12. O rozkladech grup vytvořených podgrupami

12.1. Pojem levé a pravé třídy.

Velmi důležitá vlastnost grup záleží v tom, že každá podgrupa v libovolné grupě určuje na ní jisté rozklady. Uvažujme opět o libovolné grupě $\mathfrak{G}$ a o nějaké podgrupě $\mathfrak{A} \subset \mathfrak{G}$. Nechť a značí libovolný prvek v $\mathfrak{G}$.

Podmnožina $a\mathfrak{A}$ *v* $\mathfrak{G}$, t. j. tedy *množina součinů prvku a s každým prvkem v* $\mathfrak{A}$, *nazývá se levá třída prvku a vzhledem k podgrupě* $\mathfrak{A}$ nebo stručněji, víme-li, že jde o podgrupu $\mathfrak{A}$, *levá třída prvku a*; podobně se nazývá *podmnožina* $\mathfrak{A}a$, t. j. *množina součinů každého prvku v* $\mathfrak{A}$ *s prvkem a, pravá třída prvku a vzhledem k podgrupě* $\mathfrak{A}$, stručněji: *pravá třída prvku a*. Všimněme si, že pole A podgrupy $\mathfrak{A}$ je současně levá i pravá třída prvku $\underline{1}$ vzhledem k $\mathfrak{A}$.

V několika jednoduchých větách popíšeme nejprve vlastnosti levých tříd; vlastnosti pravých tříd jsou analogické a třebaže je kvůli úspoře místa výslovně neuvádíme, doporučujeme čtenáři, aby si je rovněž promyslil.

12.2. Vlastnosti levých (pravých) tříd.

Nechť a, b značí libovolné prvky v $\mathfrak{G}$.

12.2.1. *Levá třída* $a\mathfrak{A}$ *obsahuje prvek a.*

Skutečně, protože $\mathfrak{A}$ je podgrupa, máme $\underline{1} \in \mathfrak{A}$, a odtud plyne $a = a\underline{1} \in a\mathfrak{A}$.

12.2.2. *Když a jen když $a \in \mathfrak{A}$, jest $a\mathfrak{A} = A$.*

Za účelem důkazu předpokládejme nejprve $a \in \mathfrak{A}$. Protože $\mathfrak{A}$ je podgrupa, je součin prvku a s každým prvkem v $\mathfrak{A}$ obsažen opět v $\mathfrak{A}$, takže máme vztah $a\mathfrak{A} \subset A$. Mimoto $a^{-1} \in \mathfrak{A}$ a pro libovolný prvek $x \in \mathfrak{A}$ platí $a^{-1}x \in \mathfrak{A}$, takže $a(a^{-1}x) \in a\mathfrak{A}$; avšak $a(a^{-1}x) = (aa^{-1})x = \underline{1}x = x$; vychází tedy $x \in a\mathfrak{A}$ a máme další vztah $A \subset a\mathfrak{A}$. Tedy je skutečně $a\mathfrak{A} = A$. Nechť nyní pro některý prvek $a \in \mathfrak{G}$ platí rovnost $a\mathfrak{A} = A$. Pak každý součin ax, kde $x \in \mathfrak{A}$, je obsažen v $\mathfrak{A}$, a tedy zejména (pro $x = \underline{1}$) je prvek a obsažen v $\mathfrak{A}$.

Zobecněním věty **12.2.2.** je věta:

12.2.3. *Když a jen když* $a^{-1}b \in \mathfrak{A}$, *jest* $a\mathfrak{A} = b\mathfrak{A}$.

