$ (viz 1.10) a ze surjektivit zobrazení φ máme $\varphi\varphi^{-1}(K) = K$. Dále $L_1 \supseteq L_2$ platí, právě když je $\varphi(L_1) \supseteq \varphi(L_2)$, takže tvrzení dostáváme okamžitě z 1.14 a 1.15. $\square$

1.18 Důsledek. At N je Ω -normální podgrupa Ω -grupy G a at $K \supseteq N$ je Ω -podgrupa G . Pak K/N je Ω -podgrupa Ω -grupy G/N a každou Ω -podgrupu Ω -grupy G/N lze takto jednoznačně vyjádřit. Přitom K/N je Ω -normální podgrupa G/N , právě když K je Ω -normální podgrupa G .

Důkaz. Jde o použití 1.17 pro přirozenou projekci $\pi: G \rightarrow G/N$. $\square$

1.19 Tvzení (Druhá věta o izomorfismu). At $H \supseteq N$ jsou Ω -normální podgrupy Ω -grupy G . Pak $(aN) \cdot (H/N) \mapsto aH$ je korektně definovaný izomorfismus Ω -grup $(G/N)/(H/N)$ a G/H .

Důkaz. Uvažme přirozenou projekci $\pi: G \rightarrow G/H$. Podle věty o homomorfismu 1.12 existuje homomorfismus $\psi: G/N \rightarrow G/H$ takový, že $\psi(aN) = aH$ pro všechna $a \in G$, a $\text{Ker } \psi = H/N$. Aplikujeme-li nyní První větu o izomorfismu 1.13 na epimorfismus ψ , dostaneme izomorfismus uvedený v tvrzení. $\square$

1.20 Lemma. At H a K jsou Ω -podgrupy Ω -grupy G a at H je přitom její Ω -normální podgrupa. Pak HK je jednak rovno KH , jednak to je Ω -podgrupa G .

Důkaz. Ukážeme, že HK je uzavřená na příslušné operace. At je $h_1, h_2 \in H$ a $k_1, k_2 \in K$. Pak $h_1k_1 \cdot h_2k_2 = h_1k_1h_2k_1^{-1}k_1k_2 \in HK$, $(h_1k_1)^{-1} = k_1^{-1}h_1^{-1} = k_1^{-1}h_1^{-1}k_1k_1^{-1} \in HK$ a $\omega(h_1k_1) = \omega(h_1)\omega(k_1) \in HK$. Vidíme, že HK je vskutku Ω -podgrupa. Proto je $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. $\square$

At N je Ω -normální podgrupa Ω -grupy G a $\pi: G \rightarrow G/N$ přirozená projekce. Je-li H nějaká Ω -podgrupa G , tak $\pi(H)$ je rovno HN/N a $\pi^{-1}\pi(H)$ je rovno HN . Protože obrazem Ω -podgrupy je Ω -podgrupa a vzorem Ω -podgrupy je rovněž Ω -podgrupa, tak vidíme, že HN vskutku musí být podgrupa. Tato úvaha tedy může sloužit jako jiný důkaz předchozího lemmatu. Vzhledem k 1.14 a 1.15 z ní rovněž můžeme odvodit:

1.21 Důsledek. At N je Ω -normální podgrupa Ω -grupy G a at H a K jsou takové Ω -podgrupy G , že H je Ω -normální podgrupa K . Potom HN je Ω -normální podgrupa KN . $\square$

At H je Ω -podgrupa Ω -grupy G . Pak vložení $h \mapsto h$ je monomorfismem $H \rightarrow G$. Proto z 1.14 dostáváme:

1.22 Důsledek. At H je Ω -podgrupa Ω -grupy G a at N a M jsou takové Ω -podgrupy G , že N je Ω -normální podgrupa M . Potom $H \cap N$ je Ω -normální podgrupa $H \cap M$. $\square$

Je samozřejmé, že oba předcházející důsledky bychom také snadno mohli dokázat přímo.

1.23 Tvzení (Třetí věta o izomorfismu). At N je Ω -normální podgrupa Ω -grupy G a at H je Ω -podgrupa G . Zobrazení $h \cdot (H \cap N) \mapsto hN$ je izomorfismus grup $H/H \cap N$ a HN/N .

Důkaz. Uvažme nejprve přirozenou projekci $\pi: G \rightarrow G/N$ a označme φ její restrikcí na H . Potom $\text{Im } \varphi = HN/N$ a $\text{Ker } \varphi = H \cap N$. Tvrzení nyní plyne z První věty o izomorfismu 1.13. $\square$

At G je Ω -grupa a M její podmnožina. Protože Ω -podgrupy Ω -grupy G tvoří uzávěrový systém, tak existuje nejmenší Ω -podgrupa H taková, že je $M \subseteq H$. Říkáme, že H je *generována* M , a o M hovoříme také jako o *množině generátorů* Ω -grupy H .

1.24 Lemma. At $\varphi: G \rightarrow H$ a $\psi: G \rightarrow H$ jsou dva homomorfismy Ω -grup G a H . Pak $\{a \in G; \varphi(a) = \psi(a)\}$ je Ω -podgrupa Ω -grupy G .

Důkaz. At $a, b \in G$ jsou takové, že je $\varphi(a) = \psi(a)$ a $\varphi(b) = \psi(b)$. Pak

$\varphi(a^{-1}) = (\varphi(a))^{-1} = (\psi(a))^{-1} = \psi(a^{-1})$ a $\varphi(ab) = \varphi(a)\varphi(b) = \psi(a)\psi(b) = \psi(ab)$. Pro každé $\omega \in \Omega$ je $\varphi(\omega(a)) = \omega(\varphi(a)) = \omega(\psi(a)) = \psi(\omega(a))$. $\square$

1.25 Důsledek. *At G je Ω -grupa a $\varphi \in \text{End}(G)$. Pak $\{a \in G; \varphi(a) = a\}$ je Ω -podgrupa Ω -grupy G .*

Důkaz. Stačí srovnat φ s identickým automorfismem 1_G . $\square$

1.26 Důsledek. *At G a H jsou Ω -grupy a at $M \subseteq G$ generuje G . Jsou-li $\varphi: G \rightarrow H$ a $\psi: G \rightarrow H$ takové homomorfismy Ω -grup, že $\varphi(m) = \psi(m)$ pro všechna $m \in M$, tak je $\varphi = \psi$.*

Důkaz. Množina $\{a \in G; \varphi(a) = \psi(a)\}$ je Ω -podgrupou G , která obsahuje M . Protože M generuje G , musí tato množina být rovna G . $\square$

1.27 Poznámka. Je samozřejmé, že některá z výše uvedených tvrzení by bylo možno vyslovit ve formálně obecnějším tvaru. Například podmínku, že $\varphi: G \rightarrow H$ je epimorfismus, je možné vypustit, pokud místo H píšeme $\text{Im } \varphi$. Podobně v 1.20 lze pouze předpokládat, že H je Ω -normální v nějaké Ω -podgrupě L , která obsahuje K . Cena takovýchto průhledných zobecnění je malá, neboť při aplikaci se lze stejně dobře odkázat na námi uvedené znění příslušných tvrzení.

2 Zassenhausovo lemma a jeho důsledky

Připomeňme, že svaz L je modulární, jestliže splňuje implikaci

$$c \geq a \quad \Rightarrow \quad (c \wedge b) \vee a = c \wedge (b \vee a) .$$

Protože $c \wedge (b \vee a) \geq (c \wedge b) \vee a$ je splněno vždy, stačí ověřovat nerovnost $(c \wedge b) \vee a \geq c \wedge (b \vee a)$.

K pochopení vlastnosti modularity je užitečné si představit, že chceme svazovými operacemi zobrazit prvek b do intervalu $[a; c]$. Nabízejí se dva přirozené postupy:

- (i) V prvním kroku poslat b nad a (vznikne $b \vee a$) a v druhém kroku zobrazit výsledek pod c , takže dostaneme $c \wedge (b \vee a)$.
- (ii) V prvním kroku poslat b pod c (vznikne $b \wedge c$) a v druhém kroku zobrazit výsledek nad a , takže dostaneme $a \vee (b \wedge c)$.

Modularita znamená, že oba postupy dají týž prvek svazu L . V této kapitole půjde nejen o promítání bodu do intervalu, ale i o promítání intervalů do intervalu. Vztahy modularity umožňují ztotožnit v potřebných případech „horní“ promítání (postup (i)) s „dolním“ promítáním (postup (ii)).

Jsou-li A a B podgrupy grupy G , je součin $AB = \{ab; a \in A, b \in B\}$ v některých případech také podgrupa grupy G (viz 1.20). Následující lemma ovšem platí bez ohledu na to, zda AB podgrupa je, nebo není.

2.1 Lemma (modulární vlastnost grup). *At A, B, C jsou Ω -podgrupy Ω -grupy G . Je-li $C \supseteq A$, platí $(C \cap B)A = C \cap (BA)$.*

Důkaz. Je-li $x \in (C \cap B)A$, tak $x = ba$ pro $b \in B \cap C$ a $a \in A \subseteq C$. Je tedy $ba \in C$, takže je i $x = ba \in C \cap (BA)$. Naopak, je-li $y = ba$ prvek $C \cap (BA)$, $b \in B$, $a \in A$, je $b = ya^{-1}$ prvek C , neboť y i a^{-1} patří do C . To znamená, že $b \in B \cap C$ a $y \in (B \cap C)A$. Rovnost obou množin je dokázána. $\square$

Jestliže A je Ω -normální podgrupa Ω -grupy G , tak $(C \cap B)A$ i $C \cap (BA)$ jsou jistě Ω -podgrupami G (viz 1.16 a 1.20). Proto platí

2.2 Důsledek. *Svaz Ω -normálních podgrup Ω -grupy G je modulární.* $\square$

2.3 Tvzení (Zassenhausovo lemma). *At' A, B, C, D jsou Ω -podgrupy Ω -grupy G , přičemž B je Ω -normální pogruba A a D je Ω -normální pogruba C . Pak $(A \cap D)B$ je Ω -normální pogruba $(A \cap C)B$, $(B \cap C)D$ je Ω -normální pogruba $(A \cap C)D$ a platí*

$$(A \cap C)B / (A \cap D)B \cong (A \cap C)D / (B \cap C)D .$$

Důkaz. Vyjdeme z diagramu, který vidíte na protější straně.

Pro lepší čitelnost důkazu budeme místo Ω -normální psát pouze normální. Podle 1.22 je $A \cap D$ normální v $A \cap C$ a podle 1.21 je $(A \cap D)B$ normální v $(A \cap C)B$. Podobně se ukáže, že $(B \cap C)D$ je normální v $(A \cap C)D$. Budeme se snažit pomocí Třetí věty o izomorfismu 1.23 ukázat, že platí

$$(A \cap C)B / (A \cap D)B \cong A \cap C / (A \cap D)(B \cap C) .$$

Položíme $H = (A \cap C)B$, $X = (A \cap D)B$ a vyjdeme z faktu, že X je normální v H . Protože H lze vyjádřit jako $(A \cap C)X$, tak je podle Třetí věty o izomorfismu $X \cap A \cap C$ normální v $A \cap C$ a $H/X \cong A \cap C / X \cap A \cap C$.

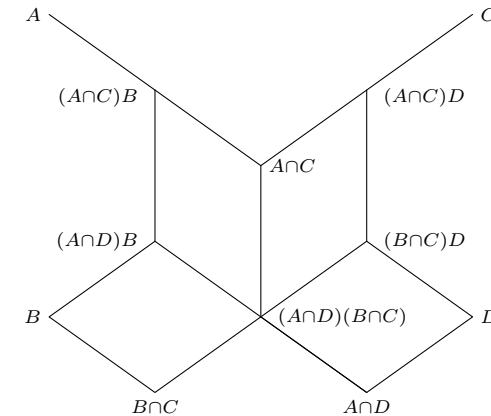
Z 2.1 dostáváme $X \cap A \cap C = (A \cap C) \cap (B(A \cap D)) = (A \cap C \cap B)(A \cap D) = (B \cap C)(A \cap D)$, neboť $A \cap C \supseteq A \cap D$. Vedle

$$(A \cap C)B / (A \cap D)B \cong A \cap C / (A \cap D)(B \cap C)$$

symetricky platí

$$A \cap C / (A \cap D)(B \cap C) \cong (A \cap C)D / (B \cap C)D ,$$

takže hledaný izomorfismus vznikne složením nalezených izomorfismů. $\square$



O Ω -grupě řekneme, že je Ω -jednoduchá, jestliže není triviální (tj. $G \neq 1$) a neobsahuje žádnou vlastní Ω -normální podgrupu.

Subnormální Ω -řadou Ω -grupy G nazveme každou posloupnost Ω -podgrup $1 = H_0, H_1, \dots, H_n = G$ takových, že H_{i-1} je Ω -normální podgruba H_i , $1 \leq i \leq n$. Faktorgrupy H_i / H_{i-1} , $1 \leq i \leq n$, se nazývají *faktory* Ω -řady.

Subnormální Ω -řada K_j , $0 \leq j \leq m$, je *zjemněním* Ω -řady H_i , $0 \leq i \leq n$, jestliže existuje podposloupnost indexů $0 = j_0 < j_1 < \dots < j_n = m$ taková, že $K_{j_i} = H_i$ pro všechna i , $0 \leq i \leq n$.

Subnormální Ω -řady H_i , $0 \leq i \leq n$, a K_j , $0 \leq j \leq m$, jsou Ω -izomorfní, jestliže $n = m$ a existuje permutace $\sigma \in S_n$ taková, že $H_i / H_{i-1} \cong K_{\sigma(i)} / K_{\sigma(i)-1}$ pro každé i , $1 \leq i \leq n$.

Buď H_i , $0 \leq i \leq n$, subnormální Ω -řada a vyberme jeden index j , $1 \leq j \leq n$. Podle tvrzení 1.17 odpovídají Ω -podgrupy Ω -grupy H_j / H_{j-1} těm Ω -podgrupám K Ω -grupy H_j , které splňují $K \supseteq H_{j-1}$. Protože při této korespondenci se zachovávají vztahy normality (viz 1.17), vidíme, že Ω -řada H_i má zjemnění tvaru $H_0, \dots, H_{j-1}, K_1, \dots, K_{m-1}, H_j, \dots, H_n$, právě když $1 = H_{j-1} / H_{j-1}, K_1 / H_{j-1}, \dots, K_{m-1} / H_{j-1}, H_j / H_{j-1}$ je Ω -řada Ω -grupy H_j / H_{j-1} . Speciálně tedy vidíme, že Ω -řada H_i , ve které je $H_{j-1} \neq H_j$, nemá zjemnění tvaru $H_0, \dots, H_{j-1}, K, H_j, \dots, H_n$, $H_{j-1} \neq K$, $H_j \neq K$, právě když H_j / H_{j-1} je Ω -jednoduchá Ω -grupa.

Subnormální Ω -řada H_i , $0 \leq i \leq n$, se nazývá *kompoziční* Ω -řada, jestliže je každý faktor H_i / H_{i-1} , $1 \leq i \leq n$, Ω -jednoduchou Ω -grupou. (Při definici Ω -jednoduché Ω -grupy jsme vyloučili triviální jednoprvkový případ,

takže v kompoziční Ω -řadě vždy platí $H_{i-1} \neq H_i$.)

2.4 Tvzení. Ať H_i , $0 \leq i \leq n$, a K_j , $0 \leq j \leq m$, jsou dvě subnormální Ω -řady Ω -grupy G . Potom lze nalézt takové Ω -izomorfní subnormální Ω -řady $\tilde{H}_r$, $0 \leq r \leq s$, a $\tilde{K}_r$, $0 \leq r \leq s$, že $s = nm$, přičemž $\tilde{H}_r$, $0 \leq r \leq s$, je zjemněním H_i , $0 \leq i \leq n$, a $\tilde{K}_r$, $0 \leq r \leq s$ je zjemněním K_j , $0 \leq j \leq m$.

Důkaz. Budeme projektovat intervaly H_{i-1}, H_i do intervalů K_{j-1}, K_j a naopak. Izomorfismy přitom získáme z Zassenhausova lemmatu 2.3.

Pro $0 \leq i \leq n-1$ a $0 \leq j \leq m$ položíme $H_{i,j} = H_i(H_{i+1} \cap K_j)$ a pro $0 \leq i \leq n$ a $0 \leq j \leq m-1$ ať $K_{j,i} = K_j(K_{j+1} \cap H_i)$. Podle Zassenhausova lemmatu pro $0 \leq i < n$ a $0 \leq j < m$ je $H_{i,j}$ obsažena v $H_{i,j+1}$ jako Ω -normální podgrupa, $K_{j,i}$ je Ω -normální podgrupa v $K_{j,i+1}$ a platí

$$H_{i,j+1}/H_{i,j} \cong K_{j,i+1}/K_{j,i}.$$

Přitom zřejmě platí $H_{i,0} = H_i$, $H_{i,m} = H_{i+1}$, $K_{j,0} = K_j$, $K_{j,n} = K_{j+1}$.

Ať r splňuje $0 \leq r < nm$. Pak r lze jednoznačně zapsat jednak jako $am + b$, $0 \leq b < m$, jednak jako $cn + d$, $0 \leq d < n$. Položíme $\tilde{H}_r = H_{a,b}$ a $\tilde{K}_r = K_{c,d}$. Konečně ať $\tilde{H}_{nm} = \tilde{K}_{nm} = G$. Je-li $b < m-1$, je jistě $\tilde{H}_{r+1} = H_{a,b+1}$. Pro $b = m-1$ je $\tilde{H}_{r+1}$ rovno $\tilde{H}_{(a+1)m} = H_{a+1} = H_{a,m}$, takže $\tilde{H}_{r+1}$ je pro $\tilde{H}_r = H_{a,b}$ rovno $H_{a,b+1}$ ve všech případech. Podobně $\tilde{K}_{r+1}$ se rovná $K_{c,d+1}$. Vidíme tedy, že $\tilde{H}_r$, $0 \leq r \leq nm$, a $\tilde{K}_r$, $0 \leq r \leq nm$, jsou Ω -subnormální řady.

Buď nyní τ permutace množiny $\{0, 1, \dots, nm-1\}$, která prvku $am+b$, $0 \leq b < m$, přiřazuje prvek $bn+a$. Dokázali jsme, že platí $\tilde{H}_{r+1}/\tilde{H}_r \cong \tilde{K}_{\tau(r)+1}/\tilde{K}_{\tau(r)}$, takže zkonstruované Ω -subnormální řady jsou vskutku Ω -izomorfní. $\square$

2.5 Tvzení (Jordanova–Hölderova věta). *Libovolné dvě Ω -kompoziční řady Ω -grupy G jsou Ω -izomorfní.*

Důkaz. Použijeme předchozí tvrzení pro případ, kdy H_i , $0 \leq i \leq n$, a K_j , $0 \leq j \leq m$, jsou Ω -kompoziční řady. Protože $\tilde{H}_r$, $0 \leq r \leq nm$, je zjemnění Ω -kompoziční řady, musí v $nm-n$ případech platit $\tilde{H}_r = \tilde{H}_{r+1}$. Podobně je $\tilde{K}_r = \tilde{K}_{r+1}$ právě v $nm-m$ případech. Ovšem $\tilde{H}_r$, $0 \leq r \leq nm$, a $\tilde{K}_r$, $0 \leq r \leq nm$, jsou Ω -izomorfní řady, takže musí být $nm-n = nm-m$,

a tedy $n = m$. Netriviální faktory $\tilde{K}_{r+1}/\tilde{K}_r$ se shodují s faktory K_{j+1}/K_j a netriviální faktory $\tilde{H}_{r+1}/\tilde{H}_r$ se shodují s faktory H_{i+1}/H_i . Protože $\tilde{H}_r$, $0 \leq r \leq nm$ a $\tilde{K}_r$, $0 \leq r \leq nm$ jsou Ω -izomorfní, musí tedy být Ω -izomorfní i obě výchozí Ω -kompoziční řady. $\square$

2.6 Poznámka. Existenci Ω -kompoziční řady máme zaručenou u konečných Ω -grup. Obecně Ω -kompoziční řada existovat nemusí. U mnoha nekonečných Ω -grup dokonce neexistuje žádná Ω -subnormální řada v námi definovaném významu (bylo by totiž možné Ω -subnormální řady definovat i s limitními přechody, což se také v teorii nekonečných grup někdy děje).

V teorii grup se Ω -grupy prakticky výhradně používají v případě, kdy máme danu grupu G a za Ω zvolíme buď prázdnou množinu, nebo $\text{Inn}(G)$, nebo $\text{Aut}(G)$, nebo $\text{End}(G)$. Přitom se obvykle nezkoumají všechny grupy, na kterých je možné zavést příslušné Ω -operátory, ale pouze Ω -podgrupy grupy G . Je-li $\Omega = \emptyset$, tak Ω -podgrupy G jsou všechny podgrupy G , pro $\Omega = \text{Inn}(G)$ dostáváme normální podgrupy, pro $\Omega = \text{Aut}(G)$ uvažujeme charakteristické podgrupy a pro $\Omega = \text{End}(G)$ běží o úplně charakteristické podgrupy (viz též kapitola 1).

Je-li $\Omega = \emptyset$, tak subnormální Ω -řada Ω -grupy G se jednoduše nazývá *subnormální řada* grupy G a kompoziční Ω -řada Ω -grupy G je prostě *kompoziční řada* grupy G . V případě $\Omega = \text{Inn}(G)$ je subnormální Ω -řada Ω -grupy G označována jako *normální řada* grupy G a kompoziční Ω -řada Ω -grupy G jako *hlavní řada* grupy G . V případě $\Omega = \text{Aut}(G)$ mluvíme o *charakteristické řadě* a *hlavní charakteristické řadě*. Konečně v případě $\Omega = \text{End}(G)$ hovoříme o *úplně charakteristické řadě* a *hlavní úplně charakteristické řadě*.

