1. Elementární teorie grup

V této kapitolce připomeneme a shrneme základní poznatky z teorie grup, které budeme využívat.

1.1 Definice. *Grupa* je množina G s jednou binární operací $\cdot$ takovou, že

1) $(\forall a, b, c \in G):$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
2) $(\exists 1 \in G):$ $a \cdot 1 = a = 1 \cdot a$,
3) $(\forall a \in G)(\exists\, a^{-1} \in G):$ $a \cdot a^{-1} = 1 = a^{-1} \cdot a$.

Grupa G se nazývá *Abelova* (nebo také *abelovská*), pokud navíc pro každé $a, b \in G$ platí

$$a \cdot b = b \cdot a.$$

Je zvykem vynechávat znak pro operaci tam, kde nemůže dojít k omylu, proto budeme nadále místo $a \cdot b$ psát jen ab.

1.2 Definice. Nechť $(G, \cdot)$ a $(H, *)$ jsou grupy. Zobrazení $f\colon G \to H$ je *(grupový) homomorfismus*, pokud pro každé $a, b \in G$ platí

$$f(ab) = f(a) * f(b).$$

Homomorfismus, který je prostý a na, nazveme *izomorfismus* grup G a H.

Pozorný čtenář si možná všiml, že grupu a její množinu značíme stejně. To je běžné, opět tak budeme činit, pokud to nebude vést k omylům.

Označíme-li 1_G jednotkový prvek grupy G a 1_H jednotkový prvek grupy H, potom pro každý homomorfismus $f\colon G \to H$ platí:

1) $f(1_G) = 1_H$
2) $(\forall a \in G) : f(a^{-1}) = f(a)^{-1}$

1.3 Definice. Buď G grupa. Podmnožina H grupy G je její *podgrupou* (značíme $H \leq G$), pokud

1) $(\forall a, b \in H) : ab \in H$,
2) $(\forall a \in H) : a^{-1} \in H$.

Tedy podgrupa H grupy G je její podmnožina, která je sama grupou (se stejnou operací jako u G).

1.4 Definice. Podgrupa H grupy G je její *normální podgrupou* (značíme $H \trianglelefteq G$), pokud pro každé $a \in G$ platí

$$H = aHa^{-1}.$$

Průnik libovolné množiny podgrup grupy G je opět podgrupa grupy G. Stejně tak je průnik libovolné množiny normálních podgrup grupy G normální podgrupa G.

1.5 Definice. Nechť X je podmnožina grupy G. Symbolem $\langle X \rangle$ označíme průnik všech podgrup G, které obsahují X. Je to nejmenší podgrupa G obsahující X. Tuto podgrupu budeme nazývat *podgrupa generovaná množinou X*.

1.6 Definice. Nechť H je podgrupa grupy G a $a \in G$. *Pravá rozkladová třída podle H v G (reprezentovaná a)* je množina $Ha = \{ha \mid h \in H\}$. Prvek a se nazývá *reprezentant třídy Ha*. Podobně se definuje *levá rozkladová třída podle H v G* jako aH.

Platí: Nechť $H \leq G$. Potom:

- $Ha = Hb \iff ab^{-1} \in H \qquad (aH = bH \iff b^{-1}a \in H)$
- Každé dvě pravé rozkladové třídy jsou buďto disjunktní, nebo se shodují.
- Počet levých rozkladových tříd podle H je roven počtu pravých rozkladových tříd podle H.

1.7 Definice. Nechť $H \leq G$. *Index H* v G je mohutnost množiny pravých rozkladových tříd podle H v G, značíme $[G : H]$.

1.8 Věta (Lagrangeova). Nechť H je podgrupa konečné grupy G. Potom platí

$$|G| = |H| \cdot [G : H].$$

Odtud speciálně plyne, že počet prvků pdgrupy H dělí počet prvků grupy G.

Podgrupa H grupy G je normální podgrupa, právě když pro každé $a \in G$ platí $aH = Ha$. Je-li N normální podgrupa G, tvoří pravé rozkladové třídy podle N grupu mohutnosti $[G : N]$, kterou označíme G/N, násobení je definováno $Na \cdot Nb = Nab$.

1.9 Definice. Symbolem $\langle X \rangle^G$ označíme průnik všech normálních podgrup, které obsahují X. Je to nejmenší normální podgrupa G obsahující X, nazýváme ji *normální podgrupa generovaná* X, či *normální uzávěr* X *v* G.

1.10 Definice. Buď $f : G \to H$ grupový homomorfismus. *Jádrem* homomorfismu f budeme rozumět množinu $N = \{a \in G \mid f(a) = 1_H\}$, kterou označíme $\operatorname{Ker} f$.

Jádro homomorfismu $f : G \to H$ je normální podgrupa grupy G. Je-li naopak N normální podgrupa grupy G, je zobrazení $\pi : G \to G/N$ definované předpisem $\pi(a) = Na$, $a \in G$, grupovým homomorfismem, jehož jádrem je právě N. Zobrazení π nazýváme *přirozená projekce*.

1.11 Věta (První věta o izomorfismu). Nechť $f : G \to H$ je homomorfismus s jádrem N. Potom je N normální podgrupa G a platí, že $G/N \simeq \operatorname{Im}(f)$.

Důkaz. Nejprve ukážeme, že $N \trianglelefteq G$. K tomu stačí, aby pro každé $a \in G$ a $b \in N$ bylo $aba^{-1} \in N$. Ovšem

$$f(aba^{-1}) = f(a)f(b)f(a^{-1}) = f(a)f(a^{-1}) = f(a)f(a)^{-1} = 1_H,$$

tedy je skutečně N normální v G.