Skutečně, když $a^{-1}b \in \mathfrak{A}$, máme podle věty **12.2.2**: $a^{-1}b\mathfrak{A} = A$ a tedy platí tyto rovnosti: $b\mathfrak{A} = (aa^{-1})b\mathfrak{A} = a(a^{-1}b)\mathfrak{A} = a(a^{-1}b\mathfrak{A}) = a\mathfrak{A}$. Naopak plyne z rovnosti $b\mathfrak{A} = a\mathfrak{A}$ vztah $(a^{-1}b)\mathfrak{A} = A$, a tedy $a^{-1}b \in \mathfrak{A}$ podle věty **12.2.2.**

12.2.4. *Levé třídy* $a\mathfrak{A}$, $b\mathfrak{A}$ *jsou buď disjunktní nebo identické.*

Tato důležitá vlastnost levých tříd plyne z této úvahy: Mají-li obě levé třídy $a\mathfrak{A}$, $b\mathfrak{A}$ některý prvek x společný, takže $x \in a\mathfrak{A}$, $x \in b\mathfrak{A}$, pak je $a^{-1}x \in \mathfrak{A}$, $b^{-1}x \in \mathfrak{A}$ a odtud podle věty **12.2.3** vychází $a\mathfrak{A} = x\mathfrak{A} = b\mathfrak{A}$ takže obě levé třídy $a\mathfrak{A}$, $b\mathfrak{A}$ jsou identické.

12.2.5. *Levé třídy* $a\mathfrak{A}$, $b\mathfrak{A}$ *jsou ekvivalentní množiny.*

Máme ukázat, že existuje prosté zobrazení množiny $a\mathfrak{A}$ na $b\mathfrak{A}$. Každý prvek v $a\mathfrak{A}$ ($b\mathfrak{A}$) je součin ax (bx) prvku a (b) s vhodným prvkem $x \in \mathfrak{A}$ a takový prvek x jest jenom jeden, neboť z rovnosti $ax = ay$ ($bx = by$) plyne $x = y$. Naopak, když $x \in \mathfrak{A}$, máme $ax \in a\mathfrak{A}$ ($bx \in b\mathfrak{A}$). Vidíme tedy, že zobrazení $\begin{pmatrix} ax \\ x \end{pmatrix}$ je prosté zobrazení množiny $a\mathfrak{A}$ na $\mathfrak{A}$ a podobně $\begin{pmatrix} x \\ bx \end{pmatrix}$ je prosté zobrazení podgrupy $\mathfrak{A}$ na $b\mathfrak{A}$. Tedy je $\begin{pmatrix} x \\ bx \end{pmatrix}\begin{pmatrix} ax \\ x \end{pmatrix}$ prosté zobrazení množiny $a\mathfrak{A}$ na $b\mathfrak{A}$ a tím je naše tvrzení dokázáno.

Své úvahy rozšíříme nyní na případ, že vedle podgrupy $\mathfrak{A}$ máme v $\mathfrak{G}$ další podgrupu $\mathfrak{B}$.

12.2.6. *Když některé dvě levé třídy* $a\mathfrak{A}$, $b\mathfrak{B}$ *jsou incidentní, pak jejich průnik* $a\mathfrak{A} \cap b\mathfrak{B}$ *je levou třídou každého svého prvku vzhledem k podgrupě* $\mathfrak{A} \cap \mathfrak{B}$.

Vskutku, když některé dvě třídy $a\mathfrak{A}, b\mathfrak{B}$ mají společný prvek $c \in \mathfrak{G}$, pak podle vět **12.2.1** a **12.2.4** platí rovnosti $a\mathfrak{A} = c\mathfrak{A}$, $b\mathfrak{B} = c\mathfrak{B}$, takže $a\mathfrak{A} \cap b\mathfrak{B} = c\mathfrak{A} \cap c\mathfrak{B}$. Každý prvek $x \in c\mathfrak{A} \cap c\mathfrak{B}$ je součinem prvku c a jistého prvku $a' \in \mathfrak{A}$ a současně součinem prvku c a jistého prvku $b' \in \mathfrak{B}$, takže $x = ca' = cb'$; odtud vidíme, že jest $a' = b' \in \mathfrak{A} \cap \mathfrak{B}$, a tedy $x \in c(\mathfrak{A} \cap \mathfrak{B})$. Tím jsme zjistili, že platí vztah: $a\mathfrak{A} \cap b\mathfrak{B} \subset c(\mathfrak{A} \cap \mathfrak{B})$. Dále je každý prvek $x \in c(\mathfrak{A} \cap \mathfrak{B})$ součinem prvku c

a jistého prvku $c' \in \mathfrak{A} \cap \mathfrak{B}$, takže $x = cc' \in c\mathfrak{A} \cap c\mathfrak{B}$ a z toho soudíme na platnost vztahu $c(\mathfrak{A} \cap \mathfrak{B}) \subset a\mathfrak{A} \cap b\mathfrak{B}$. Tím je důkaz ukončen.