Tvrzení 2.5 lze tedy v případě $\Omega = \emptyset$ vyjádřit také tak, že libovolné dvě kompoziční řady grupy G jsou stejně dlouhé a jejich faktory jsou izomorfní. Podobná tvrzení lze samozřejmě vyslovit i pro $\Omega = \text{Inn}(G)$, $\Omega = \text{Aut}(G)$ nebo $\Omega = \text{End}(G)$, to však jistě každý zvládne.

Pojem Ω -grupy je z hlediska tohoto pojednání ryze služební, jeho zavedení nám umožnilo dokázat tvrzení 2.3 a 2.4 ve formě, která zahrnuje všechny výše zmíněné důležité speciální případy. V dalším textu již o obecně pojatých Ω -grupách takřka hovořit nebudeme, a pokud tak učiníme, budeme spíše hovořit o (běžné) grupě G , na které je dán systém operátorů Ω . (Operátor definovaný na grupě G je vlastně totéž jako endomorfismus G — viz 1.4, a bijektivní operátory odpovídají automorfismům.) Přitom o $M \subseteq G$ říkáme, že je Ω -invariantní, jestliže pro každé $\omega \in \Omega$ platí $\omega(M) \subseteq M$. Pokud

$M \subseteq G$ je Ω -invariantní, přičemž každé $\omega \in \Omega$ poskytuje automorfismus G , ke kterému lze v Ω najít i automorfismus inverzní, tak podle 1.7 pro každé $\omega \in \Omega$ platí $\omega(M) = M$.

3 Základní strukturní pojmy

Buď G grupa. Píšeme $H \leq G$, jestliže H je podgrupa G , a $H \trianglelefteq G$, jestliže H je normální podgrupa G . V případě $H \neq G$ se používá též $H < G$ a $H \triangleleft G$.

Pro $M \subseteq G$ definujeme *centralizátor* $C_G(M) = \{g \in G; gm = mg \text{ pro všechna } m \in M\}$ a *normalizátor* $N_G(M) = \{g \in G; gMg^{-1} = M\}$.

3.1 Lemma. *Ať M je podmnožina grupy G . Pak $C_G(M)$ a $N_G(M)$ jsou podgrupy grupy G a platí $C_G(M) \trianglelefteq N_G(M)$. Je-li Ω nějaký systém operátorů na G a platí-li $\omega(M) = M$ pro všechna $\omega \in \Omega$, jsou $C_G(M)$ i $N_G(M)$ grupy Ω -invariantní.*

Důkaz. Fakt, že jde o podgrupy, se ověří velmi snadno. Ať je $a \in N_G(M)$ a $b \in C_G(M)$. Chceme ukázat, že platí $aba^{-1} \in C_G(M)$, to jest, že $(aba^{-1})m(ab^{-1}a^{-1}) = m$ pro všechna $m \in M$. Ovšem $a^{-1}ma$ padne do M , takže $ba^{-1}mab^{-1}$ je rovno $a^{-1}ma$. Máme tedy $aba^{-1}mab^{-1}a^{-1} = aa^{-1}maa^{-1} = m$.

Ať je $\omega(M) = M$ pro nějaký operátor $\omega \in \Omega$ a ať je $a \in N_G(M)$ a $b \in C_G(M)$. Potom pro každé $m \in M$ existuje $m' \in M$ takové, že $m = \omega(m')$, takže $\omega(a)m\omega(a)^{-1} = \omega(a)\omega(m')\omega(a^{-1}) = \omega(am'a^{-1}) \in \omega(M) = M$ a $\omega(b)m\omega(b)^{-1} = \omega(b)\omega(m')\omega(b^{-1}) = \omega(bm'b^{-1}) = \omega(m') = m$. $\square$

3.2 Lemma. *Buď $H \leq G$. Pak je $H \trianglelefteq N_G(H)$ a $N_G(H)$ obsahuje každou grupu $K \leq G$, pro kterou platí $H \trianglelefteq K$.*

Důkaz. Toto je snadné. $\square$

Centrum grupy $Z(G)$ je rovno $\{g \in G; ag = ga \text{ pro všechna } a \in G\}$. Je tedy $Z(G) = C_G(G)$.

3.3 Tvzení. *Centrum $Z(G)$ grupy G je charakteristickou podgrupou grupy G .*

Důkaz. Ať je $g \in Z(G)$, $\varphi \in \text{Aut}(G)$ a $a \in G$. Prvek a lze vyjádřit jako $\varphi(b)$, $b \in G$, takže platí $\varphi(g) \cdot a = \varphi(g \cdot b) = \varphi(b \cdot g) = a \cdot \varphi(g)$. Pro každé $g \in Z(G)$ tedy vskutku je $\varphi(g) \in Z(G)$. $\square$

Tvrzení 3.3 se často používá souběžně s následujícím pozorováním:

3.4 Lemma. *Ať H je charakteristická podgrupa grupy K , $K \trianglelefteq G$. Pak $H \trianglelefteq G$. Je-li K navíc charakteristická v G , je i H charakteristická v G . Je-li H úplně charakteristická v K a K úplně charakteristická v G , je i H úplně charakteristická podgrupa grupy G .*

Důkaz. Pro $\varphi \in \text{Inn}(G)$ platí $\varphi(K) = K$, takže restrikce $\varphi|_K$ patří do $\text{Aut}(K)$, a je tedy $\varphi(H) = H$. Zbytek je snadný. $\square$

Podgrupa H grupy G se nazývá *subnormální*, jestliže existuje konečná posloupnost $H_1, \dots, H_k$ taková, že je $H = H_1 \triangleleft \dots \triangleleft H_k = G$. Je zřejmé, že pokud má grupa G alespoň jednu kompoziční řadu, tak subnormální grupy jsou právě všechny grupy, které se vyskytují ve všech kompozičních řadách.

3.5 Tvzení. *Platí $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ a zobrazení $G \rightarrow \text{Inn}(G)$, které $g \in G$ přiřazuje automorfismus $a \mapsto gag^{-1}$, je homomorfismus s jádrem $Z(G)$.*

Důkaz. Ať jsou g, h prvky G a ať $\varphi: a \mapsto gag^{-1}$ a $\psi: a \mapsto hah^{-1}$ jsou odpovídající vnitřní automorfismy. Pak $\psi\varphi(a) = (hg)a(hg)^{-1}$, takže popsané zobrazení $G \rightarrow \text{Inn}(G)$ je vskutku homomorfismus (viz též 1.6). Přitom platí $\varphi = 1_G$, právě když $gag^{-1} = a$ pro všechna $a \in G$, čili právě pro $g \in Z(G)$. K dokončení důkazu zbývá ukázat $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. Ať je $\alpha \in \text{Aut}(G)$. Pro všechna $a \in G$ platí $\alpha\varphi\alpha^{-1}(a) = \alpha(g \cdot \alpha^{-1}(a) \cdot g^{-1}) = \alpha(g) \cdot a \cdot (\alpha(g))^{-1}$. $\square$

Faktorgrupa $\text{Aut}(G)/\text{Inn}(G)$ se nazývá *vnější grupa automorfismů* a označuje se $\text{Out}(G)$.

Nyní sestrojíme takzvaná iterovaná centra $\vartheta_i(G)$, $i \geq 0$ (často se označu-

jí jako $Z_i(G)$). Protože budeme chtít dokázat, že $\vartheta_i(G)$ jsou charakteristické podgrupy grupy G , dokážeme nejprve tato dvě lemmata:

3.6 Lemma. *Ať $\varphi \in \text{Aut}(G)$, $N \trianglelefteq G$ a $\varphi(N) = N$. Potom $aN \mapsto \varphi(a)N$ je automorfismus grupy G/N .*

Důkaz. Buď $\pi: G \rightarrow G/N$ přirozená projekce. Potom $\pi\varphi: G \rightarrow G/N$ a dále $\text{Ker } \pi\varphi = N$, takže lze použít první větu o izomorfismu 1.13. $\square$

3.7 Lemma. *Ať N je charakteristická podgrupa grupy G a platí $N \leq K \leq G$. Je-li K/N charakteristická podgrupa grupy G/N , je K charakteristická podgrupa grupy G .*

Důkaz. Ať je $\varphi \in \text{Aut}(G)$. Pak $\varphi(N) = N$ a φ indukce automorfismus $\psi: aN \rightarrow \varphi(a)N$ grupy G/N . Z $\psi(K/N) = K/N$ plyne $\varphi(K) = K$. $\square$

Přistoupíme k sestrojení podgrup $\vartheta_i(G)$. Definice probíhá indukcí dle $i \geq 0$ a v každém kroku se ukazuje, že $\vartheta_i(G)$ je charakteristická podgrupa grupy G .

Klademe $\vartheta_0(G) = 1$. Ať je $i \geq 0$ a $\pi_i: G \rightarrow G/\vartheta_i(G)$ přirozená projekce. Pak $\vartheta_{i+1}(G) = \pi_i^{-1}(Z(G/\vartheta_i(G)))$. Podle tvrzení 3.3 je $Z(G/\vartheta_i(G))$ charakteristická podgrupa $G/\vartheta_i(G)$, takže $\vartheta_{i+1}(G)$ je charakteristická podgrupa G podle 3.7.

Grupa G se nazývá *nilpotentní*, jestliže pro některé $n \geq 0$ platí $\vartheta_n(G) = G$. Nejmenšímu takovému n se říká *stupeň nilpotence*. Je zřejmé, že nilpotentní grupy stupně 1 jsou právě všechny (netriviální) komutativní grupy. (Místo komutativní se často říká též abelovské.)

Řada $1 = \vartheta_0(G) \leq \vartheta_1(G) \leq \vartheta_2(G) \leq \dots$ se nazývá *horní centrální řada* grupy G . Je patrné, že tato řada poskytuje v případě nilpotentní grupy charakteristickou řadu, jejíž faktory jsou abelovské.

Prvek $g\vartheta_i(G)$ patří do centra $G/\vartheta_i(G)$, právě když pro všechny prvky $a \in G$ je $(g\vartheta_i(G)) \cdot (a\vartheta_i(G)) = ga\vartheta_i(G)$ rovno $ag\vartheta_i(G) = (a\vartheta_i(G)) \cdot (g\vartheta_i(G))$. Kritérium

$$g \in \vartheta_{i+1}(G) \iff \left(ga\vartheta_i(G) = ag\vartheta_i(G) \text{ pro všechna } a \in G \right)$$

využijeme v následujícím lemmatu.

3.8 Lemma.

- (i) Buď $\varphi: G \rightarrow H$ epimorfismus grup. Potom je $\varphi(\vartheta_i(G)) \leq \vartheta_i(H)$ pro všechna $i \geq 0$.
- (ii) Ať je $K \leq G$. Potom je $\vartheta_i(G) \cap K \leq \vartheta_i(K)$ pro všechna $i \geq 0$.

Důkaz. Indukcí dle $i \geq 0$, případ $i = 0$ je zřejmý.

- (i) Je-li $g \in \vartheta_{i+1}(G)$, je $ga\vartheta_i(G) = ag\vartheta_i(G)$ pro všechna $a \in G$, takže

$$\varphi(g)\varphi(a)\varphi(\vartheta_i(G)) = \varphi(a)\varphi(g)\varphi(\vartheta_i(G)) \text{ pro všechna } a \in G.$$

Protože $\varphi(a)$ probíhá H a $\varphi(\vartheta_i(G))$ leží v $\vartheta_i(H)$, platí

$$\varphi(g)b\vartheta_i(H) = b\varphi(g)\vartheta_i(H) \text{ pro všechna } b \in H.$$

- (ii) Ať je $g \in \vartheta_{i+1}(G) \cap K$. Pro všechna $k \in K$ platí

$$gk(\vartheta_i(G) \cap K) = K \cap gk\vartheta_i(G) = K \cap kg\vartheta_i(G) = kg(\vartheta_i(G) \cap K),$$

a z předpokladu $\vartheta_i(G) \cap K \leq \vartheta_i(K)$ tedy máme $gk\vartheta_i(K) = kg\vartheta_i(K)$. $\square$

3.9 Důsledek. *Buď G nilpotentní grupa stupně s . Potom každá podgrupa G i každá faktorgrupa G je nilpotentní stupně nanejvýš s .* $\square$

Prvky g, h grupy G nazveme *konjugované*, jestliže existuje $a \in G$ tak, že platí $aga^{-1} = h$. Volbou $a = 1$ dostáváme reflexivitu relace být konjugován, z $aga^{-1} = h$ plyne $g = a^{-1}ha$ (symetrie) a $aga^{-1} = h$, $bhb^{-1} = k$ dávají $(ba)g(ba)^{-1} = k$ (transitivita). Jde tedy o ekvivalenci, která indukce rozklad G do takzvaných *tříd konjugace* (někdy se říká dokonce jen tříd).

3.10 Lemma. *Ať $g \in G$ a C je třída konjugace obsahující g . Potom*

$$|C| = |G : C_G(g)|,$$

takže $C = \{g\}$, právě když je $g \in Z(G)$.

Důkaz. Pro $a, b \in G$ platí $aga^{-1} = bgb^{-1}$, právě když $b^{-1}ag = gb^{-1}a$, tedy právě když $b^{-1}a \in C_G(g)$. Počet různých hodnot tvaru aga^{-1} tudíž odpovídá počtu (levých) rozkladových tříd grupy G podle $C_G(g)$. $\square$

Podle definice bychom vlastně místo $C_G(g)$ měli psát $C_G(\{g\})$. Je to však běžná konvence, že místo množiny lze uvést prvek nebo seznam prvků. Přitom $C_G(g)$ je totéž jako $N_G(g)$, neboť u jednoprvkových množin pojmy centralizátoru a normalizátoru splývají.

Je-li $M \subseteq G$, tak $\langle M \rangle$ označuje nejmenší podgrupu G , která obsahuje M . Jak jsme již uvedli v kapitole 1, o této grupě se říká, že je *generovaná* množinou M . Řádem prvku $g \in G$ nazveme řád cyklické grupy $\langle g \rangle$ tímto prvkem generované. Je-li $\langle g \rangle$ konečná, mluvíme o prvku konečného řádu. Místo $|\langle g \rangle|$ se často píše pouze $|g|$.

O grupě G říkáme, že je *exponentu* m , jestliže $g^m = 1$ pro každé $g \in G$ a m je nejmenší takové kladné celé číslo. Grupa G je tedy exponentu m , právě když m je nejmenší společný násobek řádů jejích prvků.

Ať p je prvočíslo. Grupa G se nazývá *p-grupa*, jestliže pro každé $g \in G$ existuje $n \geq 0$ takové, že g má řád p^n .

Je-li G konečná grupa, řád každého prvku dělí $|G|$. Je-li $|G|$ mocninou prvočísla p , je tedy G jistě p -grupou. Později ukážeme, že platí i obrácené tvrzení.

Z lemmatu 3.10 okamžitě plyne:

3.11 Důsledek. Ať G je konečná grupa a ať v $R \subseteq G$ je právě po jednom reprezentantu z každé třídy konjugace, jež má alespoň dva prvky. Pak

$$|G| = |Z(G)| + \sum_{g \in R} |G : C_G(g)|. \quad \square$$

3.12 Tvrzení. Ať je $|G| = p^n$, kde p je prvočíslo a $n \geq 1$. Potom je $Z(G) \neq 1$.

Důkaz. Použijeme vyjádření $|G|$ uvedené v 3.11. Prvky $g \in R$ neleží v centru, takže $C_G(g) \neq G$ a $|G : C_G(g)|$ je tedy celé kladné číslo dělitelné prvočíslem p . Protože p dělí i $|G|$, musí p dělit $|Z(G)|$. $\square$

3.13 Důsledek. Je-li řád grupy G prvočíselnou mocninou, je G nilpotentní grupa. $\square$

Pro $a, b \in G$ definujeme *komutátor* $[a, b]$ jako $a^{-1}b^{-1}ab$. (Někdy se místo $[a, b]$ píše (a, b) .)

Jsou-li A, B podgrupy grupy G , tak $[A, B]$ označuje podgrupu generovanou množinou $\{[a, b]; a \in A \text{ a } b \in B\}$. Grupě $[G, G]$ se říká *komutant* G a označuje se G' . Pro iterované komutanty se používá jak značení $G'', G''', \dots$, tak značení $G^{(2)}, G^{(3)}, \dots$.

Formálně tedy máme $G^{(0)} = G$, $G^{(i+1)} = [G^{(i)}, G^{(i)}]$. Grupa G se nazývá *řešitelná*, jestliže $G^{(n)} = 1$ pro nějaké $n \geq 0$. Nejmenší takové n se nazývá *stupeň řešitelnosti* grupy G . Je zřejmé, že grupy stupně řešitelnosti 1 jsou právě všechny netriviální abelovské grupy.

3.14 Lemma. G' je úplně charakteristická podgrupa grupy G . Pro $N \trianglelefteq G$ platí $N \geq G'$, právě když je G/N abelovská.

Důkaz. Každý endomorfismus $\varphi \in \text{End}(G)$ převádí pro libovolné $a, b \in G$ komutátor $[a, b]$ na $[\varphi(a), \varphi(b)]$. Proto je G' úplně charakteristická. Pro $N \trianglelefteq G$ je G/N abelovská, právě když pro libovolné $a, b \in G$ je $Nab = Nba$, čili $[a, b] \in N$, a tedy $G' \leq N$. $\square$

3.15 Lemma. Je-li $H \leq G$, tak $H^{(i)} \leq G^{(i)}$ pro všechna $i \geq 0$. Je-li grupa G řešitelná, je grupa H řešitelná a má stejný nebo menší stupeň řešitelnosti.

Důkaz. Snadnou indukcí dle $i \geq 0$. Příklad $i = 0$ je zřejmý a z $H^{(i)} \leq G^{(i)}$ plyne $[H^{(i)}, H^{(i)}] \leq [G^{(i)}, G^{(i)}]$. $\square$

Z 3.14 a 3.4 plyne, že $G^{(i)}$ je úplně charakteristická podgrupa grupy G pro všechna $i \geq 0$. Můžeme tedy říci, že G je řešitelná stupně řešitelnosti nejvýše s , právě když $1 = G^{(s)}, G^{(s-1)}, \dots, G^{(0)} = G$ je úplně charakteristická řada. Faktory $G^{(i)}/G^{(i+1)}$ jsou podle 3.14 abelovské.

3.16 Tvrzení. Grupa G je řešitelná, právě když existuje subnormální řada $1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = G$, jejíž všechny faktory jsou abelovské. Přitom stupeň řešitelnosti G je roven nanejvýš m .

Důkaz. Indukcí podle m . Příklad $m = 0$ je zřejmý, předpokládejme $m > 0$. Podle indukčního předpokladu je H_{m-1} řešitelná stupně nejvýš $m-1$. Podle lemmatu 3.14 je $G' \leq H_{m-1}$, takže podle 3.15 je $(G')^{(m-1)} = G^{(m)}$ rovno 1. $\square$

3.17 Důsledek. Podgrupy a faktorgrupy řešitelné grupy G jsou řešitelné a jejich stupeň řešitelnosti nepřesahuje stupeň řešitelnosti G .

Důkaz. Pro podgrupy lze použít 3.15. Je-li $1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = G$ subnormální řada s abelovskými faktory, tak $H_0N/N \trianglelefteq H_1N/N \trianglelefteq \dots \trianglelefteq H_mN/N$ je subnormální řada G/N s abelovskými faktory. $\square$

3.18 Důsledek. Ať je $N \trianglelefteq G$ a ať N i G/N jsou řešitelné. Pak je i G řešitelná grupa. Je-li r stupeň řešitelnosti N a s stupeň řešitelnosti G/N , má G stupeň řešitelnosti nejvýš $r + s$.

Důkaz. Ať $1 = K_0 \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K_r = N$ a $1 = H_0/N \trianglelefteq H_1/N \trianglelefteq \dots \trianglelefteq H_s/N = G/N$ jsou subnormální řady s abelovskými faktory. Pak $1 = K_0 \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K_r = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_s = G$ je také subnormální řada s abelovskými faktory (použij například Druhou větu o izomorfismu 1.19). $\square$

Je-li G nilpotentní, tak je řešitelná, neboť horní centrální řada má abelovské faktory. Řešitelné grupy však nemusí být nilpotentní — jednoduchým příkladem je symetrická grupa S_4 .

4 Součiny

Konečný kartézský součin $M_1 \times M_2 \times \dots \times M_n$ množin M_i , $1 \leq i \leq n$, je nejběžnější reprezentovat jako n -tice $(m_1, m_2, \dots, m_n)$. Pokud ale pracujeme i s nekonečnými kartézskými součiny $\times_{i \in I} M_i$, je z hlediska zápisu vhodné tento součin interpretovat jako $\{a: I \rightarrow \bigcup_{i \in I} M_i; a(i) \in M_i\}$. Pro konečné součiny to znamená, že $(m_1, m_2, \dots, m_n)$ ztotožňujeme se zobrazením $m: \{1, 2, \dots, n\} \rightarrow \bigcup M_i$, $m(i) = m_i \in M_i$.