Nyní definujme zobrazení $\varphi : G/N \to H$ předpisem $\varphi(Na) = f(a)$. Ověříme, že je zobrazení φ dobře definováno a že je prosté:

$$Na = Nb \iff ab^{-1} \in N \iff f(ab^{-1}) = 1_H \iff f(a) = f(b).$$

Dále z rovností

$$\varphi(NaNb) = \varphi(Nab) = f(ab) = f(a)f(b) = \varphi(Na)\varphi(Nb)$$

plyne, že je zobrazení φ homomorfismus. Protože je zřejmě $\operatorname{Im}\varphi = \operatorname{Im} f$, je φ izomorfismus G/N na $\operatorname{Im} f$. □

1.12 Lemma. Je-li $N \trianglelefteq G$ a $H \leq G$, potom $NH = N \vee H = HN$.

1.13 Věta (Druhá věta o izomorfismu). Nechť N, H jsou podgrupy grupy G takové, že N je normální. Potom je $N \cap H \trianglelefteq H$ a platí

$$H/H \cap N \simeq NH/N.$$

Důkaz. Všimněme si, že NH/N se skládá právě z těch rozkladových tříd podle N v G, které mají reprezentanta v H. Označme π' restrikci přirozené projekce $\pi : G \to G/N$ na H. Jádro π' je rovno $N \cap H$, podle předchozí věty je tedy $H/H \cap N \simeq \operatorname{Im}\pi'$. Ovšem obraz π' je složen právě z rozkladových tříd podle N v G, které mají reprezentanta v H, což je přesně NH/N. □

1.14 Věta (Třetí věta o izomorfismu). Nechť $K \leq H \leq G$. Jsou-li K i H normální podgrupy grupy G, platí, že $H/K \trianglelefteq G/K$ a

$$(G/K)/(H/K) \simeq G/H.$$

Důkaz. Definujme zobrazení $f : G/K \to G/H$ předpisem $f(Ka) = Ha$. Snadno ověříme, že je to homomorfismus na s jádrem H/K, potom už stačí použít první větu o izomorfismu. □

1.15 Definice. Nechť $a, b \in G$. *Komutátor* a a b je prvek

$$[a, b] = aba^{-1}b^{-1}.$$

Symbolem G' označíme *derivovanou podgrupu* grupy G, což je grupa generovaná všemi komutátory.

1.16 Tvrzení. G' je normální podgrupa G. Navíc je pro $H \trianglelefteq G$ grupa G/H Abelova, právě když $G' \leq H$.

Důkaz. První část plyne ze snadného pozorování, že $c[a,b] = [cac^{-1}, cbc^{-1}]c$ pro každé $a,b,c \in G$, tedy též $cG' = G'c$ pro každé $c \in G$.

Druhá část se skládá ze dvou implikací. Nechť je nejprve G/H abelovská, potom pro každé $a,b \in G$ platí

$$Hab = HaHb = HbHa = Hba.$$

Odtud máme, že $aba^{-1}b^{-1} \in H$, H obsahuje všechny komutátory a tudíž i G' jimi generovanou. Provedeme-li tyto úvahy opačným směrem, dostaneme platnost zbývající implikace. □

Cvičení

1) Buď G grupa. Pro $a_1, \ldots, a_n \in G$ označme

$$[a_1, \ldots, a_n] = a_1 a_2 \cdots a_n a_1^{-1} a_2^{-1} \cdots a_n^{-1}.$$

Dokažte, že

$$G' = \{[a_1, \ldots, a_n] \mid n \in \mathbb{N}, a_i \in G\}.$$

Návod: $[a,b][c,d] = [a, ba^{-1}, b^{-1}, c, dc^{-1}, d^{-1}]$

2) Buď T těleso a označme $T[x,y]$ okruh všech polynomů v proměnných x,y nad tělesem T. Označme $T[x], T[y]$ podokruhy okruhu $T[x,y]$ polynomů v proměnné x, resp. y. Buď G množina všech matic tvaru

$$A = \begin{pmatrix} 1 & f(x) & h(x,y) \\ 0 & 1 & g(y) \\ 0 & 0 & 1 \end{pmatrix},$$

kde $f(x) \in T[x], g(y) \in T[y]$ a $h(x,y) \in T[x,y]$.

a) Dokažte, že G s maticovým násobením je grupa.

Návod: Matici A označme (f,g,h). Ověřte, že

$$(f_1,g_1,h_1)(f_2,g_2,h_2) = (f_1+f_2, g_1+g_2, h_1+h_2+f_1g_2),$$

$$(f,g,h)^{-1} = (-f, -g, fg-h).$$

b) Dokažte, že $G' = \{(0,0,h) \mid h \in T[x,y]\}$.

Návod: Platí

$$[(f_1,g_1,h_1),(f_2,g_2,h_2)] = (0,0,f_1g_2 - f_2g_1),$$

na druhou stranu pro $h(x,y) = \sum a_{ij}x_iy_j$ platí

$$(0,0,h) = \prod_{i,j} [(a_{ij}x_i, 0, 0), (0, y_j, 0)].$$

c) Ukažte, že $\{[g,h] \mid g,h \in G\} \subsetneq G'$.

Návod: Polynom $h(x,y) = x^2 + xy + y^2$ není tvaru $p(x,y) = f_1(x)g_2(y) - f_2(x)g_1(y)$, hodnost matice $h(x,y)$ je totiž 3, ale hodnost matice libovolného $p(x,y)$ je nejvýše 2. Matice A_h polynomu $h(x,y) = \sum a_{ij}x_iy_j$ je matice, kde v i-tém řádku a j-tém sloupci je číslo a_{ij}.