12.2.7. *Když $\mathfrak{A} \subset \mathfrak{B}$, pak z incidence levých tříd $a\mathfrak{A}, b\mathfrak{B}$ plyne $a\mathfrak{A} \subset \subset b\mathfrak{B}$.*

Vskutku, ze vztahu $\mathfrak{A} \subset \mathfrak{B}$ plyne $\mathfrak{A} \cap \mathfrak{B} = \mathfrak{A}$, podle **1.7.3**; z vět **12.2.6**, **12.2.4** soudíme, že platí rovnost: $a\mathfrak{A} \cap b\mathfrak{B} = a\mathfrak{A}$ a odtud vychází $a\mathfrak{A} \subset b\mathfrak{B}$ podle **1.7.3.**

Jak jsme se již zmínili, mají pravé třídy vzhledem k podgrupě $\mathfrak{A}$ vlastnosti analogické. Mezi levými a pravými třídami vzhledem k podgrupě $\mathfrak{A}$ je tento vztah:

12.2.8. *Levá třída $a\mathfrak{A}$ a pravá třída $\mathfrak{A}b$ jsou ekvivalentní množiny.*

Máme ukázat, že existuje prosté zobrazení množiny $a\mathfrak{A}$ na $\mathfrak{A}b$. Podle věty **12.2.5** existuje prosté zobrazení $\boldsymbol{a}$ množiny $a\mathfrak{A}$ na $\mathfrak{A}$ a podobně (protože vlastnosti pravých tříd jsou analogické) existuje prosté zobrazení $\boldsymbol{b}$ množiny $\mathfrak{A}b$ na $\mathfrak{A}$. Zobrazení složené $\boldsymbol{b}^{-1}\boldsymbol{a}$ je tedy prosté zobrazení množiny $a\mathfrak{A}$ na $\mathfrak{A}b$.

12.3. Levé (pravé) rozklady grupy.

12.3.1. *Definice.* Uvažujme nyní o systému všech podmnožin v $\mathfrak{G}$, které jsou levými třídami vzhledem k $\mathfrak{A}$ vždy některého prvku v $\mathfrak{G}$. Podle věty **12.2.1** je každý prvek $a \in \mathfrak{G}$ obsažen v levé třídě $a\mathfrak{A}$ a tato jest ovšem prvkem našeho systému; podle věty **12.2.4** jsou každé dva prvky našeho systému disjunktní. Systém, o nějž jde, je tedy rozklad grupy $\mathfrak{G}$. Tento rozklad grupy $\mathfrak{G}$ se nazývá *rozklad grupy $\mathfrak{G}$ v levé třídy vytvořený podgrupou $\mathfrak{A}$*, stručněji: *levý rozklad vytvořený podgrupou $\mathfrak{A}$*, a označujeme jej $\mathfrak{G}/_l\mathfrak{A}$.

Podobně se ukáže, že systém všech podmnožin v $\mathfrak{G}$, které jsou pravými třídami vzhledem k $\mathfrak{A}$ vždy některého prvku v $\mathfrak{G}$, je rozklad grupy $\mathfrak{G}$, a to t. zv. *rozklad grupy $\mathfrak{G}$ v pravé třídy vytvořený podgrupou $\mathfrak{A}$*, stručněji: *pravý rozklad vytvořený podgrupou $\mathfrak{A}$*, a označujeme jej symbolem $\mathfrak{G}/_p\mathfrak{A}$.