Jsou-li G_i , $i \in I \neq \emptyset$, grupy, tak jejich *kartézský součin* $\prod_{i \in I} G_i$ je grupa definovaná na $\times_{i \in I} G_i$ s neutrálním prvkem $e: i \mapsto 1$, inverzními prvky $a^{-1}: i \mapsto (a(i))^{-1}$ a binární operací $a \cdot b: i \mapsto a(i)b(i)$. Ověřit, že jde vskutku o grupu, je snadné. Stejně tak je snadné nahlédnout, že projekce $\pi_j: a \mapsto a(j)$ je epimorfismem $\prod_{i \in I} G_i \rightarrow G_j$ pro každé $j \in I$.

Uvažme podmnožinu $\times_{i \in I} G_i$ tvořenou všemi zobrazeními a , pro která $a(i) \neq 1$ platí pouze pro konečně mnoho $i \in I$. Tato podmnožina zjevně tvoří podgrupu $\prod_{i \in I} G_i$. Budeme ji značit $\coprod_{i \in I} G_i$ a nazývat *direktní součin*. Pro každé $j \in I$ definujeme zobrazení $\mu_j: G_j \rightarrow \prod_{i \in I} G_i$ tak, že pro $g \in G_j$ a $i \neq j$ platí $\mu_j(g)(j) = g$ a $\mu_j(g)(i) = 1$. Je zřejmé, že $\mu_j: G_j \rightarrow \prod_{i \in I} G_i$ je monomorfismus (prvky $\mu_j(G_j)$ jsou všechny I -tice, které mohou mít pouze j -tou složku různou od 1).

4.1 Lemma. Ať G_i , $i \in I \neq \emptyset$, jsou grupy a $G = \prod_{i \in I} G_i$. Potom

- (i) $\mu_j(G_j) \trianglelefteq G$ pro všechna $j \in I$;
- (ii) $\mu_j(G_j) \cap \langle \mu_i(G_i); i \in I, i \neq j \rangle = 1$ pro každé $j \in I$;
- (iii) $\langle \mu_i(G_i); i \in I \rangle = G$.

Důkaz. Buď $j \in I$, $b \in \mu_j(G_j)$ a $a \in G$. Pro index $i \neq j$ je jistě $aba^{-1}(i) = a(i)(a(i))^{-1} = 1$, takže $aba^{-1} \in \mu_j(G_j)$. Je-li $a \in \langle \mu_i(G_i); i \in I, i \neq j \rangle$, tak platí $a(j) = 1$, odsud (ii). Konečně platí, že $a(i) \neq 1$ jen pro konečně mnoho indexů $i_1, i_2, \dots, i_r$, takže $a = \mu_{i_1}(a(i_1)) \cdot \mu_{i_2}(a(i_2)) \cdot \dots \cdot \mu_{i_r}(a(i_r))$. $\square$

Ukážeme, že vlastnosti podgrup $\mu_i(G_i) \cong G_i$ uvedené v 4.1 plně charakterizují direktní součin grup v tom smyslu, že kdykoliv najdeme podgrupy grupy G splňující tyto vlastnosti, tak G je izomorfní direktnímu součinu těchto grup.

4.2 Lemma. *At $H \trianglelefteq G$, $K \trianglelefteq G$ a $H \cap K = 1$. Pak $hk = kh$ pro všechna $h \in H$ a $k \in K$.*

Důkaz. Komutátor $[h, k] = h^{-1}k^{-1}hk$ patří do $H \cap K$. □

4.3 Tvzení. *At G je grupa s normálními podgrupami N_i , $i \in I$. Jestliže platí $\langle N_i; i \in I \rangle = G$ a pro každé $j \in I$ je $N_j \cap \langle N_i; i \in I, i \neq j \rangle = 1$, tak zobrazení $\alpha: \prod_{i \in I} N_i \rightarrow G$, $\alpha(a) = \prod_{i \in I} a(i)$, je izomorfismus grup.*

Důkaz. Nejprve musíme ověřit korektnost definice. Ať je $a(i) \neq 1$ pro $i \in \{i_1, i_2, \dots, i_r\}$ a $a(i) = 1$ v ostatních případech. Hodnota $\prod_{i \in I} a(i)$ závisí jen na hodnotách $a(i_1), a(i_2), \dots, a(i_r)$ a je určena jednoznačně, jestliže pro libovolnou permutaci $\sigma \in S_r$ platí $a(i_1) \cdot a(i_2) \cdot \dots \cdot a(i_r) = a(i_{\sigma(1)}) \cdot a(i_{\sigma(2)}) \cdot \dots \cdot a(i_{\sigma(r)})$. To však je podle 4.2 a podmínek tvrzení splněno. Stejně tak z 4.2 plyne, že $\alpha(ab) = \alpha(a)\alpha(b)$ pro všechna $a, b \in \prod_{i \in I} N_i$. Protože $\alpha(\mu_i(g)) = g$ pro každé $g \in N_i$, $i \in I$, vidíme, že platí $\alpha(\mu_i(N_i)) = N_i$, takže z $\langle N_i; i \in I \rangle = G$ plyne, že α je epimorfismus. Jeho jádro je zjevně triviální, takže vskutku jde o izomorfismus. □

Jestliže podgrupy $N_i \trianglelefteq G$ splňují podmínky tvrzení 4.3, často píšeme přímo $G = \prod_{i \in I} N_i$ a ztotožňujeme tak vzor a obraz zkonstruovaného izomorfismu.

Direktní součin dvou grup tedy popisuje situaci, kdy grupu G je možno vyjádřit ve tvaru $G = HK$, $H \cap K = 1$, $H \trianglelefteq G$ a $K \trianglelefteq G$. Pak $(h, k) \mapsto hk$ je izomorfismus $H \times K$ na G . Situaci, kdy platí $G = HK$, $H \cap K = 1$, $H \trianglelefteq G$ a $K \leq G$, vystihuje konstrukce semidirektního součinu.

Jejími parametry jsou grupy H, K a homomorfismus $\varphi: K \rightarrow \text{Aut}(H)$. Místo $\varphi(k)$, $k \in K$, budeme psát φ_k . Pro každé $k \in K$ je tedy φ_k automorfismem H a platí $\varphi_{k_1 k_2} = \varphi_{k_1} \varphi_{k_2}$.

Semidirektní součin $S(H, K, \varphi)$ je grupa definovaná na $H \times K$ binární operací $(h_1, k_1) \cdot (h_2, k_2) = (h_1 \varphi_{k_1}(h_2), k_1 k_2)$ s inverzními prvky $(h, k)^{-1} = (\varphi_k^{-1}(h^{-1}), k^{-1})$ a neutrálním prvkem $(1, 1)$.

Je samozřejmě třeba ověřit, že se jedná o grupu. Protože φ_1 je identický

automorfismus, tak jistě máme $(h, k)(1, 1) = (h, k) = (1, 1)(h, k)$. Podobně

$$\begin{aligned} (h, k)^{-1} \cdot (h, k) &= \\ (\varphi_k^{-1}(h^{-1})\varphi_k^{-1}(h), k^{-1}k) &= \\ (\varphi_k^{-1}(1), 1) = (1, 1) &= (h\varphi_k\varphi_k^{-1}(h^{-1}), kk^{-1}) \\ &= (h, k) \cdot (h, k)^{-1}. \end{aligned}$$

Zbývá ověřit asociativitu. Platí

$$\begin{aligned} ((h_1, k_1) \cdot (h_2, k_2)) \cdot (h_3, k_3) &= (h_1 \varphi_{k_1}(h_2), k_1 k_2) \cdot (h_3, k_3) \\ &= (h_1 \varphi_{k_1}(h_2) \varphi_{k_1 k_2}(h_3), k_1 k_2 k_3) \end{aligned}$$

a

$$\begin{aligned} (h_1, k_1) \cdot ((h_2, k_2) \cdot (h_3, k_3)) &= (h_1, k_1) \cdot (h_2 \varphi_{k_2}(h_3), k_2 k_3) \\ &= (h_1 \varphi_{k_1}(h_2 \varphi_{k_2}(h_3)), k_1 k_2 k_3), \end{aligned}$$

přičemž $\varphi_{k_1}(h_2 \varphi_{k_2}(h_3))$ je rovno $\varphi_{k_1}(h_2) \varphi_{k_1}(\varphi_{k_2}(h_3)) = \varphi_{k_1}(h_2) \varphi_{k_1 k_2}(h_3)$.

4.4 Lemma. *At H a K jsou grupy a $\varphi: K \rightarrow \text{Aut}(H)$ je homomorfismus grup. Položme $\tilde{H} = \{(h, 1); h \in H\}$, $\tilde{K} = \{(1, k); k \in K\}$ a $G = S(H, K, \varphi)$. Pak platí $\tilde{H} \trianglelefteq G$, $\tilde{K} \leq G$, $\tilde{H} \cap \tilde{K} = 1$ a $\tilde{H}\tilde{K} = \tilde{K}\tilde{H} = G$.*

Důkaz. Vztahy $\tilde{H} \leq G$, $\tilde{K} \leq G$ a $\tilde{H} \cap \tilde{K} = 1$ jsou očividné a z $(h, 1) \cdot (1, k) = (h, k)$ plyne $\tilde{K}\tilde{H} = G$. Zbývá ukázat normalitu $\tilde{H}$. Ať je $g \in H$ a $(h, k) \in H \times K$. Platí $(h, k) \cdot (g, 1) \cdot (\varphi_k^{-1}(h^{-1}), k^{-1}) = (h\varphi_k(g), k) \cdot (\varphi_k^{-1}(h^{-1}), k^{-1}) = (h\varphi_k(g)h^{-1}, 1)$. □

Položíme-li v poslední identitě $h = 1$, vidíme, že vnitřní automorfismus příslušný prvku $(1, k)$ se na $\tilde{H}$ shoduje s φ_k . To je také důvod, proč při splnění vztahů uvedených v závěru předchozího lemmatu je možné G ztotožnit se semidirektním součinem.

4.5 Tvzení. *At G je grupa s podgrupami $H \trianglelefteq G$, $K \leq G$ takovými, že $H \cap K = 1$ a $HK = G$. Pro každý prvek $k \in K$ označme φ_k restrikci vnitřního automorfismu $g \mapsto kgk^{-1}$ na H . Pak $k \mapsto \varphi_k$ je homomorfismus $K \rightarrow \text{Aut}(H)$ a $(h, k) \mapsto hk$ je izomorfismus $S(H, K, \varphi) \rightarrow G$.*

Důkaz. To, že $\varphi: K \rightarrow \text{Aut}(H)$ je homomorfismus, plyne z 3.5 a faktu, že H je normální podgrupa G (φ vznikne složením restrikce homomorfismu $G \rightarrow \text{Inn}(G)$ na K s homomorfismem $\text{Inn}(G) \rightarrow \text{Aut}(H)$, který každému vnitřnímu automorfismu přiřazuje jeho restrikci na H – zde užíváme normalitu H). Zobrazení $(h, k) \mapsto hk$ je bijekce $H \times K$ na G , neboť z $h_1k_1 = h_2k_2$ plyne $h_2^{-1}h_1 = k_2k_1^{-1} \in K \cap H = 1$, takže $h_2 = h_1$ a $k_2 = k_1$. Zbývá ukázat, že jde o homomorfismus. Ovšem $(h_1, k_1) \cdot (h_2, k_2) = (h_1\varphi_{k_1}(h_2), k_1k_2)$ se zobrazí na $h_1\varphi_{k_1}(h_2)k_1k_2 = h_1k_1h_2k_1^{-1}k_1k_2 = h_1k_1 \cdot h_2k_2$. $\square$

5 Sumy abelovských grup

V této kapitole budeme pracovat pouze s abelovskými grupami, a proto budeme používat výhradně aditivní notaci. V aditivní notaci se inverzním prvkům říká *opačné* a značí se $-a$. Neutrální prvek se klade roven 0 a místo direktní součín se říká *direktní suma*, značeno $\bigoplus_{i \in I} G_i$. V abelovské grupě jsou všechny podgrupy normální, takže faktorgrupu G/H lze sestrojit ke každé podgrupě $H \leq G$.

Otázku, kdy danou Abelovu grupu G je možno vyjádřit jako direktní sumu jejích podgrup, je možno řešit pomocí 4.3. U Abelových grup však můžeme podmínky tohoto tvrzení formulovat o něco silněji, neboť pro $H_i \leq G$, $i \in I$, je $\langle H_i; i \in I \rangle$ rovno $\sum H_i = \{\sum_{i \in I} h_i; h_i \in H_i \text{ a } h_i \neq 0 \text{ jen pro konečně mnoho } i \in I\}$. (V zápisu $\sum_{i \in I} h_i$ se v dalším vždy předpokládá, že je $h_i \neq 0$ jen pro konečně mnoho $i \in I$.)

Tak, jak je obvyklé, budeme psát $G = \bigoplus_{i \in I} H_i$ i v případě, kdy H_i jsou podgrupy G a zobrazení $\alpha: \bigoplus_{i \in I} H_i \rightarrow G$, $\alpha(\sum h_i) = \sum \alpha(h_i)$ je izomorfismus (viz 4.3 a za ním následující poznámku).

Tvrzení 4.3 nyní můžeme vyslovit v následující formě.

5.1 Tvrzení. *Ať G je abelovská grupa a ať H_i , $i \in I$, jsou její podgrupy. Potom G je rovno $\bigoplus_{i \in I} H_i$, právě když je splněna některá z následujících dvou ekvivalentních podmínek.*

- (i) Platí $G = \sum_{i \in I} H_i$ a z $\sum_{i \in I} h_i = 0$, $h_i \in H_i$, vždy plyne $h_i = 0$ pro

všechna $i \in I$.

- (ii) Každý prvek $g \in G$ lze vyjádřit právě jedním způsobem jako $\sum_{i \in I} h_i$, kde $h_i \in H_i$. $\square$

Ať G je abelovská grupa. Prvky konečného řádu se v abelovských grupách někdy nazývají *torzní*. Množině všech torzních prvků grupy G se říká *torzní část*. Jsou-li všechny prvky G torzní, mluvíme o G jako o *torzní grupě*. Je-li 0 jediným torzním prvkem G , nazýváme G *beztorzní grupou*.

5.2 Tvrzení. *Ať je G abelovská grupa a T její torzní část. Pak T je podgrupa grupy G a faktorgrupa G/T je beztorzní grupa.*

Důkaz. Ať jsou $a, b \in T$. Pak $ra = 0 = sb$ pro nějaká $r > 0$, $s > 0$. Zjevně platí $r(-a) = 0 = (rs)(a+b)$, takže T je vskutku podgrupa. Ať $r(g+T) = T$ pro nějaké $g \in G$ a $r > 0$. To znamená $rg \in T$, takže $s(rg) = 0$ pro nějaké $s > 0$. Odsud plyne $(sr)g = 0$, a tedy $g \in T$. Vidíme, že G/T je beztorzní. $\square$

Podmnožina B abelovské grupy G se nazývá *volná báze*, jestliže libovolné zobrazení $\varphi: B \rightarrow H$, kde H je abelovská grupa, lze rozšířit na homomorfismus $\psi: G \rightarrow H$, a navíc $\langle B \rangle = G$. ($\mathbb{Z} \langle B \rangle = G$ samozřejmě plyne, že homomorfismus ψ je určen jednoznačně.)

5.3 Lemma. *Předpokládejme, že B_1 a B_2 jsou stejně mohutné množiny, přičemž B_1 je volnou bází abelovské grupy G_1 a B_2 je volnou bází abelovské grupy G_2 . Potom jsou G_1 a G_2 izomorfní.*

Důkaz. Ať $\varphi: B_1 \rightarrow B_2$ je bijekce a ať $\psi_1: G_1 \rightarrow G_2$ je homomorfismus rozšiřující φ , zatímco $\psi_2: G_2 \rightarrow G_1$ je homomorfismus rozšiřující φ^{-1} . Pak $\psi_2\psi_1$ rozšiřuje id_{B_1} a $\psi_1\psi_2$ rozšiřuje id_{B_2} . Protože id_{G_i} také rozšiřuje id_{B_i} , $i = 1, 2$, vidíme, že platí $\psi_2\psi_1 = \text{id}_{G_1}$ a $\psi_1\psi_2 = \text{id}_{G_2}$, takže ψ_1 a ψ_2 jsou vzájemně inverzní izomorfismy. $\square$

Buď $I \neq \emptyset$. Podle definice direktní sumy se grupa $F = \bigoplus_{i \in I} \mathbb{Z}$ skládá ze všech zobrazení $a: I \rightarrow \mathbb{Z}$ takových, že $a(i) \neq 0$ pro konečně mnoho $i \in I$. Pro každé $i \in I$ označme f_i ten prvek $a \in F$, pro který $a(i) = 1$ a $a(j) = 0$, je-li $j \in I$ a $j \neq i$. Je zřejmé, že každé $a \in F$ lze vyjádřit jako $\sum a(i)f_i$.

5.4 Lemma. *At H je abelovská grupa a at $h_i \in H$ pro každé $i \in I$, $I \neq \emptyset$. Zobrazení $\varphi : F \rightarrow H$, $a \mapsto \sum a(i)h_i$, je jediný homomorfismus grup $F \rightarrow H$, který zobrazí f_i na h_i pro každé $i \in I$.*

Důkaz. Je-li $\psi : F \rightarrow H$ takový homomorfismus, musí být $\psi(a) = \psi(\sum a(i)f_i) = \sum a(i)\psi(f_i) = \sum a(i)h_i = \varphi(a)$. Přitom pro $a, c \in F$ je $\varphi(a + c) = \sum (a + c)(i)h_i = \sum (a(i) + c(i))h_i = \sum a(i)h_i + \sum c(i)h_i = \varphi(a) + \varphi(c)$. $\square$

Z 5.4 plyne, že $\{f_i; i \in I\}$ je volnou bází abelovské grupy F . Toho využijeme pro popis všech volných abelovských grup.

5.5 Tvzení. *At je G abelovská grupa a at $B \subseteq G$ generuje G . Potom je ekvivalentní:*

- (i) B je volná báze G ;
- (ii) $G = \bigoplus_{b \in B} \langle b \rangle$, kde $\langle b \rangle \cong \mathbb{Z}$ pro všechna $b \in B$;
- (iii) pro každou konečnou podmnožinu $C \subseteq B$ platí $\sum_{c \in C} a_c c = 0$, kde $a_c \in \mathbb{Z}$, jedině tehdy, je-li $a_c = 0$ pro každé $c \in C$;
- (iv) pro každou konečnou podmnožinu $C \subseteq B$ platí $\sum_{c \in C} a_c c = \sum_{c \in C} b_c c$, kde a_c a b_c jsou celá čísla, právě tehdy, když je $a_c = b_c$ pro všechna $c \in C$.

Důkaz. Platí-li (iii) nebo (iv), tak okamžitě vidíme, že každé $b \in B$ je nekonečného řádu. Ekvivalence (ii), (iii) a (iv) je proto jen zvláštním případem 5.1. Položme $I = B$. Homomorfismus $\varphi : F \rightarrow G$, $a \mapsto \sum a(b)b$, který existuje podle 5.4, je vždy surjektivní, neboť B generuje G . Pokud platí (iii), tak je injektivní, takže je izomorfismem a $B = \{\varphi(f_b); b \in B\}$ je volnou bází, protože je obrazem volné báze. Naopak, je-li B volnou bází, tak existuje homomorfismus $G \rightarrow F$, který zobrazuje $b \in B$ na $f_b \in F$. Tento homomorfismus je inverzí φ , takže φ je izomorfismus i v tomto případě, a proto platí (iii). $\square$

Grupa, ve které lze nalézt (aspoň jednu) volnou bází, se nazývá *volná*.

5.6 Tvzení. *Každá konečně generovaná beztorzní abelovská grupa je volná.*

Důkaz. At G je beztorzní a $G = \langle b_1, \dots, b_n \rangle$, kde n je nejmenší možné. Předpokládejme, že G není volná, a ze všech $(h_1, \dots, h_n) \neq (0, \dots, 0)$, které splňují $\sum_{i=1}^n h_i b_i = 0$, vyberme takovou, aby $h = \min\{|h_i|; 1 \leq i \leq n, h_i \neq 0\}$ bylo nejmenší možné. Je-li $G = \langle b'_1, \dots, b'_n \rangle$, tak stejným způsobem určíme hodnotu h' a $\{b_1, \dots, b_n\}$ vybereme tak, aby vždy platilo $h \leq h'$.

Bez újmy na obecnosti můžeme předpokládat $h_1 = h$. At h nedělí některou z hodnot h_i , například h_2 . Pak $h_2 = hq + r$, kde q a r jsou celá čísla a $0 < r < h$. Položme $s = \sum_{i \geq 3} h_i b_i$. Platí $0 = s + (hq + r)b_2 + hb_1 = s + rb_2 + h(qb_2 + b_1)$. Tím však dostáváme spor, neboť je $G = \langle b_1 + qb_2, b_2, \dots, b_n \rangle$ a $0 < r < h$.

Vidíme tedy, že $h_i = hk_i$ pro každé i , $1 \leq i \leq n$, takže $\sum_{i=1}^n h_i b_i$ se rovná $h(\sum_{i=1}^n k_i b_i)$, a k_1 je 1. Ovšem $h > 0$ a G je beztorzní, takže $\sum_{i=1}^n h_i b_i = 0$ implikuje $\sum_{i=1}^n k_i b_i = 0$, a tedy $b_1 = -\sum_{i \geq 2} k_i b_i$. To je však spor s minimalitou velikosti báze. $\square$

5.7 Tvzení. *At G je volná abelovská grupa. Pak všechny její volné báze mají stejnou mohutnost.*

Důkaz. At B_i , $i = 1, 2$, jsou dvě volné báze. Každý prvek G lze vyjádřit jako sumu násobků konečného počtu generátorů z B_i . To jednak znamená, že $|G| = |B_i|$, je-li volná báze B_i nekonečná, jednak z konečnosti B_1 plyne, že k vyjádření prvků B_1 potřebujeme jen konečně mnoho prvků B_2 , takže v takovém případě je i B_2 konečná. Můžeme tedy předpokládat, že B_1 a B_2 jsou konečné.

Položme $N = \{2a; a \in G\}$. Pak N je podgrupa G a je-li $\{x_1, x_2, \dots, x_k\}$ volná báze G , tak $N = \{\sum_{i=1}^k a_i x_i; a_i \text{ je sudé}\}$. Odsud plyne $|G/N| = 2^k$, takže $|B_1| = |B_2|$ dostáváme z $2^{|B_1|} = 2^{|B_2|}$. $\square$

5.8 Tvzení. *At H je taková podgrupa abelovské grupy G , že G/H je volná abelovská grupa. Pak $G = H \oplus F$ pro nějakou podgrupu $F \leq G$, $F \cong G/H$.*

Důkaz. Uvažme takovou $B \subseteq G$, že $b + H \neq c + H$ pro libovolná $b, c \in B$, $b \neq c$, a že $\{b + H; b \in B\}$ je volná báze G/H . Je-li $C \subseteq B$ konečná a $\sum_{c \in C} a_c c \in H$, tak $\sum_{c \in C} a_c (c + H) = 0$, takže $a_c = 0$ pro všechna $c \in C$. To ovšem znamená, že je $\langle B \rangle \cap H = 0$. Protože $\{b + H; b \in B\}$ generuje G/H , vidíme, že také platí $\langle B \rangle + H = G$, takže lze položit $F = \langle B \rangle$. $\square$

5.9 Důsledek. Je-li G konečně generovaná abelovská grupa, tak G lze vyjádřit jako $T \oplus F$, kde T je torzní část, která je konečně generovaná, a F je konečně generovaná volná grupa.

Důkaz. Vzhledem k 5.6 a 5.8 si stačí uvědomit, že je-li $G = \langle M \rangle$ a $N \trianglelefteq G$, tak $G/N = \langle a + N; a \in M \rangle$. $\square$

Je-li G abelovská grupa a p prvočíslo, tak $G_{(p)} = \{a \in G; p^n a = 0 \text{ pro nějaké } n \geq 1\}$ se nazývá *p-primární komponenta* grupy G . Protože $p^n a = 0$ a $p^m b = 0$ implikují $p^n(-a) = 0$ a $p^{\max(n,m)}(a+b) = 0$, vidíme, že $G_{(p)}$ tvoří podgrupu grupy G .

5.10 Tvzení. Bud' G torzní abelovská grupa. Pak $G = \bigoplus_{p \in \mathbb{P}} G_{(p)}$, kde $\mathbb{P}$ značí množinu všech prvočísel.

Důkaz. Ať $a \in G$ má řád nm , přičemž $n > 1$ a $m > 1$ jsou nesoudělná. Pak existují $r, s \in \mathbb{Z}$ taková, že je $rn + sm = 1$, takže $rna + sma = a$, přičemž m dělí řád rna a n dělí řád sma . Odsud je patrné, že platí $\langle G_{(p)}; p \in \mathbb{P} \rangle = G$. Vyberme $q \in \mathbb{P}$ a ať $\widehat{G} = \langle G_{(p)}; p \in \mathbb{P} \setminus \{q\} \rangle$. Je-li $a \in \widehat{G}$, řád a není dělitelný prvočíslem q . Proto platí $G_{(q)} \cap \widehat{G} = 0$ a zbytek plyne z 4.3. $\square$

Pro torzní grupu $G = \langle B \rangle$ je každý prvek $g \in G$ možno vyjádřit jako $\sum_{b \in B} a_b b$, kde $a_b \neq 0$ jen pro konečně mnoho $b \in B$, a v těchto případech je $0 < a_b < o(b)$, kde $o(b)$ je řád prvku b . Odsud plyne, že G je konečně generovaná, právě když je konečná.

Ať G je abelovská p -grupa. Pak $S = \{a \in G; pa = 0\}$ zjevně tvoří podgrupu grupy G , říká se jí *dolní vrstva*. Na S můžeme pohlížet též jako na vektorový prostor nad tělesem $\mathbb{Z}_p$, a tím pádem S je možno vyjádřit jako $\bigoplus_{b \in B} \langle b \rangle$, kde B je nějaká báze tohoto vektorového prostoru.

5.11 Lemma. Ať G je abelovská p -grupa a ať S je její dolní vrstva. Pro $a \in G \setminus S$ platí, že je řádu p^{k+1} , právě když $a + S \in G/S$ je řádu p^k .

Důkaz. Ať $|a + S| = p^h$ a $|a| = p^k$, přičemž $a \notin S$. Je tedy $h \geq 1$ a $k \geq 2$. Z $p(p^{k-1}a) = 0$ plyne $p^{k-1}a \in S$, takže $h \leq k - 1$. Z $p^h a \in S$ plyne $h + 1 \geq k$. $\square$

5.12 Lemma. Ať G je konečná p -grupa a ať S je její dolní vrstva. Necht'

$B = \langle g_1, \dots, g_k \rangle$, kde $g_i \in G \setminus S$, $1 \leq i \leq k$. Potom $B = \bigoplus (\langle g_i \rangle; 1 \leq i \leq k)$ právě když $(B + S)/S = \bigoplus (\langle g_i + S \rangle; 1 \leq i \leq k)$.

Důkaz. Podle 5.1 první vztah platí, pokud je splněna implikace

$$\sum \lambda_i g_i = 0 \Rightarrow p^{h_i} \mid \lambda_i \text{ pro každé } i \in \{1, \dots, k\},$$

kde $p^{h_1}, \dots, p^{h_k}$ jsou řády prvků $g_1, \dots, g_k$.

Z 5.11 vidíme, že druhý vztah odpovídá implikaci

$$\sum \nu_i (g_i + S) = S \Rightarrow p^{h_i-1} \mid \nu_i \text{ pro každé } i \in \{1, \dots, k\}.$$

To lze zapsat také jako

$$\sum \nu_i g_i \in S \Rightarrow p^{h_i-1} \mid \nu_i \text{ pro každé } i \in \{1, \dots, k\}.$$

Je-li $\sum \nu_i g_i \in S$, je $\sum p \nu_i g_i = 0$, takže prvá z uvedených implikací dostačuje pro platnost druhé.

Nyní budeme dokazovat opačný směr. Ať $\sum \lambda_i g_i = 0$. Pak $\sum \lambda_i g_i \in S$, a proto $p_i^{h_i-1} \mid \lambda_i$. Máme $g_i \notin S$, a tedy $h_i \geq 2$. Položme $\nu_i = \lambda_i/p$. Z $p(\sum \nu_i g_i) = 0$ plyne $\sum \nu_i g_i \in S$, takže $p_i^{h_i-1} \mid \nu_i$ a $p_i^{h_i} \mid \lambda_i$. $\square$

5.13 Lemma. Ať G je konečná abelovská p -grupa. Pak je G možno vyjádřit jako direktní sumu cyklických grup.

Důkaz. Budeme postupovat indukcí dle $|G|$. Označme S dolní vrstvu G . Je-li $G = S$, tak lemma plyne z toho, že G můžeme chápat jako vektorový prostor nad $\mathbb{Z}_p$. Ať je $G \neq S$. Potom z indukčního předpokladu plyne existence $a_i \in G \setminus S$, $1 \leq i \leq k$, takových, že $G/S = \langle a_1 + S \rangle \oplus \dots \oplus \langle a_k + S \rangle$. Označme H podgrupu G generovanou prvky $a_1, \dots, a_k$. Podle 5.12 je $H = \langle a_1 \rangle \oplus \dots \oplus \langle a_k \rangle$. Z vlastností vektorových prostorů vyplývá existence $U \leq S$ takového, že $S = (H \cap S) \oplus U$. Máme $H \cap U = 0$, a $H + U = G$ plyne z $H + S = G$ a $S \subseteq H + U$. Tudíž $G = H \oplus U$, přičemž každý z obou sčítanců lze vyjádřit jako direktní sumu cyklických grup. $\square$

5.14 Lemma. Ať A_i , $1 \leq i \leq m$, jsou cyklické grupy řádu p^{a_i} , $1 \leq a_1 \leq \dots \leq a_m$, a B_j , $1 \leq j \leq n$, jsou cyklické grupy řádu p^{b_j} , $1 \leq b_1 \leq \dots \leq b_n$.

Je-li $\bigoplus_{i=1}^m A_i \cong \bigoplus_{j=1}^n B_j$, tak platí $n = m$ a $a_i = b_i$ pro všechna i , $1 \leq i \leq n$.

Důkaz. Položme $G = \bigoplus A_i$, ať S je dolní vrstva G a ať g_i generuje A_i , $1 \leq i \leq m$. Prvky $p^{a_i-1}g_i$ leží v S a každý prvek S je jejich jednoznačnou lineární kombinací. Proto $n = m = \dim S$. Postupujeme dále indukcí podle řádu G . Je-li $G = S$, není co dokazovat. Ať tedy S je vlastní podgrupa G .

Označme m_1 počet hodnot a_i , které jsou rovné 1. Podobně ať n_1 označuje počet b_i rovných 1. Z 5.12 plyne $G/S = \langle g_{m_1+1} + S \rangle \oplus \cdots \oplus \langle g_m + S \rangle$, takže indukční předpoklad dává $m - m_1 = m - n_1$ a $a_{m_1+1} - 1 = b_{m_1+1} - 1, \dots, a_m - 1 = b_m - 1$. Zbytek je zřejmý. $\square$

5.15 Tvzení. Ať G je konečně generovaná abelovská grupa. Pak G je možno vyjádřit jako direktní sumu cyklických grup, které jsou buď nekonečné, nebo řádu mocniny prvočísla. Toto vyjádření je až na izomorfismus jednoznačné.

Důkaz. Existence plyne z 5.9, 5.6, 5.10 a 5.13. Seskupíme-li cyklické grupy konečného řádu, dostaneme torzní část T grupy G . Počet nekonečných cyklických grup odpovídá počtu sčítanců ve vyjádření volné grupy G/T . Ten je však jednoznačný podle 5.7.

Seskupíme-li cyklické grupy řádu mocniny prvočísla p , dostaneme p -primární komponentu $G_{(p)}$. Její rozklad na direktní sumu cyklických grup je až na izomorfismus jednoznačný podle 5.14. $\square$

6 Divisibilní grupy

V této kapitole se budeme zabývat pouze abelovskými grupami. Abelovská grupa G se nazývá *divisibilní*, jestliže rovnice $nx = g$ má řešení pro každé $g \in G$ a $n \in \mathbb{Z}$, $n \neq 0$.

Nejsnáze přístupným příkladem divisibilní grupy je aditivní grupa racionálních čísel.

6.1 Lemma.

- (i) Je-li G divisibilní grupa a $H \leq G$, tak je i G/H divisibilní.
- (ii) Direktní suma $\bigoplus_{i \in I} G_i$ je divisibilní, právě když každá z grup G_i je divisibilní.
- (iii) Kartézský součin $\prod_{i \in I} G_i$ je divisibilní, právě když každá z grup G_i je divisibilní. $\square$

Důkaz uvedených skutečností je snadný. Dále dokážeme, že pojem divisibilní grupy odpovídá pojmu injektivní grupy.

Abelovská grupa G se nazývá *injektivní*, jestliže pro libovolný monomorfismus abelovských grup $\alpha: A \rightarrow B$ a libovolný homomorfismus $\gamma: A \rightarrow G$ existuje homomorfismus $\beta: B \rightarrow G$ takový, že $\gamma = \beta \circ \alpha$. (Řečeno neformálně, homomorfismy do G lze přetahovat přes nadgrupy.)

6.2 Lemma. Ať A a B jsou podgrupy abelovské grupy G . Ať $\varphi: A \rightarrow H$ a $\psi: B \rightarrow H$ jsou homomorfismy grup. Předpokládejme, že φ a ψ se shodují na $A \cap B$. Pak $a + b \mapsto \varphi(a) + \psi(b)$ je korektně definovaný homomorfismus $A + B \rightarrow H$.

Důkaz. Je-li $a + b = c + d$, kde $a, c \in A$ a $b, d \in B$, tak z $a - c = d - b$ plyne $\varphi(a) + \psi(b) = \varphi(c) + \varphi(a) - \varphi(c) + \psi(b) = \varphi(c) + \psi(d) - \psi(b) + \psi(b) = \varphi(c) + \psi(d)$, takže definice je vskutku korektní. Dále pro $e \in A$ a $f \in B$ máme $\varphi(a + e) + \psi(b + f) = ((\varphi(a) + \psi(b))) + ((\varphi(e) + \psi(f)))$, a proto jde o homomorfismus. $\square$

6.3 Tvzení. Abelovská grupa G je injektivní, právě když je divisibilní.

Důkaz. Ať G je injektivní, $\alpha: n\mathbb{Z} \rightarrow \mathbb{Z}$ vložení inkluzí a $\gamma(ni) = ig$. Z injektivty plyne, že existuje homomorfismus $\beta: \mathbb{Z} \rightarrow G$ takový, že $\beta \circ \alpha = \gamma$.

Potom je $n \cdot \beta(1) = \beta(n) = g$, takže rovnice $nx = g$ vskutku má řešení.

Ať je naopak G divisibilní, $\alpha: A \rightarrow B$ monomorfismus a $\gamma: A \rightarrow G$ homomorfismus. Budeme uvažovat množinu $\mathcal{M}$ všech homomorfismů $\mu: C \rightarrow G$ takových, že je $\text{Im } \alpha \subseteq C \subseteq B$ a $\mu \circ \alpha = \gamma$. Tato množina je neprázdná, neboť obsahuje $\mu: \text{Im } \alpha \rightarrow G$ takové, že je $\mu(\alpha(a)) = \gamma(a)$ pro každé $a \in A$. Jsou-li $\mu_i: C_i \rightarrow G$ prvky $\mathcal{M}$, $i \in I$, které jsou lineárně uspořádány inkluzí, je $\bigcup_{i \in I} \mu_i: \bigcup_{i \in I} C_i \rightarrow G$ jistě opět prvek $\mathcal{M}$. Proto dle Zornova lemmatu lze nalézt $\mu: C \rightarrow G$, které patří do $\mathcal{M}$ a které nelze již rozšířit. Chceme dokázat, že pak je C rovno B . Proto budeme předpokládat, že C je vlastní podmnožinou B , a ukážeme, že v takovém případě je μ možno rozšířit. Ať je $b \in B \setminus C$ a $D = \langle b, C \rangle = \{mb + c; m \in \mathbb{Z} \text{ a } c \in C\}$. Budeme se snažit $\mu: C \rightarrow G$ rozšířit na $\nu: D \rightarrow G$. Nejprve uvážíme, že $\langle b \rangle \cap C$ je rovno $\langle nb \rangle$ pro nějaké $n \geq 0$, a označíme $\mu(nb)$ jako h . Protože h je prvek divisibilní grupy G , $h = ng$ pro nějaké $g \in G$. Definujme $\psi: \langle b \rangle \rightarrow G$ tak, že $\psi(mb) = mg$ pro každé $m \in \mathbb{Z}$. Protože $\psi(nb) = ng = h = \mu(nb)$, lze podle 6.2 homomorfismus $\nu: D \rightarrow G$ definovat tak, že je $\nu(mb + c) = mg + \mu(c)$ pro každé $m \in \mathbb{Z}$ a každé $c \in C$. $\square$

6.4 Důsledek. Ať G je abelovská grupa a $H \leq G$ je její divisibilní podgrupa. Pak $G = H \oplus C$ pro nějakou podgrupu $C \leq G$.

Důkaz. Ať $j: H \rightarrow G$ označuje vložení H do G . Podle 6.3 existuje $\pi: G \rightarrow H$, že $\pi \circ j = \text{id}_H$. Nyní stačí položit $C = \text{Ker } \pi$, neboť pro každé $g \in G$ je $g - \pi(g) \in C$. $\square$

6.5 Lemma. Ať G je divisibilní grupa. Potom její torzní část T je rovněž divisibilní.

Důkaz. Ať je $h \in T$, $n \in \mathbb{Z}$ a $ng = h$ pro nějaké $g \in G$. Je-li $mh = 0$, je $nmg = 0$, takže g padne do T . $\square$

6.6 Důsledek. Každou divisibilní grupu G je možno vyjádřit jako direktní sumu beztorzní divisibilní grupy a p -primárních komponent $G_{(p)}$. Všechny p -primární komponenty jsou přitom rovněž divisibilní grupy. $\square$

6.7 Lemma. Buď G beztorzní divisibilní grupa. Je-li $h \in G$ a $n \in \mathbb{Z}$, $n \neq 0$, tak existuje jediné $g \in G$ takové, že je $ng = h$. Pro $q \in \mathbb{Q}$, $q = \frac{a}{b}$,

definujme $q \cdot h$ jako (jediné) řešení rovnice $bx = ah$. Pak G je vektorový prostor nad $\mathbb{Q}$.

Důkaz. Je-li $ng_1 = ng_2 = h$, tak $n(g_1 - g_2) = 0$, a protože G je beztorzní, je $g_1 = g_2$. Z $bx = ah$ plyne $(bm)x = (am)h$ pro každé $m > 0$, takže definice $q \cdot h$ nezáleží na způsobu zápisu racionálního čísla ve tvaru zlomku. Zbývá ukázat $q \cdot (h_1 + h_2) = q \cdot h_1 + q \cdot h_2$, $q_1 \cdot (q_2 \cdot h) = (q_1 q_2) \cdot h$ a $(q_1 + q_2) \cdot h = q_1 \cdot h + q_2 \cdot h$.

Z $bx = a(h_1 + h_2)$, $bx_1 = ah_1$ a $bx_2 = ah_2$ jistě plyne $x = x_1 + x_2$. Je-li $b_2 x_2 = a_2 h$ a $b_1 x_1 = a_1 x_2$, je také $b_2 b_1 x = a_1 a_2 h$, a konečně z $b_1 x_1 = a_1 h$ a $b_2 x_2 = a_2 h$ plyne $b_1 b_2 (x_1 + x_2) = (a_1 b_2 + a_2 b_1) h$. $\square$

6.8 Důsledek. Beztorzní abelovská grupa G je divisibilní, právě když je izomorfní sumě libovolného počtu kopií aditivní grupy racionálních čísel. $\square$

Zbývá charakterizovat divisibilní p -grupy, kde $p \geq 2$ je prvočíslo.

6.9 Lemma. Ať G je abelovská p -grupa. Potom G je divisibilní, právě když pro každé $g \in G$ má rovnice $px = g$ alespoň jedno řešení. Iterací dostáváme, že i každá rovnice $p^k x = g$, $k \geq 1$, má řešení.

Důkaz. Hledejme řešení rovnice $nx = g$, kde $n = p^k m$, přičemž m je nesoudělné s p . Ať $p^k h = g$. Protože násobení m je automorfismem cyklické p -grupy $\langle h \rangle$, lze h vyjádřit jako mh' . $\square$

Buď G divisibilní p -grupa a S její dolní vrstva. Pro každé $g \in S$, $g \neq 0$, sestrojíme posloupnost $h_0 = 0$, $h_1 = g$, $h_2, \dots$, tak, že $ph_{j+1} = h_j$. Z divisibility G plyne, že taková posloupnost vždy existuje, byť g ji nemusí určovat jednoznačně. Položíme ještě $C(g) = \bigcup_{j \geq 0} \langle h_j \rangle$. Protože je $\langle h_j \rangle \subseteq \langle h_{j+1} \rangle$, je $C(g)$ podgrupa G (pro libovolné $u, v \in C(g)$ totiž existuje $j \geq 0$, že je $\{u, v\} \subseteq \langle h_j \rangle$).

6.10 Lemma.

- (i) $C(g)$ je divisibilní podgrupa G .
- (ii) Je-li $S = \bigoplus_{i \in I} \langle g_i \rangle$, $g_i \neq 0$, a G je divisibilní, je $G = \bigoplus_{i \in I} C(g_i)$.

Důkaz.

- (i) Ať je $u \in C(g)$ a $j \geq 0$ je nejmenší takové, že u padne do $\langle h_j \rangle$. Pak $u = mh_j$ pro nějaké $m > 0$, takže $u = p(mh_{j+1})$.
- (ii) Ukážeme nejprve, že ze $\sum_{i \in I} u_i = 0$, kde $u_i \in C(g_i)$, plyne $u_i = 0$ pro všechna $i \in I$. Postupujeme sporem a předpokládáme, že $\sum_{i \in I} u_i = 0$, přičemž $\sum_{i \in I} |u_i|$ je nejmenší možné. Pak $\sum_{i \in I} |pu_i| < \sum_{i \in I} |u_i|$, $\sum_{i \in I} pu_i = 0$, a tedy $u_i \in S$ pro všechna $i \in I$. To ovšem znamená $u_i \in \langle g_i \rangle$ a máme spor s předpokladem $S = \bigoplus_{i \in I} \langle g_i \rangle$.

Dokázali jsme, že je $C(g_{i_0}) \cap \langle C(g_i); i \in I \text{ a } i \neq i_0 \rangle = 0$, takže G obsahuje podgrupu $H = \bigoplus_{i \in I} C(g_i)$. Ta je ovšem divisibilní podle 6.1, a tedy $G = H \oplus C$ podle 6.4. Protože $H \supseteq S$, je $C \cap S = 0$, takže $C = 0$ a $G = H$. $\square$

6.11 Lemma. Grupa $C(g)$ je izomorfní p -primární komponentě C grupy $\mathbb{Q}/\mathbb{Z}$. Přitom $C = \{\frac{a}{p^k} + \mathbb{Z}; 0 \leq a < p^k \text{ a } k \geq 1\}$.