V dalších větách popíšeme vlastnosti levých rozkladů grupy. Vlastnosti pravých rozkladů jsou analogické, a proto je pro úsporu místa neuvádíme. Poslední věta **12.3.5** udává vztah mezi levými a pravými rozklady.

12.3.2. *Zákryt a zjemnění levého rozkladu.*

Nechť jsou v grupě $\mathfrak{G}$ dány dvě podgrupy $\mathfrak{A}$, $\mathfrak{B}$. Zkoumejme, kdy levý rozklad grupy $\mathfrak{G}$ vytvořený podgrupou $\mathfrak{A}$ ($\mathfrak{B}$) je zákrytem (zjemněním) levého rozkladu vytvořeného podgrupou $\mathfrak{B}$ ($\mathfrak{A}$), t. j. $\mathfrak{G}/_l\mathfrak{A} \geqq \mathfrak{G}/_l\mathfrak{B}$.

Když levý rozklad grupy $\mathfrak{G}$ vytvořený podgrupou $\mathfrak{A}$ je zákrytem levého rozkladu vytvořeného podgrupou $\mathfrak{B}$, pak zejména pole A podgrupy $\mathfrak{A}$ je součtem některých levých tříd vzhledem k podgrupě $\mathfrak{B}$ a mezi těmito levými třídami je pole B podgrupy $\mathfrak{B}$, neboť obě množiny A, B mají společný prvek $\underline{1}$; z toho soudíme, že podgrupa $\mathfrak{A}$ je nadgrupou na $\mathfrak{B}$, t. j. $\mathfrak{A} \supset \mathfrak{B}$. Když naopak podgrupa $\mathfrak{A}$ leží na $\mathfrak{B}$, soudíme, podle věty **12.2.7**, že každá levá třída vzhledem k $\mathfrak{A}$ je součtem všech levých tříd vzhledem k podgrupě $\mathfrak{B}$, které jsou s ní incidentní; vidíme, že pak levý rozklad grupy $\mathfrak{G}$ vytvořený podgrupou $\mathfrak{A}$ ($\mathfrak{B}$) je zákrytem (zjemněním) levého rozkladu vytvořeného podgrupou $\mathfrak{B}$ ($\mathfrak{A}$). Došli jsme k tomuto výsledku:

Levý rozklad grupy $\mathfrak{G}$ vytvořený podgrupou $\mathfrak{A}$ ($\mathfrak{B}$) je zákrytem (zjemněním) levého rozkladu vytvořeného podgrupou $\mathfrak{B}$ ($\mathfrak{A}$) tehdy a jen tehdy, když podgrupa $\mathfrak{A}$ je nadgrupou na $\mathfrak{B}$, t. j. $\mathfrak{A} \supset \mathfrak{B}$.

12.3.3. *Nejmenší společný zákryt dvou levých rozkladů.*

Nechť v grupě $\mathfrak{G}$ jsou dány dvě *vzájemně zaměnitelné* podgrupy $\mathfrak{A}$, $\mathfrak{B}$. V odst. **11.5.2** jsme viděli, že pak existuje součin $\mathfrak{A}\mathfrak{B}$ podgrup $\mathfrak{A}$, $\mathfrak{B}$ a je podgrupou v $\mathfrak{G}$.

Ukážeme, *že nejmenší společný zákryt levých rozkladů grupy $\mathfrak{G}$ vytvořených podgrupami $\mathfrak{A}$, $\mathfrak{B}$ je levý rozklad vytvořený podgrupou $\mathfrak{A}\mathfrak{B}$, t. j.* $[\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{B}] = \mathfrak{G}/_l\mathfrak{A}\mathfrak{B}$.