Důkaz. Nulový prvek $\mathbb{Q}/\mathbb{Z}$ je roven $\mathbb{Z}$ a každý nenulový prvek $\alpha \in \mathbb{Q}/\mathbb{Z}$ lze jednoznačně zapsat jako $\frac{a}{b} + \mathbb{Z}$, kde $0 < a < b$, a a b jsou nesoudělná. Řád α je roven $\min\{r > 0; r \cdot \frac{a}{b} \in \mathbb{Z}\} = \min\{r > 0; b \text{ dělí } ra\} = b$. Vyjádření p -primární komponenty C ve znění lemmatu je tedy správné.

Ať $\pi: \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z}$ označuje přirozenou projekci. Pak zjevně $C = \pi(D)$, kde $D = \{\frac{a}{p^k}; a \in \mathbb{Z} \text{ a } k \geq 0\}$. Přitom D je podgrupa $\mathbb{Q}(+, -, 0)$.

Grupa $C(g)$ je rovna sjednocení cyklických podgrup $\langle h_j \rangle$, $j \geq 0$, $ph_{j+1} = h_j$. Indukcí okamžitě dostaneme $p^i h_{j+i} = h_j$ pro každé $j \geq 0$, $i \geq 0$.

Definujme $\psi: D \rightarrow C(g)$ tak, že $\psi(\frac{a}{p^k}) = ah_k$. Protože pro $i \geq 0$ je $ah_k = ap^i h_{k+i}$, je definice ψ korektní (tj. $\psi(\frac{a}{p^k}) = ah_k$ i v případě, kdy p dělí a). Pro $\frac{a}{p^k} \in D$ a $\frac{b}{p^j} \in D$ a $m \geq \max\{k, j\}$ máme

$$\begin{aligned} \psi\left(\frac{a}{p^k} + \frac{b}{p^j}\right) &= \psi\left(\frac{ap^{m-k} + bp^{m-j}}{p^m}\right) \\ &= (ap^{m-k} + bp^{m-j})h_m \\ &= ap^{m-k}h_m + bp^{m-j}h_m \\ &= \psi\left(\frac{ap^{m-k}}{p^m}\right) + \psi\left(\frac{bp^{m-j}}{p^m}\right) \end{aligned}$$

$$= \psi\left(\frac{a}{p^k}\right) + \psi\left(\frac{b}{p^j}\right),$$

takže ψ je homomorfismus.

Je zjevně $\text{Im } \psi = C(g)$ a $\text{Ker } \psi = \mathbb{Z}$, takže podle věty o homomorfismu 1.12 je $\psi = \varphi\pi$ pro izomorfismus $\varphi: D/\mathbb{Z} \cong C(g)$. $\square$

Divisibilní p -grupa C z předchozího lemmatu se nazývá *Prüferova grupa* a značívá se $C(p_\infty)$.

6.12 Tvzení. Ať $G = \bigcup_{j \geq 0} H_j$, kde $|H_j| = p^j$, p je prvočíslo, a $H_j \subseteq H_{j+1}$ pro každé $j \geq 0$. Potom je $G \cong C(p_\infty)$ divisibilní grupa.

Důkaz. Je-li h_j generátor H_j , lze jistě nalézt generátor h_{j+1} grupy H_{j+1} , který splňuje $ph_{j+1} = h_j$. Indukcí dle j můžeme sestavit posloupost takových generátorů. Podle 6.9 je G divisibilní, a protože H_1 je její dolní vrstva, plyne tvrzení z 6.11. $\square$

Shrnutím 6.1, 6.6, 6.8, 6.10(ii), 6.11 a 6.12 dostáváme

6.13 Tvzení. Abelovská grupa G je divisibilní, právě když je sumou libovolného počtu kopií aditivní grupy $\mathbb{Q}$ a Prüferových grup $C(p_\infty)$, kde p probíhá všechna prvočísla. $\square$

7 Působení grupy na množině

Buď Ω množina a $S(\Omega)$ příslušná symetrická grupa. *Působením* (či *akcí*) grupy G na Ω rozumíme každý homomorfismus $\varphi: G \rightarrow S(\Omega)$.

Pro označení takového homomorfismu se místo písmena (zde φ) používá také binární symbol (řekněme $*$). Pak se místo $\varphi(g)(\omega)$ píše $g * \omega$. Častý je také funkcionální zápis $g(\omega)$, přičemž v takovém případě je z kontextu zřejmé, o jakou akci jde.

Působení φ se nazývá *věrné*, je-li $\text{Ker } \varphi = 1$. Obecně o $\text{Ker } \varphi$ mluvíme jako o jádru akce.

7.1 Lemma. *Atť G je grupa a Ω množina. Necht' $g * \omega$ je definováno pro každé $g \in G$ a $\omega \in \Omega$. Potom $*$ je působením grupy G na Ω , právě když pro všechna $g, h \in G$ a $\omega \in \Omega$ platí*

- (i) $g * (h * \omega) = (gh) * \omega$,
- (ii) $1 * \omega = \omega$.

Důkaz. Spojením (i) a (ii) dostáváme $g * (g^{-1} * \omega) = \omega = g^{-1} * (g * \omega)$ pro všechna $g \in G$ a $\omega \in \Omega$. Odsud plyne, že zobrazení $\omega \mapsto g * \omega$ je permutací pro libovolné $g \in G$, takže (i) vyjadřuje právě skutečnost, že $*$ je homomorfismem $G \rightarrow S(\Omega)$. $\square$

Nyní se přidržíme nejjednoduššího (tj. funkcionálního) zápisu působení.

7.2 Lemma. *Atť G působí na Ω .*

- (i) *Pro každé $\omega \in \Omega$ je $G_\omega = \{g \in G; g(\omega) = \omega\}$ podgrupa G .*
- (ii) *Pro $\alpha, \beta \in \Omega$ píšme $\alpha \sim \beta$, právě když existuje $g \in G$ takové, že platí $g(\alpha) = \beta$. Relace $\sim$ je ekvivalence na Ω .*

Důkaz.

- (i) Z $g, h \in G_\omega$ plyne $(gh)(\omega) = g(h(\omega)) = g(\omega) = \omega$ a $g^{-1}(\omega) = \omega$ je patrné z $g(g^{-1}(\omega)) = \omega = g(\omega)$.
- (ii) Reflexivita a symetrie jsou zřejmé, uvažme transitivitu. Ať tedy $g(\alpha) = \beta$ a $h(\beta) = \gamma$. Potom ovšem $(hg)(\alpha) = h(g(\alpha)) = h(\beta) = \gamma$. $\square$

Podgrupa G_ω se nazývá *stabilizátor* ω a ekvivalenčním třídám $\sim$ se říká *orbity transitivity* (nebo pouze *orbity*).

7.3 Lemma. *Atť G působí na Ω a $\alpha \in \Omega$. Pro každé $g \in G$ je $gG_\alpha g^{-1} = G_{g(\alpha)}$. Podgrupa $H \leq G$ je konjugovaná s G_α , právě když $H = G_\beta$ pro nějaké $\beta \in \Omega$, které leží ve stejné orbitě transitivity jako α .*

Důkaz. Vskutku $h \in gG_\alpha g^{-1} \Leftrightarrow g^{-1}hg \in G_\alpha \Leftrightarrow g^{-1}hg(\alpha) = \alpha \Leftrightarrow h(g(\alpha)) = g(\alpha)$. Přitom $\alpha, \beta \in \Omega$ leží ve stejné orbitě transitivity, právě když $g(\alpha) = \beta$ pro nějaké $g \in G$. $\square$

Působení G na Ω , které má jedinou orbitu transitivity, se nazývá *transitivní*. Působení se nazývá *semiregulární*, jestliže $G_\alpha = 1$ pro všechna $\alpha \in \Omega$, a *regulární*, jestliže je současně transitivní a semiregulární.

Je-li $\Gamma \subseteq \Omega$ a G působí na Ω , tak $g(\Gamma) = \Gamma$ platí po všechna $g \in G$, právě když je Γ sjednocením (libovolného počtu) orbit transitivity. Je zřejmé, že v takovém případě každé $g \in G$ permutuje množinu Γ , takže z působení G na Ω zúžením dostáváme působení G na Γ .

7.4 Lemma. *Atť G působí na Ω a $\Gamma \subseteq \Omega$ je orbitou transitivity prvku $\alpha \in \Omega$. Atť g je prvek G a atť $g(\alpha) = \beta$. Pak $gG_\alpha = \{h \in G; h(\alpha) = \beta\}$ a $|\Gamma| = |G : G_\alpha|$.*

Důkaz. Pro prvek $h \in G$ platí $gG_\alpha = hG_\alpha \Leftrightarrow h^{-1}g \in G_\alpha \Leftrightarrow h^{-1}g(\alpha) = \alpha \Leftrightarrow g(\alpha) = h(\alpha)$. Každému prvku $\gamma \in \Gamma$ přiřadíme $\{h \in G; h(\alpha) = \gamma\}$. Dokázali jsme, že jde o zobrazení Γ na množinu všech levých rozkladových tříd podle G_α . Protože pro každé $\gamma \in \Gamma$ je $\gamma = h(\alpha)$ pro nějaké $h \in G$, je toto zobrazení surjektivní. Přímou z definice plyne, že je také injektivní, takže vskutku platí $|\Gamma| = |G : G_\alpha|$. $\square$

Buď H podgrupa G a ať Ω je množina všech levých rozkladových tříd podle H . Pro všechna $g, h, k \in G$ platí $g(h(kH)) = (gh)(kH)$ a $1(hH) = hH$. Zobrazení $g: hH \mapsto (gh)H$ tedy podle 7.1 poskytují působení G na Ω . Této akci se říká *působení translací G na levých rozkladových třídách podgrupy H* .

7.5 Lemma. *Uvažme působení translací grupy G na levých rozkladových třídách podgrupy H . Jeho jádrem je největší normální podgrupa N obsažená*

v H . Působení je transitivní a pro každé $g \in G$ je stabilizátor G_{gH} roven gHg^{-1} .

Důkaz. Z $(gh^{-1})(hH) = gH$ plyne, že jde o transitivní působení. Pro prvek $h \in G$ platí $h \in G_{gH} \Leftrightarrow (hg)H = gH \Leftrightarrow hg \in gH \Leftrightarrow h \in gHg^{-1}$. Je tedy $G_{gH} = gHg^{-1}$, a speciálně $G_H = H$. Jádrem působení leží ve stabilizátoru H , a tedy v H . Stačí tedy nahlédnout, že každá normální podgrupa $M \trianglelefteq G$, obsažená v H , leží v jádru. Ovšem $M \leq H$ implikuje $gMg^{-1} = M \leq gHg^{-1} = G_{gH}$, takže prvky z M vskutku působí jako identita. $\square$

Ať nyní Ω označuje množinu $\{kHk^{-1}; k \in G\}$, tj. množinu všech grup konjugovaných s H . Místo kHk^{-1} budeme též psát kH . Pro všechna $g, h, k \in G$ platí $g({}^h(kH)) = ({}^{gh})({}^kH)$ a ${}^1(kH) = {}^kH$. Zobrazení $g: {}^hH \mapsto {}^{gh}H$ tedy podle 7.1 poskytují působení G na Ω . Této akci se říká *působení G konjugací* (na podgrupách konjugovaných s H).

7.6 Lemma. Uvažme působení G konjugací na podgrupách konjugovaných s podgrupou H . Jeho jádrem je největší normální podgrupa N obsažená v normalizátoru $N_G(H)$. Působení je transitivní a pro každé $g \in G$ je stabilizátor $G_{gHg^{-1}}$ roven $N_G(gHg^{-1}) = gN_G(H)g^{-1}$.

Důkaz. Z $({}^{gh^{-1}})hH = {}^gH$ plyne, že jde o transitivní působení. Pro $h \in G$ platí $h \in G_{gHg^{-1}} \Leftrightarrow {}^h(gHg^{-1}) = gHg^{-1} \Leftrightarrow h \in N_G({}^gH)$. Jádrem působení je tedy obsaženo v $G_H = N_G(H)$ a pro každé $M \trianglelefteq G$, $M \leq N_G(H)$, $g \in G$, máme ${}^gM = M \leq {}^g(N_G(H)) = N_G({}^gH)$. (Pro ověření vztahu ${}^g(N_G(H)) = N_G({}^gH)$ je dobré si uvědomit, že $N_G(\varphi(H)) = \varphi(N_G(H))$ platí pro libovolný automorfismus $\varphi \in \text{Aut}(G) \geq \text{Inn}(G)$.) $\square$

Kombinací 7.4 a 7.6 dostáváme

7.7 Důsledek. Podgrupa H grupy G je konjugována s právě $|G : N_G(H)|$ podgrupami. $\square$

7.8 Poznámka. Působení translací je možno obecněji definovat na množině $\mathcal{P}(G)$ všech podmnožin grupy G předpisem $g: A \mapsto gA$. Výchů popsané působení je zúžením této akce na orbitu levých rozkladových tříd podgrupy H .

Podobně působení konjugací lze definovat na $\mathcal{P}(G)$ jako $g: A \mapsto {}^gA$, kde gA rozumíme gAg^{-1} .

7.9 Poznámka. Zde uvedené definice předpokládají skládání zobrazení zprava doleva. Při opačném směru skládání zobrazení bychom uvažovali působení translacemi zprava, a tedy bychom pracovali s působením translací na pravých rozkladových třídách H . Podobně při působení konjugací bychom uvažovali zobrazení $g: A \mapsto A^g$, kde $A^g = g^{-1}Ag$. V literatuře je označení, které vychází ze skládání zleva doprava (tedy z opačného směru, než jaký používáme), daleko rozšířenější.

Je-li $\varphi: X \rightarrow Y$ bijekce, tak je zvykem značit φ_* zobrazení $S(X) \rightarrow S(Y)$, které zobrazí permutaci γ na $\varphi\gamma\varphi^{-1}$.

7.10 Lemma. Ať $\varphi: X \rightarrow Y$ a $\psi: Y \rightarrow Z$ jsou bijekce. Potom jsou zobrazení $\varphi_*: S(X) \rightarrow S(Y)$ a $\psi_*: S(Y) \rightarrow S(Z)$ izomorfismy grup a platí $\varphi_*\psi_* = (\varphi\psi)_*$ a $(\varphi^{-1})_* = (\varphi_*)^{-1}$.

Důkaz. Pro všechna $\gamma \in S(X)$ je $(\varphi^{-1})_*\varphi_*(\gamma) = \varphi^{-1}(\varphi\gamma\varphi^{-1})\varphi = \gamma$ a podobně je $\varphi_*(\varphi^{-1})_*(\gamma') = \gamma'$ pro každé $\gamma' \in S(Y)$. Proto jsou zobrazení $(\varphi^{-1})_*$ a φ_* vzájemně inverzní. Jsou-li γ_1 a γ_2 dvě permutace X , je $\varphi_*(\gamma_1\gamma_2)$ rovno $\varphi\gamma_1\gamma_2\varphi^{-1} = \varphi\gamma_1\varphi^{-1}\varphi\gamma_2\varphi^{-1} = \varphi_*(\gamma_1)\varphi_*(\gamma_2)$. Konečně pro každé $\gamma \in S(X)$ platí $\psi_*\varphi_*(\gamma) = (\psi\varphi)\gamma(\psi\varphi)^{-1} = (\psi\varphi)\gamma(\psi\varphi)^{-1} = (\psi\varphi)_*\gamma$. $\square$

Dvě působení $\varphi: G \rightarrow S(\Omega)$ a $\psi: G \rightarrow S(\Gamma)$ nazveme *ekvivalentní*, právě když existuje bijekce $\alpha: \Omega \rightarrow \Gamma$ taková, že platí $\psi = \alpha_*\varphi$. (Všimněte si, že $\psi = \alpha_*\varphi$ platí právě tehdy, když je rovnost $\psi(g)\alpha = \alpha\varphi(g)$ splněna pro každé $g \in G$.)

7.11 Tvzení. Ať ψ je transitivní působení G na množině Γ , $\gamma \in \Gamma$ a $H = \{g \in G; \psi(g)(\gamma) = \gamma\}$. Uvažme působení G translacemi na množině Ω všech levých rozkladových tříd H a označme toto působení φ . Definujme zobrazení $\alpha: \Omega \rightarrow \Gamma$ tak, že $\alpha(gH) = \psi(g)(\gamma)$. Pak α je korektně definováno, je to bijekce a platí $\psi = \alpha_*\varphi$.

Důkaz. Ať $gH = kH$, kde $g, k \in G$. Potom $g^{-1}k \in H$, takže $\psi(g^{-1}k)(\gamma) = \gamma$, a tedy $\psi(g)(\gamma) = \psi(g)\psi(g^{-1}k)(\gamma) = \psi(k)(\gamma)$. Zobrazení α je tedy korektně

ně definováno. Z $\alpha(gH) = \alpha(hH)$ plyne $\psi(h^{-1}g)(\gamma) = \gamma$, tedy $h^{-1}g \in H$ a $gH = hH$. Vidíme, že α je injektivní zobrazení. Protože ψ je transitivní akce, lze pro každé $\eta \in \Gamma$ nalézt $g \in G$, že je $\psi(g)(\gamma) = \eta$, takže $\eta = \alpha(gH)$. Dokázali jsme, že $\alpha: \Omega \rightarrow \Gamma$ je bijekce. Zbývá ověřit $\psi(g)\alpha = \alpha\varphi(g)$. Pro každé $h \in H$ ovšem platí $\psi(g)\alpha(hH) = \psi(gh)(\gamma) = \alpha(ghH) = \alpha\varphi(g)(hH)$. $\square$

Z tvrzení 7.11 tedy plyne, že každé transitivní působení G je ekvivalentní působení translací na levých rozkladových třídách vhodné podgrupy H . Podle 7.5 je toto působení regulární, právě když H je triviální podgrupa, tj. $H = 1$. Je-li $H = 1$, tak rozkladové třídy podle H jsou právě jednobodové množiny $\{g\}$. Ztotožníme-li $\{g\}$ a g , vidíme, že v tomto případě jde o působení levými translacemi

$$L_a: G \rightarrow G, \quad g \mapsto ag.$$

Každé regulární působení G je tedy ekvivalentní působení levými translacemi.

8 Sylowovy věty

Ať G je konečná grupa řádu n a $p \geq 2$ je prvočíslo. V množině $\mathcal{M}_p(G)$ podgrup $H \leq G$ takových, že $|H|$ je mocnina p , uvažme maximální podgrupy. Těmto podgrupám se říká *Sylowovy p -podgrupy* a jejich množina se značí $\text{Syl}_p(G)$. Je tedy $\text{Syl}_p(G) = \{P \in \mathcal{M}_p(G); \text{pro všechna } H \in \mathcal{M}_p(G) \text{ z } H \supseteq P \text{ plyne } H = P\}$.

Jestliže p nedělí n , tak $\text{Syl}_p(G)$ je podle Lagrangeovy věty množina, která obsahuje pouze triviální grupu. Předpokládejme, že p dělí n . K tomu, abychom věděli, že Sylowovy p -podgrupy jsou netriviální, stačí ukázat, že G obsahuje alespoň jeden prvek řádu p .

8.1 Lemma. *Buďte p prvočíslo, G konečná grupa a ať p dělí $|G|$. Pak G obsahuje alespoň jeden prvek řádu p .*

Důkaz. Postupujeme indukcí podle $|G|$. Předpokládejme, že je $g \in G \setminus Z(G)$. Potom $C_G(g)$ je vlastní podgrupa G , a v případě, že p dělí $|C_G(g)|$, můžeme použít indukční předpoklad. Ať pro všechna $g \in G \setminus Z(G)$ prvočíslo p nedělí $|C_G(g)|$. Pak podle Lagrangeovy věty p dělí $|G : C_G(g)|$, a z 3.11 dostáváme, že p musí dělit i $|Z(G)|$. Nyní již stačí použít klasifikaci konečných abelovských grup (?). $\square$

Protože předpokládáme, že p dělí $n = |G|$, je množina $\text{Syl}_p(G)$ neprázdná. Vyberme $P, Q \in \text{Syl}_p(G)$, přičemž může být i $P = Q$. Je-li $\varphi \in \text{Aut}(G)$, tak je jistě $\varphi(P) \in \text{Syl}_p(G)$. Proto platí i $\mathcal{P} \subseteq \text{Syl}_p(G)$, kde $\mathcal{P} = \{gPg^{-1}; g \in G\}$. Uvažme, jak Q působí na $\mathcal{P}$ konjugací. Z lematu 7.4 plyne, že velikost každé orbity akce Q na $\mathcal{P}$ je rovna mocnině prvočísla p , přičemž orbita je jednobodová (a tedy rovna $\{gPg^{-1}\}$ pro nějaké $g \in G$), právě když pro všechna $h \in Q$ je $hgPg^{-1}h^{-1} = gPg^{-1}$. To ale znamená $Q \leq N_G(gPg^{-1})$, a protože $R = gPg^{-1}$ je normální v $N_G(R)$, je QR podgrupa podle 1.20, přičemž její řád je roven $|QR : Q| \cdot |Q| = |R : Q \cap R| \cdot |Q|$ podle Třetí věty o izomorfismu 1.23. Tudíž QR je opět řádu mocniny prvočísla p a z maximality Q a R vyplývá $Q = QR = R$. Formulujeme učiněné pozorování jako lemma.

8.2 Lemma. *Ať prvočíslo p dělí řád konečné grupy G , $P \in \text{Syl}_p(G)$ a $\mathcal{P} = \{gPg^{-1}; g \in G\}$. Buď také $Q \in \text{Syl}_p(G)$ a uvažme působení Q na $\mathcal{P}$ konjugací. Toto působení poskytuje nanejvýš jednu jednobodovou orbitu, a to právě tehdy, když platí $Q \in \mathcal{P}$. Velikost ostatních orbit je rovna některé kladné mocnině prvočísla p .* $\square$

Podle 8.2 je tedy $|\mathcal{P}| \equiv 1 \pmod{p}$, jestliže je $Q \in \mathcal{P}$, a $|\mathcal{P}| \equiv 0 \pmod{p}$, jestliže je $Q \notin \mathcal{P}$. Ovšem definice $\mathcal{P}$ nezávisí na volbě Q . Za Q lze vždy zvolit P , a protože P patří do $\mathcal{P}$, musí vždy nastat prvá možnost, tj. $|\mathcal{P}| \equiv 1 \pmod{p}$. Jelikož nemůže současně platit $|\mathcal{P}| \equiv 1 \pmod{p}$ a $|\mathcal{P}| \equiv 0 \pmod{p}$, vidíme, že je $\text{Syl}_p(G) \subseteq \mathcal{P}$, a tedy $\text{Syl}_p(G) = \mathcal{P}$. Dokázali jsme:

8.3 Tvrzení. *Ať prvočíslo p dělí řád konečné grupy G . Potom všechny Sylowovy p -podgrupy grupy G jsou konjugovány a jejich počet je roven $kp + 1$ pro nějaké $k \geq 0$.* $\square$

Z tvrzení 8.3 plyne, že všechny Sylowovy p -podgrupy G mají stejný řád

p^s , kde p^s dělí $n = |G|$.

8.4 Tvzení. *At G je konečná grupa řádu $n = p^r m$, kde p je prvočíslo, p nedělí m a $r \geq 1$. Potom každá Sylowova p -podgrupa grupy G má řád p^r .*

Důkaz. Podle 8.3 a 7.7 je $|Syl_p(G)| = |G : N_G(P)| \equiv 1 \pmod p$, kde $P \in Syl_p(G)$. Z Lagrangeovy věty máme $|G| = |G : N_G(P)| \cdot |N_G(P) : P| \cdot |P|$, takže stačí ukázat, že p nedělí $|N_G(P) : P|$. Předpokládejme opak a ať $\pi : N_G(P) \rightarrow N_G(P)/P$ je přirozený homomorfismus. Z 8.1 plyne, že $N_G(P)/P$ obsahuje prvek a řádu p . Pak ovšem $\pi^{-1}(\langle a \rangle)$ je podgrupa $N_G(P)$ řádu $p \cdot |P|$, což je spor s volbou $P \in Syl_p(G)$. $\square$

Z lemmatu 8.1 a Lagrangeovy věty také plyne, že konečná grupa G obsahuje prvek prvočíselného řádu p , právě když p dělí $|G|$. To mimo jiné znamená, že konečná grupa je p -grupou, právě když je řádu mocniny p .

Buď H nějaká netriviální p -podgrupa konečné grupy G . Potom existuje podgrupa $P \in Syl_p(G)$, že platí $H \leq P$. Přitom P je nilpotentní (3.13), a tedy řešitelná. Předpokládejme, že je $H \neq P$. V příští kapitole (tvrzení 9.8) ukážeme, že v každé nilpotentní grupě K z $M < K$ plyne $M < N_K(M)$. Proto je i $H < N_P(H)$, takže H je subnormální podgrupa P a leží v nějaké kompoziční řadě grupy P . Protože faktory kompoziční řady konečné řešitelné grupy jsou cyklické a prvočíselného řádu, vidíme, že pro vhodnou podgrupu $U \leq P$ platí $H \triangleleft U$ a $|U : H| = p$.

8.5 Tvzení. *Buď G konečná grupa řádu n a p buď prvočíslo. At H je podgrupa grupy G řádu p^k , $k \geq 0$, a ať p^{k+1} dělí n . Potom existuje grupa $K \leq G$ řádu p^{k+1} taková, že je $H \trianglelefteq K$.* $\square$

Tvrzení 8.3, 8.4 a 8.5 se nazývají *Sylowovy věty*.

9 Nilpotentní grupy

Tuto kapitolu zahájíme několika pozorováními, která se týkají množinových operátorů a stojí vně teorie grup.

Ať $\mathcal{S}$ je nějaký systém podmnožin množiny Σ a ať $\alpha : \mathcal{S} \rightarrow \mathcal{S}$ a $\beta : \mathcal{S} \rightarrow \mathcal{S}$ jsou zobrazení. Budeme vždy předpokládat, že platí

(0) $\Sigma \in \mathcal{S}$ a $\mathcal{S}$ obsahuje nejmenší prvek I .

Pro každé $S \in \mathcal{S}$ tedy platí $S \supseteq I$ a současně je $\{I, \Sigma\} \subseteq \mathcal{S}$. Uvedené podmínky jsou splněny, například je-li $\mathcal{S}$ uzávěrový systém nad Σ .

Uvážíme ještě tyto podmínky:

- (1) jsou-li $S_1, S_2 \in \mathcal{S}$ a $S_1 \subseteq S_2$, tak je $\alpha(S_1) \subseteq \alpha(S_2)$ a $\beta(S_1) \subseteq \beta(S_2)$;
- (2) $\alpha\beta(S) \supseteq S$ a $\beta\alpha(S) \subseteq S$ pro každé $S \in \mathcal{S}$.

9.1 Lemma. *At platí (0) a (1).*

- (i) Jsou-li $I = A_0, A_1, A_2, \dots, A_m$ takové množiny z $\mathcal{S}$, že je $A_{i+1} \subseteq \alpha(A_i)$ pro všechna i , $0 \leq i < m$, tak je $A_m \subseteq \alpha^m(I)$.
- (ii) Jsou-li $\Sigma = B_0, B_1, B_2, \dots, B_n$ takové množiny z $\mathcal{S}$, že je $B_{i+1} \supseteq \beta(B_i)$ pro všechna i , $0 \leq i < n$, tak je $B_n \supseteq \beta^n(\Sigma)$.

Důkaz. Indukcí podle i dokážeme $A_i \subseteq \alpha^i(I)$. Případ $i = 0$ je zřejmý, ať tedy $A_i \subseteq \alpha^i(I)$ platí a je $0 \leq i < m$. Pak dle (i) máme $A_{i+1} \subseteq \alpha(A_i) \subseteq \alpha^{i+1}(I)$. Druhá část se dokáže podobně. $\square$

9.2 Lemma. *At platí (0), (1) a (2). Jestliže $\alpha^n(I) = \Sigma$ pro nějaké $n \geq 0$, tak $\beta^m(\Sigma) = I$ pro nějaké $m \geq 0$, a naopak. Jsou-li n a m nejmenší možná čísla uvedených vlastností, tak platí $n = m$ a pro každé i , $0 \leq i \leq n$, je $\alpha^i(I) \supseteq \beta^{n-i}(\Sigma)$.*

Důkaz. Předpokládejme $\alpha^n(I) = \Sigma$ a ať n je nejmenší možné. Položme $B_i = \alpha^{n-i}(I)$, $0 \leq i \leq n$. Pak $B_0 = \Sigma$, $B_n = I$ a $\alpha(B_{i+1}) = B_i$, je-li $0 \leq i < n$. Podle (2) je $B_{i+1} \supseteq \beta\alpha(B_{i+1}) = \beta(B_i)$, takže $B_i = \alpha^{n-i}(I) \supseteq \beta^i(\Sigma)$ platí podle 9.1 (ii), a je tedy $\beta^n(\Sigma) = I$ a $n \geq m$.

Podobně z $\beta^m(\Sigma) = I$, kde m je nejmenší možné, dostáváme pro $A_i = \beta^{m-i}(\Sigma)$, že je $A_0 = I$, $A_m = \Sigma$ a $\beta(A_{i+1}) = A_i$, $0 \leq i < m$. Podle (2) je $A_{i+1} \subseteq \alpha\beta(A_{i+1}) = \alpha(A_i)$, takže 9.1 (i) implikuje $A_i = \beta^{m-i}(\Sigma) \subseteq \alpha^i(I)$, a máme $\alpha^m(I) = \Sigma$, $m \geq n$. $\square$

Buď nyní G grupa. Předchozí poznatky budeme interpretovat v situaci, kdy je $\Sigma = G$ a $\mathcal{S}$ označuje svaz všech normálních podgrup grupy G .

Je-li $H \trianglelefteq G$, tak $\alpha(H)$ ať (na chvíli) označuje $\pi^{-1}(Z(G/H))$, kde $\pi: G \rightarrow G/H$ je přirozený homomorfismus. Podobně ať $\beta(H)$ označuje grupu $[G, H]$.

Z $H \trianglelefteq G$ plyne $\alpha(H) \trianglelefteq G$ podle 3.3 a 1.18. To, že platí $\beta(H) \trianglelefteq G$, dostáváme z následujícího lemmatu.

9.3 Lemma. Ať G je Ω -grupa a H i K jsou Ω -normální podgrupy G . Potom je $[H, K]$ rovněž Ω -normální podgrupa G a platí $[H, K] \subseteq H \cap K$.

Důkaz. Buďte $\omega \in \Omega \cup \text{Inn}(G)$, $h \in H$ a $k \in K$. Potom $\omega([h, k]) = [\omega(h), \omega(k)]$, přičemž $\omega(h) \in H$ a $\omega(k) \in K$. Odsud plyne, že $[H, K]$ je Ω -normální. Uvažme nyní prvky $h \in H$ a $k \in K$. Pak $[h, k] = (h^{-1}k^{-1}h) \cdot k \in K$ a současně $[h, k] = h^{-1} \cdot (k^{-1}hk) \in H$. $\square$

9.4 Lemma. Pro $H \leq G$ platí $H \trianglelefteq G$, právě když je $[H, G] \leq H$.

Důkaz. Ať je $h \in H$ a $g \in G$. Potom ghg^{-1} padne do H , právě když $ghg^{-1}h^{-1}$ padne do H . $\square$

9.5 Lemma. Ať $H \leq K \leq G$ jsou grupy. Potom $[K, G] \leq H$ platí, právě když je $H \trianglelefteq G$ a $K/H \leq Z(G/H)$.

Důkaz. Z $[K, G] \leq H$ plyne $[H, G] \leq H$, takže podle 9.4 můžeme předpokládat $H \trianglelefteq G$. Pak $[K, G] \leq H \iff$ pro všechna $k \in K$, $g \in G$ je $k^{-1}g^{-1}kgH = H$, tedy $kgH = gkH \iff kH \in Z(G/H)$ pro všechna $k \in K \iff K/H \leq Z(G/H)$. $\square$

Ať je $H \trianglelefteq G$, $K \trianglelefteq G$ a $H \leq K$. Pak je jistě i $\alpha(H) \leq \alpha(K)$ a $\beta(H) \leq \beta(K)$. Je-li $K = \alpha(H)$, tak podle 9.5 je $[K, G] = \beta\alpha(H) \leq H$. Je-li $H = \beta(K)$, tak opět podle 9.5 máme $K/H \leq Z(G/H)$, takže $\alpha\beta(K) \geq K$. Podmínky (0), (1) a (2) jsou pro operátory α a β tedy splněny.

Posloupnost podgrup $H_0 \leq H_1 \leq \dots \leq H_r$ grupy G takových, že je $[H_i, G] \leq H_{i-1}$ pro všechna i , $1 \leq i \leq r$, se nazývá *centrální řada*. Podle 9.4 je $H_j \trianglelefteq G$, $0 \leq j \leq r$.

Pro $i \geq 1$ definujeme $\gamma_i(G)$ tak, že $\gamma_1(G) = G$ a $\gamma_{i+1}(G) = [\gamma_i(G), G]$.

Z 9.3 plyne, že $\gamma_i(G)$ je úplně charakteristická podgrupa grupy G . Posloupnosti $\gamma_1(G) \geq \gamma_2(G) \geq \gamma_3(G) \geq \dots$ se říká *dolní centrální řada*.

Aplikací 9.2 a 9.1 na centrální řady dostáváme:

9.6 Tvzení. Buď G grupa a $s \geq 0$. Následující podmínky jsou ekvivalentní:

- (i) G je nilpotentní grupa stupně s ;
- (ii) $\vartheta_s(G) = G$, přičemž s je nejmenší této vlastnosti;
- (iii) $\gamma_{s+1}(G) = 1$, přičemž s je nejmenší této vlastnosti. $\square$

9.7 Tvzení. Grupa G je nilpotentní, právě když existuje alespoň jedna centrální řada $1 = H_0 \leq H_1 \leq \dots \leq H_r = G$. Přitom je $r \geq s$, kde s je stupeň nilpotence G . Pro každé i , $0 \leq i \leq r$, platí $H_i \leq \vartheta_i(G)$ a $\gamma_{i+1}(G) \leq H_{r-i}$. $\square$

Nyní přistoupíme k charakterizaci konečných nilpotentních grup. Začneme obecnějším tvrzením.

9.8 Tvzení. Je-li H vlastní podgrupa nilpotentní grupy G , je H i vlastní podgrupou svého normalizátoru $N_G(H)$.

Důkaz. Zvolme $i \geq 0$ největší takové, že je $\vartheta_i(G) \leq H$. Potom je $\vartheta_{i+1}(G) \setminus H$ neprázdná množina a $\vartheta_{i+1}(G)/\vartheta_i(G) = Z(G/\vartheta_i(G)) \leq N_{G/\vartheta_i(G)}(H/\vartheta_i(G))$ implikuje $\vartheta_{i+1}(G) \leq N_G(H)$. $\square$

9.9 Důsledek. Každá maximální podgrupa nilpotentní grupy je normální. $\square$

Abychom ukázali, že tvrzení 9.8 a důsledek 9.9 je možné u konečných grup obrátit, poukážeme nejprve na širokou třídu podgrup, které jsou rovny svému normalizátoru.

9.10 Tvzení. Buďte G konečná grupa, p prvočíslo a P Sylowova p -podgrupa G . Je-li $G \geq H \geq N_G(P)$, je $H = N_G(H)$.

Důkaz. Uvažme libovolné $a \in N_G(H)$. Pak z $P \leq H$ plyne $aPa^{-1} \leq H$, takže je $\{P, aPa^{-1}\} \subseteq \text{Syl}_p(H)$. To znamená, že $aPa^{-1} = hPh^{-1}$ pro nějaké

$h \in H$ a $a^{-1}h \in N_G(P)$. Z $N_G(P) \leq H$ máme $a^{-1}h \in H$, a tedy i $a \in H$. $\square$

9.11 Lemma. Buďte G_j , $j \in J$, grupy a ať $G = \coprod_{j \in J} G_j$.

- (i) Pro každé $i \geq 0$ platí $\vartheta_i(G) = \coprod_{j \in J} \vartheta_i(G_j)$.
- (ii) Pro každé $i \geq 1$ platí $\gamma_i(G) = \coprod_{j \in J} \gamma_i(G_j)$.

Důkaz. Důkaz provedeme indukcí, přičemž první krok je v obou případech triviální.

- (i) Pro $a \in G$ platí $a \in \vartheta_{i+1}(G)$, právě když je $[a, g] \in \vartheta_i(G)$ pro každé $g \in G$, což podle indukčního předpokladu znamená $[a(j), g(j)] \in \vartheta_i(G_j)$ pro každé $j \in J$, čili $a(j) \in \vartheta_{i+1}(G_j)$ pro každé $j \in J$.
- (ii) Grupa $\gamma_{i+1}(G)$ je generována množinou $\{[g, a]; g \in G, a \in \gamma_i(G)\}$, kterážto množina v každé ze složek $j \in J$ generuje podle indukčního předpokladu grupu $\gamma_{i+1}(G_j)$, takže vskutku platí $\gamma_{i+1}(G) = \coprod_{j \in J} \gamma_{i+1}(G_j)$. $\square$

9.12 Tvzení. Buď G konečná grupa. Následující podmínky jsou ekvivalentní.

- (i) G je nilpotentní;
- (ii) každá vlastní podgrupa G je vlastní ve svém normalizátoru;
- (iii) všechny maximální podgrupy G jsou normální;
- (iv) všechny Sylowovy podgrupy G jsou normální;
- (v) G je součin svých Sylowových podgrup.

Důkaz. Implikace (i) $\Rightarrow$ (ii) plyne z 9.8; (ii) $\Rightarrow$ (iii) je zřejmé; (iii) $\Rightarrow$ (iv) plyne z 9.10, neboť podgrupa obsahující $N_G(P)$, $P \in \text{Syl}_p(G)$, by nebyla normální; dále (v) $\Rightarrow$ (i) dostáváme z 3.13 a 9.11. Zbývá dokázat (iv) $\Rightarrow$ (v).

Ať $p_1, \dots, p_k$ jsou všechny prvočíselné dělitele $|G|$ a ať $P_1, \dots, P_k$ jsou odpovídající Sylowovy podgrupy. Z $P_i \trianglelefteq G$ plyne, že P_i je jedinou Sylowovou p_i -podgrupou, takže P_i se skládá právě ze všech prvků řádu mocniny prvočísla p_i . Prvek řádu $p_1^{r_1} \dots p_k^{r_k}$ je součinem prvků řádu $p_1^{r_1}, \dots, p_k^{r_k}$ (viz. (?)), takže platí $G = \langle P_i; 1 \leq i \leq k \rangle$. Podle 9.3 platí $[P_i, P_j] \leq P_i \cap P_j = 1$, kdykoliv je $1 \leq i < j \leq k$, takže prvky z P_i a prvky z P_j spolu

komutují. Odsud plyne, že řád grupy $\langle P_j; 1 \leq j \leq k \text{ a } i \neq j \rangle$ není dělitelný p_i , tudíž je $P_i \cap \langle P_j; 1 \leq j \leq k \text{ a } i \neq j \rangle = 1$. Nyní již lze použít 4.3. $\square$

10 Volné grupy a jejich podgrupy

Množina X se nazývá *volná báze* grupy G , jestliže X generuje G a každé zobrazení $f: X \rightarrow H$, kde H je grupa, lze rozšířit na homomorfismus $g: G \rightarrow H$. (Z 1.26 okamžitě plyne, že f určuje g jednoznačně.) Grupa G se nazývá *volná*, jestliže má (alespoň jednu) volnou bázi.

10.1 Lemma. Ať G je volná grupa s bází X a H je volná grupa s bází Y . Mají-li X a Y stejnou mohutnost, je $G \cong H$.

Důkaz. Bijekce $f: X \rightarrow Y$ a $f^{-1}: Y \rightarrow X$ lze rozšířit na homomorfismy $g: G \rightarrow H$ a $h: H \rightarrow G$. Potom zúžení hg na X a gh na Y jsou identity, takže musí být i $hg = \text{id}_G$ a $gh = \text{id}_H$. $\square$

Buď nyní X nějaká neprázdná množina a předpokládejme, že $X^{-1} = \{x^{-1}; x \in X\}$ má s X prázdný průnik. Přitom $(x^{-1})^{-1}$ ztotožňujeme s x , a to pro každé $x \in X$. Ať W je volný monoid slov nad $X^{\pm 1} = X \cup X^{-1}$, tj. $W = \{x_1 \dots x_n; x_i \in X^{\pm 1}, n \geq 0\}$. Na W pohlížíme jako na množinu s binární operací skládání slov (kde $x_1 \dots x_n \cdot y_1 \dots y_m = x_1 \dots x_n y_1 \dots y_m$) a s nulární operací prázdného slova λ .

Jestliže pro $u, v \in W$ lze nalézt slova $u_1, u_2 \in W$ a $x \in X^{\pm 1}$, že je $u = u_1 x x^{-1} u_2$ a $v = u_1 u_2$, budeme psát $(u, v) \in \varrho$. Nejmenší ekvivalenci na W , která obsahuje relaci ϱ , označme $\sim$. Přitom $u \sim v$ zřejmě platí právě tehdy, lze-li najít posloupnost $u = u_0, \dots, u_k = v$ takovou, že je $k \geq 0$ a pro každé i , $1 \leq i \leq k$, je buď $(u_{i-1}, u_i) \in \varrho$ nebo $(u_i, u_{i-1}) \in \varrho$.

Z $u \sim v$ zjevně plyne $wu \sim wv$ a $uw \sim vw$ pro libovolné $w \in W$. Je-li $u_1 \sim v_1$ a $u_2 \sim v_2$, tak máme $u_1 u_2 \sim v_1 u_2 \sim v_1 v_2$. Označme $[u]$ třídu ekvivalence $\sim$ obsahující u . Právě jsme ukázali, že na $W/\sim$ lze vztahem $[u] \cdot [v] = [uv]$ korektně definovat binární operaci. Tato operace je asociativní a $[\lambda]$ je jejím jednotkovým prvkem. Pro $u = x_1 \dots x_n \in W$ položíme $\bar{u} =$

$x_n^{-1} \dots x_1^{-1}$. (Často se místo $\bar{u}$ píše rovnou u^{-1} .) Zjevně z $(u, v) \in \varrho$ plyne $(\bar{u}, \bar{v}) \in \varrho$, takže definice $[u]^{-1} = [\bar{u}]$ je korektní. Protože je $u\bar{u} \sim \bar{u}u \sim \lambda$, vidíme, že jsme na $W/\sim$ definovali grupovou strukturu. O této grupě záhy ukážeme, že je volná.

Slovo $u \in W$ nazveme *redukované*, jestliže nelze nalézt $v \in W$ tak, aby platilo $(u, v) \in \varrho$.

10.2 Lemma. *Každá třída ekvivalence $\sim$ obsahuje právě jedno redukované slovo.*

Důkaz. Není-li slovo redukované, lze z něj postupně vypouštět dvojice xx^{-1} , $x \in X^{\pm 1}$, a to až do chvíle, kdy v něm žádnou takovou dvojici nelze nalézt. Každá třída $\sim$ tedy obsahuje alespoň jedno redukované slovo. Je však třeba ukázat, že pro každá dvě redukováná slova $u, v \in W$ z $u \sim v$ plyne $u = v$.

Postupujeme sporem. Pro každé $u = x_1 \dots x_n \in W$ označme $l(u)$ jeho délku, tedy $l(u) = n$. Ať $u, v \in W$ poskytují nejmenší protipříklad ve smyslu, že je $u \neq v$, $u \sim v$, u a v jsou redukováná, přičemž lze sestavit posloupnost $u = u_0, \dots, u_k = v$, ve které je $(u_{i-1}, u_i) \in \varrho$ nebo $(u_i, u_{i-1}) \in \varrho$ pro každé i , $1 \leq i \leq k$, a součet $l(u_0) + \dots + l(u_k)$ je nejmenší možný. Spor obdržíme nalezením posloupnosti $u = u'_0, \dots, u'_{k'} = v$, ve které bude $(u'_{j-1}, u'_j) \in \varrho$ nebo $(u'_j, u'_{j-1}) \in \varrho$ pro každé j , $1 \leq j \leq k'$, a $\sum_{j=0}^{k'} l(u'_j) < \sum_{i=0}^k l(u_i)$.

Protože u_0 a u_k jsou redukováná, musí být $(u_1, u_0) \in \varrho$ a $(u_{k-1}, u_k) \in \varrho$. Je tedy $l(u_1) > l(u_0)$ a $l(u_k) < l(u_{k-1})$. Ať $l(u_i)$ nabývá pro $i = r$ největší možné hodnoty. Pak je $1 \leq r < k$ a platí $(u_r, u_{r-1}) \in \varrho$ a $(u_r, u_{r+1}) \in \varrho$. Můžeme tedy u_{r-1} zapsat jako ab , u_{r+1} jako cd , přičemž existují $x, y \in X^{\pm 1}$, že $u_r = axx^{-1}b = cyy^{-1}d$.

Protože místo posloupnosti $u_0, \dots, u_k$ bychom mohli vyšetřovat posloupnost $u_k, \dots, u_0$, lze předpokládat $l(a) \leq l(c)$. Je-li $l(a) = l(c)$, je $a = c$, $b = d$, $x = y$, $u_{r-1} = u_{r+1}$ a podposloupnost u_{r-1}, u_r, u_{r+1} lze nahradit jednočlennou posloupností u_{r-1} . Lze tedy předpokládat $l(a) < l(c)$.

Ať je $l(c) = l(a) + 1$. Pak $c = ax$, $y = x^{-1}$ a $b = y^{-1}d$, takže $u_r = axx^{-1}xd$ a $u_{r-1} = axd = u_{r+1}$.

Zbývá případ $l(c) \geq l(a) + 2$. Potom b lze zapsat jako $b'b''$ tak, že $c = axx^{-1}b'$, a tudíž $u_r = axx^{-1}b'yy^{-1}d$, $u_{r-1} = ab'yy^{-1}d$ a $u_{r+1} = axx^{-1}b'd$. Položíme-li $u'_r = ab'd$, je $(u_{r-1}, u'_r) \in \varrho$, $(u_{r+1}, u'_r) \in \varrho$, takže podposloupnost u_{r-1}, u_r, u_{r+1} lze nahradit posloupností u_{r-1}, u'_r, u_{r+1} . $\square$

10.3 Tvzení. *Grupa $W/\sim$ je volná a $\{[x]; x \in X\}$ je její volná báze.*

Důkaz. Ať H je grupa a $f: X \rightarrow H$ je zobrazení. Definujme zobrazení $g: W/\sim \rightarrow H$ tak, že pro $u = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \in W$, kde $\varepsilon_i \in \{-1, 1\}$ a $x_i \in X$, položíme $g([u]) = (f(x_1))^{\varepsilon_1} \dots (f(x_n))^{\varepsilon_n}$. Je-li $(u, v) \in \varrho$ nebo $(v, u) \in \varrho$, je hodnota $g([v])$ určena stejně, a proto je definice g korektní. Z $g([uv]) = g([u])g([v])$ plyne, že jde o homomorfismus. $\square$

Protože v každé třídě ekvivalence $\sim$ leží právě jedno redukované slovo, můžeme volnou grupu s bází X sestavit také jako množinu F všech redukováných slov nad X , kde pro $u, v \in F$ je $u \cdot v$ rovno $u'v'$ tak, že $u = u'w$, $v = w^{-1}v'$ a $u'v'$ je redukované slovo. Slovo w je zjevně určeno jednoznačně a odpovídá maximálnímu koncovému úseku u , který se v inverzní podobě zrcadlí na počátku slova v .

10.4 Tvzení. *Buď G volná grupa a ať X je její volná báze. Uvažme přirozený homomorfismus $\pi: G \rightarrow G/G'$. Pak $\pi(X)$ je volná báze abelovské grupy G/G' , přičemž $\pi(X)$ a X mají stejnou mohutnost.*

Důkaz. Uvažme volnou abelovskou grupu H s bází Y , přičemž $\alpha: X \rightarrow Y$ je bijekce a $\beta: G \rightarrow H$ příslušné rozšíření. Podle 3.14 je $\text{Ker } \beta \geq G'$, takže pro všechna $x_1, x_2 \in X$ z $x_1G' = x_2G'$ plyne $x_1 \text{Ker } \beta = x_2 \text{Ker } \beta$, a tedy i $\beta(x_1) = \beta(x_2)$ a $x_1 = x_2$. Zobrazení π je proto na X injektivní. Ať A je abelovská grupa a $f: \pi(X) \rightarrow A$ nějaké zobrazení. Zobrazení $f' = f \circ \pi: X \rightarrow A$ je možno rozšířit na $g': G \rightarrow A$, přičemž $\text{Ker } g' \geq G'$ dle 3.14. Podle Věty o homomorfismu 1.12 lze tedy g' vyjádřit jako $g \circ \pi$, kde $g: G/G' \rightarrow A$, přičemž pro $x \in X$ je $g(\pi(x)) = g'(x) = f'(x) = f(\pi(x))$. $\square$

10.5 Důsledek. *Ať F_i je volná grupa s bází X_i , $i = 1, 2$. Pak $F_1 \cong F_2$, právě když X_1 a X_2 mají stejnou mohutnost.*

Důkaz. Implikace zprava doleva je obsahem lemmatu 10.1. Obrácenou implikaci převádí předchozí tvrzení 10.4 na již známé tvrzení 5.7 pro volné abelovské grupy. $\square$

Chceme-li ověřit některou z vlastností volné grupy, bývá výhodné pracovat s grupou redukováných slov nad nějakou množinou X . Tuto grupu budeme značit $F(X)$.

V grupě $F(X)$ zápis $u_1 \dots u_k$ znamená výsledek (opakované) grupové operace. Redukované slovo $u = u_1 \dots u_k$ se, jak víme, nemusí rovnat slovu v , které vznikne pouhou konkatenací slov $u_1, \dots, u_k$. (Přitom $u = v$ nastane, právě když v je redukované.) Pokud však řekneme, že $u_1 \dots u_k$ je redukované slovo, tak tím budeme mínit, že konkatenace slov $u_1, \dots, u_k$ je redukované slovo (tedy, že nastává případ $u = v$).

Uvědomte si, že uvedená konvence je poměrně přirozená. Jestliže totiž říkám, že $u_1 \dots u_k$ je redukované slovo, tak tím naznačuji, že nevyznačenou binární operaci interpretuji jinak nežli jako binární operaci grupy $F(X)$, protože výsledek této operace je redukované slovo vždy.

Abychom se v dalším vyhnuli jakýmkoliv nedorozuměním, vyjmenujeme nyní explicitně podmínky, za kterých platí, že $u_1 \dots u_k$ je redukované slovo.

Předně musí být všechna slova $u_1, \dots, u_k$ redukovaná (jsou to prvky $F(X)$). Protože 1 odpovídá prázdnému slovu, může být kterýkoli z prvků u_i roven 1. Je-li $1 \leq i < j \leq k$, $u_i \neq 1$, $u_j \neq 1$, $u_r = 1$ pro všechna r splňující $i < r < j$, $x \in X^{\pm 1}$ je poslední symbol u_i a $y \in X^{\pm 1}$ je první symbol u_j , tak musí platit $x \neq y^{-1}$.

10.6 Tvzení. *Bud' $G = \langle X \rangle$ grupa. Pak X je volnou bází G , jestliže $x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} \neq 1$, kdykoliv je $n \geq 1$ a pro každé i , $1 \leq i \leq n$, platí $x_i \in X$, $\varepsilon_i \in \{-1, 1\}$, přičemž pro $i < n$ je $x_i \neq x_{i+1}$ nebo $\varepsilon_i \neq -\varepsilon_{i+1}$.*

Důkaz. Ať $F(X)$ je volná grupa redukovaných slov nad X , přičemž $g: F(X) \rightarrow G$ je epimorfismus, který splňuje $g(x) = x$ pro všechna $x \in X$. Tento epimorfismus je injektivní, právě když je splněna podmínka tvrzení. $\square$

10.7 Lemma. *Bud' $Y \subseteq F(X)$ a ať každé $y \in Y$ je rovno redukovanému slovu $a_y b_y c_y$, kde b_y je různé od 1. Ať je $Y \cap Y^{-1} = \emptyset$ a položme $a_{y^{-1}} = (c_y)^{-1}$, $b_{y^{-1}} = (b_y)^{-1}$ a $c_{y^{-1}} = (a_y)^{-1}$. Předpokládejme, že pro libovolná $y, z \in Y^{\pm 1}$, jež splňují $z \neq y^{-1}$ a kde délka a_y nepřesahuje délku c_z , lze nalézt slovo $w_{z,y} \in F(X)$ takové, že platí $zy = a_z b_z w_{z,y} b_y c_y$, přičemž poslední slovo je redukované. Potom Y je volná báze grupy $\langle Y \rangle$.*

Důkaz. Budte $y, z \in Y$, $y^{-1} \neq z$. Pak $w_{z,y} \in F(X)$ takové, že $a_z b_z w_{z,y} b_y c_y$ je redukované slovo, jež je v $F(X)$ rovno zy , existuje bez ohledu na délky a_y a c_z . Je-li totiž délka $a_y = (c_{y^{-1}})^{-1}$ větší než délka $c_z = (a_{z^{-1}})^{-1}$,

je $(zy)^{-1} = y^{-1}z^{-1}$ v $F(X)$ podle našich předpokladů rovno redukovanému slovu $a_{y^{-1}} b_{y^{-1}} w_{y^{-1}, z^{-1}} b_{z^{-1}} c_{z^{-1}}$, a inverzí dostáváme redukované slovo $a_z b_z (w_{y^{-1}, z^{-1}})^{-1} b_y c_y$.

Uvažme nyní $n \geq 1$ a $y_i \in Y^{\pm 1}$, $1 \leq i \leq n$, taková, že $y_i^{-1} \neq y_{i+1}$ platí pro každé i , $1 \leq i < n$. Potom $y_1 \dots y_n$ je rovno redukovanému slovu $a_{y_1} b_{y_1} w_{y_1, y_2} b_{y_2} w_{y_2, y_3} b_{y_3} \dots b_{y_{n-1}} w_{y_{n-1}, y_n} c_{y_n}$, které je různé od 1, neboť b_{y_1} je různé od 1. Množina Y je volnou bází grupy $\langle Y \rangle$ podle tvrzení 10.6. $\square$

Nyní vsuneme tvrzení, jež umožňuje konstruovat množinu generátorů podgrupy H grupy G v případě, kdy je dána množina generátorů X grupy G a kdy H je rovno stabilizátoru G_ω nějaké akce G na Ω , $\omega \in \Omega$. Přitom předpokládáme, že pro každé $\gamma \in \Gamma$, kde Γ je orbita tranzitivity, jež obsahuje ω , je vybrán prvek $g_\gamma \in G$ takový, že $g_\gamma(\omega) = \gamma$. Rovněž předpokládáme $g_\omega = 1$.

10.8 Lemma. *Pro každé $x \in X^{\pm 1}$ a $\gamma \in \Gamma$ položme $s_{x,\gamma} = g_{x(\gamma)}^{-1} x g_\gamma$. Potom*

- (i) $s_{x,\gamma} = 1$ právě když $x g_\gamma \in \{g_\eta; \eta \in \Gamma\}$;
- (ii) $s_{x,\gamma} \in H$ pro všechna $x \in X^{\pm 1}$ a $\gamma \in \Gamma$;
- (iii) $(s_{x,\gamma})^{-1} = s_{x^{-1}, x(\gamma)}$.

Důkaz.

- (i) Jistě je $s_{x,\gamma} = 1$, právě když platí $x g_\gamma = g_{x(\gamma)}$. Je-li $x g_\gamma$ rovno g_η pro nějaké $\eta \in \Gamma$, tak platí $x(\gamma) = x g_\gamma(\omega) = g_\eta(\omega) = \eta$.
- (ii) Zde stačí ověřit $s_{x,\gamma}(\omega) = \omega$.
- (iii) Jelikož platí $x^{-1}(x\gamma) = \gamma$, tak je $s_{x^{-1}, x(\gamma)}$ rovno $g_\gamma^{-1} x^{-1} g_{x(\gamma)} = (s_{x,\gamma})^{-1}$. $\square$

10.9 Tvzení. *Ať grupa $G = \langle X \rangle$ působí na množině Ω , $\omega \in \Omega$, a ať $\Gamma \subseteq \Omega$ je orbita tranzitivity, která obsahuje ω . Ať dále je pro každé $\gamma \in \Gamma$ vybrán prvek $g_\gamma \in G$ takový, že $g_\gamma(\omega) = \gamma$. Předpokládejme $g_\omega = 1$. Potom $G_\omega = \langle g_{x(\gamma)}^{-1} x g_\gamma; x \in X \text{ a } \gamma \in \Gamma \rangle$.*

Důkaz. Použijeme opět označení $s_{x,\gamma} = g_{x(\gamma)}^{-1} x g_\gamma$. Podle 10.8(ii) a 10.8(iii) stačí dokázat, že každé $g = x_n \dots x_1 \in G_\omega$, kde $x_i \in X^{\pm 1}$, $1 \leq i \leq n$, lze vyjádřit jako součin prvků $s_{x,\gamma}$, $x \in X^{\pm 1}$ a $\gamma \in \Gamma$. Položme $\gamma_i = x_i \dots x_1(\omega)$,

$0 \leq i \leq n$. Jelikož je $g \in G_\omega$, tak platí $\gamma_0 = \gamma_n = \omega$, a tedy $g_{\gamma_0} = g_{\gamma_n} = 1$. Proto je $g = g_{\gamma_n}^{-1} x_n \cdots x_1 g_{\gamma_0}$ rovno $(g_{\gamma_n}^{-1} x_n g_{\gamma_{n-1}}) \cdots (g_{\gamma_1}^{-1} x_1 g_{\gamma_0})$. Pro každé i , $1 \leq i \leq n$, platí $x_i(\gamma_{i-1}) = \gamma_i$, takže jsme dokázali, že g je rovno $s_{x_n, \gamma_{n-1}} \cdots s_{x_1, \gamma_0}$. $\square$

Buď G grupa a H její podgrupa. Množina $T \subseteq G$ se nazývá *levou transversálou* podgrupy H , jestliže splňuje podmínky

$$(i) \ t_1 H = t_2 H \Rightarrow t_1 = t_2 \text{ pro všechna } t_1, t_2 \in T \quad \text{a} \quad (ii) \ \bigcup_{t \in T} tH = G.$$

Je-li splněna jen implikace (i), mluvíme o částečné (parciální) transversále.

10.10 Tvzení. Ať grupa $G = \langle X \rangle$ má podgrupu H a ať $T \subseteq G$ je levá transversála H , přičemž je $1 \in T$. Položme $\Omega = \{gH; g \in G\}$ a ať $t_\omega \in T \cap \omega$ pro všechna $\omega \in \Omega$. Potom $t_{x\omega}^{-1} x t_\omega$ je prvek H pro všechna $x \in X$ a $\omega \in \Omega$ a podgrupa H je generována množinou

$$Y = \{t_{x\omega}^{-1} x t_\omega; x \in X, \omega \in \Omega \text{ a } xt_\omega \notin T\}.$$

Přitom $Y^{\pm 1} = \{t_{x\omega}^{-1} x t_\omega; x \in X^{\pm 1}, \omega \in \Omega \text{ a } xt_\omega \notin T\}$ a podmínka $xt_\omega \notin T$ je ekvivalentní podmínce $x^{-1}t_{x\omega} \notin T$.

Důkaz. Uvažme působení grupy G na levých rozkladových třídách H translacemi. Podle předpokladu tvrzení je $t_H = 1$ a $t_\omega(H) = \omega$ pro všechna $\omega \in \Omega$. Podle 10.9 je grupa H generována množinou všech prvků $t_{x\omega}^{-1} x t_\omega$, $x \in X$ a $\omega \in \Omega$. Podle 10.8(i) se $t_{x\omega}^{-1} x t_\omega$ rovná 1, právě když je $xt_\omega \in T$, takže je $H = \langle Y \rangle$.

Je-li $\omega \in \Omega$ a $x \in X^{\pm 1}$, tak $xt_\omega \in T$ nastane podle 10.8 (i) a (iii) právě pro $x^{-1}t_{x\omega} \in T$. Z tohoto důvodu z 10.8 (iii) také dostáváme $Y^{-1} = \{t_{x\omega}^{-1} x t_\omega; x \in X^{-1}, \omega \in \Omega \text{ a } xt_\omega \notin T\}$. $\square$

Všimněte si, že množina Ω je konečná, právě když H je podgrupa konečného indexu.

10.11 Důsledek. Buďte G konečně generovaná grupa a H její podgrupa konečného indexu. Potom je i H konečně generovaná. $\square$

Naším cílem nyní bude ukázat, že každá podgrupa H volné grupy $F(X)$ je opět volná. Budeme postupovat takzvanou Reidemeisterovou-Schreierovou metodou a hledat množinu generátorů ve tvaru daném tvrzením 10.10. (Volnost podgrupy volné grupy lze ovšem dokázat i jinak. Nielsenova metoda je přitažlivá svou konstrukční povahou a geometrická metoda svou elegancí. Reidemeisterova-Schreierova metoda však vyžaduje nejmenší množství dodatečných definic.)

Je-li T (částečná) levá transversála podgrupy H volné grupy $F(X)$, která má tu vlastnost, že pro každé redukované slovo $vw \in T$ je $w \in T$, mluvíme o (částečné) *Schreierově transversále*. Všimněte si, že každá Schreierova transversála musí nutně obsahovat jednotkový prvek.

10.12 Lemma. Ke každé podgrupě H volné grupy $F(X)$ existuje alespoň jedna Schreierova transversála.

Důkaz. Uspořádejme množinu všech částečných Schreierových transversál podgrupy H inkluzí. Sjednocení řetězce do sebe vřazených takovýchto transversál je opět částečná Schreierova transversála H . Podle Zornova lematu existuje částečná Schreierova transversála T , která je vůči uspořádání inkluzí maximální. Předpokládejme, že redukované slovo $w \in F(X)$ neleží v $\bigcup_{t \in T} tH$ a že w je nejkratší možné. Jistě je $T \neq \emptyset$, takže $w \neq 1$ a $w = xv$, kde $x \in X^{\pm 1}$ a $vH = tH$ pro nějaké $t \in T$. Je tedy $xtH = wH$, a kdyby t začínalo x^{-1} , měli bychom $xt \in T$. To však podle volby w možné není, takže $T \cup \{xt\}$ je částečná Schreierova transversála. To je ovšem spor s maximalitou T , takže T musí být úplná Schreierova transversála. $\square$

10.13 Tvzení. Buď H podgrupa volné grupy $F(X)$ redukovaných slov nad X a ať T je Schreierova transversála H . Ať $\Omega = \{gH; g \in F(X)\}$ a ať pro každé $\omega \in \Omega$ je $T \cap \omega = \{t_\omega\}$. Položme $Y = \{t_{x\omega}^{-1} x t_\omega; x \in X, \omega \in \Omega \text{ a } xt_\omega \notin T\}$. Potom je Y volnou bází H a každé slovo $t_{x\omega}^{-1} x t_\omega \in Y$ je redukované.

Důkaz. Podle 10.10 je $H = \langle Y \rangle$ a $Y^{\pm 1} = \{t_{x\omega}^{-1} x t_\omega; x \in X^{\pm 1}, \omega \in \Omega \text{ a } xt_\omega \notin T\}$. Podmínku $xt_\omega \notin T$ lze přitom vyjádřit též jako $x^{-1}t_{x\omega} \notin T$. Slovo t_ω v takovém případě nezačíná symbolem x^{-1} (bylo by $xt_\omega = t_{x\omega}$) a slovo $t_{x\omega}$ nezačíná symbolem x (bylo by $x^{-1}t_{x\omega} = t_\omega$). Každé ze slov $y = t_{x\omega}^{-1} x t_\omega \in Y^{\pm 1}$ je proto redukované, přičemž vyznačené x je počátkem

nejkratšího koncového úseku slova y , který neleží v T . Položíme $a_y = t_{x\omega}^{-1}$, $b_y = x$ a $c_y = t_\omega$. Jelikož y^{-1} je rovno $t_\omega^{-1}x^{-1}t_{x\omega}$, tak platí $a_{y^{-1}} = (c_y)^{-1}$, $b_{y^{-1}} = (b_y)^{-1}$ a $c_{y^{-1}} = (a_y)^{-1}$.

Ověřili jsme, že jsou splněny úvodní předpoklady lemmatu 10.7, a k dokončení důkazu stačí podle 10.7 doložit, že pro libovolná $y, y' \in Y^{\pm 1}$, $y = t_{x\omega}^{-1}xt_\omega$ a $y' = t_{x'\omega'}^{-1}x't_{\omega'}$, kde je $y' \neq y^{-1}$ a délka $t_{\omega'}$ není menší než délka $t_{x\omega}^{-1}$, lze nalézt $w \in F(X)$ takové, že slovo $x'wx$ je redukované a je v $F(X)$ rovno $x't_{\omega'} \cdot t_{x\omega}^{-1}x$. Přitom $y' \neq y^{-1}$ nastane, právě když uspořádané dvojice $(x^{-1}, x\omega)$ a (x', ω') jsou různé, a proto hledané $w \in F(X)$ jistě existuje, mají-li slova $t_{\omega'}$ a $t_{x\omega}^{-1}$ stejnou délku. Ať tedy je $t_{\omega'}$ delší než $t_{x\omega}^{-1}$. Pak požadovaného vyjádření nemusíme dosáhnout jedině v případě, když $t_{\omega'}$ končí slovem $x^{-1}t_{x\omega}$. Pak by ale bylo $x^{-1}t_{x\omega} \in T$, a to není možné. $\square$

10.14 Důsledek. Každá podgrupa volné grupy je volná. $\square$

11 Definující relace a volný součin grup

11.1 Lemma. Buď G grupa a $A \subseteq G$.

(i) Ať H označuje grupu generovanou A . Pak

$$H = \{a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k}; a_i \in A \text{ a } |\varepsilon_i| = 1 \text{ pro všechna } 1 \leq i \leq k\}.$$

(ii) Ať N označuje nejmenší normální podgrupu G , která obsahuje A . Pak N je generována množinou

$$\bigcup_{g \in G} (gAg^{-1}) = \{gag^{-1}; g \in G, a \in A\}.$$

Důkaz.

(i) V H jistě leží všechny prvky G , které lze vyjádřit jako součin $a_1^{\varepsilon_1} \dots a_k^{\varepsilon_k}$, kde $k \geq 0$, $\varepsilon_i \in \{-1, 1\}$ a $a_i \in A$ pro $1 \leq i \leq k$. (Je-li $k = 0$, jde

o jednotkový prvek.) Naopak, prvky tohoto tvaru jsou jistě uzavřeny na součin a inverzní operaci, takže jde o podgrupu obsahující A .

(ii) V N jistě leží všechny prvky tvaru gag^{-1} , kde $g \in G$ a $a \in A$, a proto v ní leží i podgrupa těmito prvky generovaná. Přitom tato podgrupa je normální, neboť $h(gag^{-1})h^{-1} = (hg)a(hg)^{-1}$ pro všechna $g, h \in G$ a $a \in A$. $\square$

Je-li grupa G generována množinou X a F je volná grupa redukováných slov s bází X , lze identitu id_X rozšířit na epimorfismus $\pi: F \rightarrow G$. Jádrem $N = \text{Ker } \pi$ tohoto epimorfismu je normální podgrupa grupy F , která je podle 10.14 volná, a proto je buď triviální, nebo nekonečná. Dvojice $(F; N)$ charakterizuje grupu G až na izomorfismus, neboť platí $G \cong F/N$. Takový popis ovšem není nijak úsporný, neboť F i N jsou nekonečné množiny. Proto je nahrazujeme menšími množinami, které ve většině důležitých případů konečné jsou a ze kterých můžeme F i N jednoznačně odvodit. Místo F se uvádí pouze množina generátorů X a místo N se uvažuje taková množina $R \subseteq F$, že N je rovna nejmenší normální podgrupě F , která obsahuje R . Tím se dostáváme k pojmu prezentace.

Ať pro každou množinu X označuje $F(X)$ volnou grupu redukováných slov s bází X .

Trojici $(X; R; \pi)$ nazveme *prezentací grupy* G , jestliže je $\pi: F(X) \rightarrow G$ epimorfismus, $R \subseteq F(X)$ a $\text{Ker } \pi$ je nejmenší normální podgrupa $F(X)$, která obsahuje R . Grupě $\text{Ker } \pi$ se říká *jádro prezentace*.

Trojice $(X; R; \pi)$ se většinou udává jako dvojice $(X; R)$. V takovém případě se předpokládá, že X je obsaženo v G , generuje G a π je indukováno identitou id_X .

Každý prvek $r \in R$ lze, jak je zřejmé, nahradit prvkem r^{-1} nebo prvkem srs^{-1} , kde $s \in F(X)$ je libovolné.

Prvky R se většinou zapisují jako rovnosti, přičemž zápis $u = v$ znamená $uv^{-1} \in R$. Rovnosti chápeme symetricky, a proto je na místě ověřit, že $u = v$ má v tomto kontextu stejný význam jako $v = u$. Že tomu tak je, plyne ze vztahu $vu^{-1} = (uv^{-1})^{-1}$.

Rovnostem $u = v$, které definují prvky R , se říká *definující relace*. Definující relaci $u = v$ můžeme místo uv^{-1} chápat jako zadání prvku $u^{-1}v$, neboť uv^{-1} a $u^{-1}v$ jsou v $F(X)$ konjugované. Definující relace $u = v$ uvedená v prezentaci $(X; R; \pi)$ grupy G znamená, že v grupě G platí $\pi(u) = \pi(v)$,

nikoliv, že v grupě $F(X)$ je slovo u rovno slovu v .

Například jednou z prezentací grupy kvaternionů generované prvky a, b je $(a, b; a^4, (ab)^2b^{-2}, a^2b^{-2})$, což se zapisuje ve formě definujících relací jako $(a, b; a^4 = 1, (ab)^2 = b^2, a^2 = b^2)$.

Je-li množina R konečná, mluvíme o *konečně prezentované grupě*.

Lze dokázat, že neexistuje algoritmus který by uměl o každé prezentaci rozhodnout, zda je, či není prezentací triviální grupy. Existují však nepřilíš komplikované algoritmické postupy, o kterých se ví, že v případě, kdy zadaná prezentace určuje konečnou grupu, naleznou nějakou úplnou transversálu jádra prezentace. Zde se těmito algoritmy zabývat nebudeme a uvedeme pouze následující pozorování, které nám v mnoha případech umožňuje dokázat, že daná prezentace určuje nějakou předem známou grupu.

11.2 Lemma. *Ať $R \subseteq F(X)$ a $n > 0$ vyhovují podmínce, že pro každou grupu H , pro kterou existuje epimorfismus $\psi: F(X) \rightarrow H$ splňující $R \subseteq \text{Ker } \psi$, platí $|H| \leq n$. Je-li $\varphi: F(X) \rightarrow G$ epimorfismus, $R \subseteq \text{Ker } \varphi$ a $|G| \geq n$, je $(X; R; \varphi)$ prezentací G , a platí $|G| = n$.*

Důkaz. Ať N je nejmenší normální podgrupa $F(X)$, která obsahuje R a ať $\pi: F(X) \rightarrow F(X)/N$ je přirozená projekce. Položíme-li $H = F(X)/N$, tak podle předpokladu je $|F(X)/N| \leq n$, čili $|F(X) : N| \leq n$. Protože předpokládáme $R \subseteq \text{Ker } \varphi$, je i $N \subseteq \text{Ker } \varphi$, takže $n \leq |G| = |F(X) : \text{Ker } \varphi| \leq |F(X) : \text{Ker } \varphi| \cdot |\text{Ker } \varphi : N| = |F(X) : N| \leq n$. Musí tudíž platit $|G| = n$ a $|\text{Ker } \varphi : N| = 1$, čili $\text{Ker } \varphi = N$. $\square$

Ve zbytku této kapitoly se budeme věnovat konstrukci takzvaného volného součinu grup.

Ať G_i , $i \in I$, je neprázdný systém grup a ať pro $i, j \in I$, $i \neq j$, je $G_i \cap G_j = 1$.

Pro každé $i \in I$ označme $G_i \setminus \{1\}$ symbolem G_i^* a položme $V = \bigcup_{i \in I} G_i^*$. Ať W je volný monoid slov nad V . Jednotkovým prvkem monoidu W je prázdné slovo, a to budeme značit 1. Abychom odlišili operaci skládání slov ve W od binárních operací grup G_i , použijeme symbol $\bullet$ pro skládání slov. Na W definujeme relaci ϱ tak, že $(u, v) \in \varrho$ platí, právě když lze nalézt $u_1, u_2 \in W$, $i \in I$ a $w_1, w_2 \in G_i^*$ takové, že platí $u = u_1 \bullet w_1 \bullet w_2 \bullet u_2$ a $v = u_1 \bullet (w_1 w_2) \bullet u_2$. (Slovo v má délku o jedna menší než u , je-li $w_1 \neq w_2^{-1}$, a o dvě menší než u , je-li $w_1 = w_2^{-1}$.) Nejmenší ekvivalenci na W , která

obsahuje relaci ϱ , označíme $\sim$. Přitom $u \sim v$ zřejmě platí právě tehdy, lze-li najít posloupnost $u = u_0, \dots, u_k = v$ takovou, že je $k \geq 0$ a pro každé i , $1 \leq i \leq k$, je buď $(u_{i-1}, u_i) \in \varrho$ nebo $(u_i, u_{i-1}) \in \varrho$.

Z $u \sim v$ zjevně plyne $w \bullet u \sim w \bullet v$ a $u \bullet w \sim v \bullet w$ pro libovolné $w \in W$. Je-li $u_1 \sim v_1$ a $u_2 \sim v_2$, tak máme $u_1 \bullet u_2 \sim v_1 \bullet u_2 \sim v_1 \bullet v_2$. Označme $[u]$ třídu ekvivalence $\sim$ obsahující u . Právě jsme ukázali, že na $W/\sim$ lze vztahem $[u] \cdot [v] = [u \bullet v]$ korektně definovat binární operaci. Tato operace je asociativní a $[1]$ je jejím jednotkovým prvkem. Pro $u = u_1 \bullet \dots \bullet u_n \in W$ položme $\bar{u} = u_n^{-1} \bullet \dots \bullet u_1^{-1}$ (kde inverzní operaci provádíme v té grupě G_i , do které příslušný prvek patří). Zjevně z $(u, v) \in \varrho$ plyne $(\bar{u}, \bar{v}) \in \varrho$, takže definice $[u]^{-1} = [\bar{u}]$ je korektní. (Místo $\bar{u}$ se obvykle také píše u^{-1} .) Protože je $u \bullet \bar{u} \sim \bar{u} \bullet u \sim 1$, vidíme, že jsme na $W/\sim$ definovali strukturu grupy. Těto grupě se říká *volný součin grup G_i , $i \in I$* .

Slovo $u \in W$ nazveme *redukované*, jestliže nelze nalézt $v \in W$ tak, aby platilo $(u, v) \in \varrho$.

11.3 Lemma. *Každá třída ekvivalence $\sim$ obsahuje právě jedno redukované slovo.*

Důkaz. Není-li slovo redukované, lze postupně spojit dvojice sousedících prvků téže grupy G_i , $i \in I$, a to až do chvíle, kdy v něm žádnou takovou dvojici nelze nalézt. Každá třída $\sim$ tedy obsahuje alespoň jedno redukované slovo. Je však třeba ukázat, že pro každá dvě redukovaná slova $u, v \in W$ z $u \sim v$ plyne $u = v$.

Postupujme sporem. Pro každé $u = u_1 \bullet \dots \bullet u_n \in W$ označme $l(u)$ jeho délku, tedy $l(u) = n$. Ať $u, v \in W$ jsou různá redukovaná slova, $u \sim v$, $u = u_0, \dots, u_k = v$, přičemž $(u_{i-1}, u_i) \in \varrho$ nebo $(u_i, u_{i-1}) \in \varrho$ pro každé i , $1 \leq i \leq k$. Předpokládejme, že součet $l(u_0) + \dots + l(u_k)$ je nejmenší možný. Spor obdržíme tak, že nalezneme posloupnost $u = u'_0, \dots, u'_{k'} = v$, ve které je $(u'_{j-1}, u'_j) \in \varrho$ nebo $(u'_j, u'_{j-1}) \in \varrho$ pro každé j , $1 \leq j \leq k'$, a $\sum_{j=0}^{k'} l(u'_j) < \sum_{i=0}^k l(u_i)$.

Protože u_0 a u_k jsou redukovaná, musí být $(u_1, u_0) \in \varrho$ a $(u_{k-1}, u_k) \in \varrho$. Je tedy $l(u_1) > l(u_0)$ a $l(u_k) < l(u_{k-1})$. Ať $l(u_i)$ nabývá pro $i = r$ největší možné hodnoty. Pak je $1 \leq r < k$ a platí $(u_r, u_{r-1}) \in \varrho$ a $(u_r, u_{r+1}) \in \varrho$. Můžeme tedy u_{r-1} zapsat jako $a \bullet m \bullet b$, u_{r+1} jako $c \bullet n \bullet d$, přičemž existují $i, j \in I$, $e, f \in G_i^*$ a $g, h \in G_j^*$, že $u_r = a \bullet e \bullet f \bullet b = c \bullet g \bullet h \bullet d$.

Protože místo posloupnosti $u_0, \dots, u_k$ bychom mohli vyšetřovat po-

sloupnost $u_k, \dots, u_0$, lze předpokládat $l(a) \leq l(c)$. Je-li $l(a) = l(c)$, je $a = c$, $b = d$, $e = g$, $f = h$ a $i = j$, takže je $u_{r-1} = u_{r+1}$ a podposloupnost u_{r-1}, u_r, u_{r+1} lze nahradit jednočlennou posloupností u_{r-1} . Zbývá vyšetřit případ $l(a) < l(c)$.

Ať je $l(c) = l(a) + 1$. Pak $c = a \bullet e$, $f = g$, $i = j$ a $b = h \bullet d$, takže $u_r = a \bullet e \bullet f \bullet h \bullet d$, $u_{r-1} = a \bullet (ef) \bullet h \bullet d$ a $u_{r+1} = a \bullet e \bullet (fh) \bullet d$. Položme $\tilde{u}_r = a \bullet (efh) \bullet d$. Místo posloupnosti u_{r-1}, u_r, u_{r+1} lze použít posloupnost $u_{r-1}, \tilde{u}_r, u_{r+1}$.

Zbývá případ $l(c) \geq l(a) + 2$. Potom b lze zapsat jako $b' \bullet b''$ tak, že $c = a \bullet e \bullet f \bullet b'$, tudíž $u_r = a \bullet e \bullet f \bullet b' \bullet g \bullet h \bullet d$, $u_{r-1} = a \bullet (ef) \bullet b' \bullet g \bullet h \bullet d$, a $u_{r+1} = a \bullet e \bullet f \bullet b' \bullet (gh) \bullet d$. Položíme-li $\tilde{u}_r = a \bullet (ef) \bullet b' \bullet (gh) \bullet d$, je $(u_{r-1}, \tilde{u}_r) \in \varrho$, $(u_{r+1}, \tilde{u}_r) \in \varrho$, takže podposloupnost u_{r-1}, u_r, u_{r+1} lze nahradit posloupností $u_{r-1}, \tilde{u}_r, u_{r+1}$. $\square$

Vidíme, že důkaz 11.3 se téměř doslova shoduje s důkazem 10.2. To je, mimo jiné, dáno skutečností, že volná grupa $F(X)$ je izomorfní volnému součinu cyklických grup generovaných prvky volné báze X .

11.4 Důsledek. *Bud' $G = W/\sim$ volný součin grup G_i , $i \in I$. Pro každé $i \in I$ ať μ_i označuje zobrazení $G_i \rightarrow G$, $g \mapsto [g]$. Pak $\mu_i: G_i \rightarrow G$ je monomorfismus grup pro každé $i \in I$.*

Důkaz. Že jde o homomorfismus, je zřejmé, neboť pro $g, h \in G_i$ platí $[g \bullet h] = [gh]$. Každé ze slov $g, g \in G_i$, je redukované, a proto z 11.3 plyne, že jde o monomorfismus. $\square$

Protože v každé třídě ekvivalence $\sim$ leží právě jedno redukované slovo, můžeme volný součin grup G_i , $i \in I$, ztotožnit s množinou všech redukováných slov. Násobek dvou redukováných slov u a v je pak redukované slovo w , ve kterém se na styku slov u a v spojí prvky z téže grupy (přitom může vzniknout 1, takže může dojít k opakovanému spojování). Operace ve volném součinu se značíva obvykle také $\cdot$, symbol $\bullet$ jsme použili pouze pro větší přehlednost.

Literatura

- M. Aschbacher: *Finite group theory*, Cambridge, 1986.
- V. A. Belongov, A. N. Fomin: *Matričnice predstavenija v teorii konečných grupp*, Nauka, Moskva, 1976.
- L. Beran: *Grupy a svazy*, SNTL, Praha, 1974.
- L. Bican: *Algebra I a II*, Univerzita Karlova, Praha, 1984.
- W. Burnside: *The theory of groups of finite order*, Cambridge, 1911, dotisk Dover Publ., New York, 1955.
- R. D. Carmichael: *Groups of finite order*, Ginn & Co., Boston, 1937.
- L. E. Dickson: *Linear groups with an exposition of the Galois field theory*, Teubner, Lipsko, 1901, dotisk Dover Publ., New York, 1958.
- Jean Dieudonné: *Le Géométrie des groupes classiques*, Springer-Verlag, 1971 (třetí vydání); ruský překlad: Žan D'jodonne: *Geometrija klasičeskich grupp*, Mir, Moskva, 1974 (přeložil E. B. Vinberg).
- Marshall Hall, Jr.: *The theory of groups*, The Macmillan Company, New York, 1959; ruský překlad: M. Choll: *Teorija grupp*, Izdatel'stvo inostrannej literatury, Moskva, 1962.
- B. Huppert: *Endliche gruppen I*, Springer-Verlag, 1967.
- G. James a M. Liebeck: *Representations and characters of groups*, Cambridge, 1993.
- M. I. Kargapolova, Ju. I. Merzljakov: *Osnovy teorii grupp*, Nauka, Moskva, 1977.
- A. G. Kuroš: *Lekcii po obščej algebre*, Fizmatgiz, Moskva, 1962; český překlad: *Kapitoly z obecné algebry*, Academia, Praha, 1968, 1977.
- R. Lyndon a P. Schupp: *Combinatorial group theory*, Springer-Verlag, 1977.
- W. Magnus, A. Karrass, D. Solitar: *Combinatorial group theory*, Cambridge, 1993; ruský překlad: V. Magnus, A. Karras, D. Soliter: *Kombinatornaja teorija grupp*, Nauka, Moskva, 1974.
- W. A. Manning: *Primitive groups*, Stanford University Publ., 1921.
- D. S. Passman: *Permutation groups*, Benjamin, 1968.
- L. Procházka a kol.: *Algebra*, Academia, Praha, 1990.
- L. Procházka: *Úvod do studia reprezentací grup*, Karolinum, Praha, 1999.
- D. J. S. Robinson: *A Course in the theory of groups*, Springer-Verlag, 1982.

Literatura

- J. J. Rotman: *An Introduction to the theory of groups*, Springer-Verlag, 1991 (čtvrté vydání).
- W. R. Scott: *Group theory*, Prentice-Hall, Inc., Englewood Cliffs, 1964.
- Jean-Pierre Serre: *Représentations linéaires des groupes finis*, Hermann, Paris, 1967; ruský překlad: Ž.-P. Serr: *Linejnyje predstavenija konečných grupp*, Mir, Moskva, 1970; anglická novější verze: Jean-Pierre Serre: *Linear Representations of Finite Groups*, Springer-Verlag, 1977.
- Charles C. Sims: *Computations with finitely presented groups*, Cambridge, 1994.
- W. Specht: *Gruppentheorie*, Springer-Verlag, 1956.
- M. Suzuki: *Group theory, I a II*, Springer-Verlag, 1982 a 1986.
- W. Wielandt: *Finite permutation groups*, Academic Press, 1964.
- H. Zassenhaus: *The theory of groups*, Vandenhoeck & Ruprecht, Göttingen, 1956 (druhé vydání).

Seznam symbolů

$ G $	5	$ g $	25
$S(X)$	6	$[a, b]$	25
$\text{Inn}(G)$	7	G'	26
$\text{Aut}(G)$	7	$\prod_{i \in I} G_i$	28
$\text{End}(G)$	7	$\prod_{i \in I} G_i$	28
$ G : H $	8	$S(H, K, \varphi)$	29
$\text{Ker } \varphi$	9	$\bigoplus_{i \in I} G_i$	31
$\text{Im } \varphi$	9	$C(p_\infty)$	42
$C_G(M)$	21	$g * \omega$	43
$N_G(M)$	21	G_ω	44
$Z(G)$	21	$\sim$	44
$\text{Out}(G)$	22	${}^k H$	45
$\vartheta_i(G)$	22	$\text{Syl}_p(G)$	47
$Z_i(G)$	23	$(X; R; \pi)$	62
$\langle M \rangle$	25	$\text{Ker } \pi$	62