Vskutku, především vidíme, přihlížejíce ke vztahům $\mathfrak{A} \subset \mathfrak{A}\mathfrak{B}$, $\mathfrak{B} \subset \mathfrak{A}\mathfrak{B}$ a k větě **12.3.2**, že rozklad $\mathfrak{G}/_l\mathfrak{A}\mathfrak{B}$ je společným zákrytem rozkladů $\mathfrak{G}/_l\mathfrak{A}$, $\mathfrak{G}/_l\mathfrak{B}$. Máme ukázat, že se dvě třídy $c\mathfrak{A}$, $p\mathfrak{A} \in \mathfrak{G}/_l\mathfrak{A}$ dají spojit v rozkladu $\mathfrak{G}/_l\mathfrak{B}$ tehdy a jen tehdy, když leží v téže třídě rozkladu $\mathfrak{G}/_l\mathfrak{A}\mathfrak{B}$.

a) Když levé třídy $c\mathfrak{A}$, $p\mathfrak{A}$ leží v téže třídě rozkladu $\mathfrak{G}/_l\mathfrak{A}\mathfrak{B}$, jest $p = cba$, při čemž $b \in \mathfrak{B}$, $a \in \mathfrak{A}$ značí vhodné prvky. Vidíme, že obě třídy $c\mathfrak{A}$, $p\mathfrak{A}$ jsou incidentní s třídou $c\mathfrak{B} \in \mathfrak{G}/_l\mathfrak{B}$, a tím je zjištěno, že se dají spojit v rozkladu $\mathfrak{G}/_l\mathfrak{B}$.

b) Když existuje řetězec v $\{\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{B}\}$ od $c\mathfrak{A}$ do $p\mathfrak{A}$,

$$c_1\mathfrak{A}, \ldots, c_\alpha\mathfrak{A} \quad (c_1 = c,\ c_\alpha = p),$$

jsou každé dvě sousední třídy $c_\beta\mathfrak{A}, c_{\beta+1}\mathfrak{A}$ incidentní s jistou třídou $d_\beta\mathfrak{B}$, takže existují prvky $x_\beta \in c_\beta\mathfrak{A} \cap d_\beta\mathfrak{B}$, $y_\beta \in d_\beta\mathfrak{B} \cap c_{\beta+1}\mathfrak{A}$ $(\beta = 1, \ldots, \alpha - 1)$. Prvky $x_\gamma, y_{\gamma-1}$ $(\gamma = 1, \ldots, \alpha;\ y_0 = c_1,\ x_\alpha = c_\alpha)$ leží v téže třídě $c_\gamma\mathfrak{A}$ a podobně prvky x_β, y_β v téže třídě $d_\beta\mathfrak{B}$; z toho soudíme, že platí vzorce $x_\gamma = y_{\gamma-1}a_\gamma$, $y_\beta = x_\beta b_\beta$, v nichž $a_\gamma \in \mathfrak{A}$, $b_\beta \in \mathfrak{B}$ značí vhodné prvky. Z těchto vzorců vychází $c_\alpha = c_1a_1b_1 \ldots b_{\alpha-1}a_\alpha \in c_1\mathfrak{A}\mathfrak{B}$ a tím je zjištěno, že levé třídy $c\mathfrak{A}$, $p\mathfrak{A}$ leží v téže třídě $c\mathfrak{A}\mathfrak{B} \in \mathfrak{G}/_l\mathfrak{A}\mathfrak{B}$.

12.3.4. *Největší společné zjemnění dvou levých rozkladů.*

Nechť v grupě $\mathfrak{G}$ jsou dány dvě podgrupy $\mathfrak{A}$, $\mathfrak{B}$.

Ukážeme, že *největší společné zjemnění levých rozkladů grupy $\mathfrak{G}$ vytvořených podgrupami $\mathfrak{A}$, $\mathfrak{B}$ je levý rozklad vytvořený podgrupou $\mathfrak{A} \cap \mathfrak{B}$, t. j.* $(\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{B}) = \mathfrak{G}/_l(\mathfrak{A} \cap \mathfrak{B})$.

Vskutku, největší společné zjemnění rozkladů $\mathfrak{G}/_l\mathfrak{A}$, $\mathfrak{G}/_l\mathfrak{B}$ je systém všech neprázdných průniků vždy některé levé třídy $a\mathfrak{A}$ s některou levou třídou $b\mathfrak{B}$ (odst. 2.7.1). Každý neprázdný průnik $a\mathfrak{A} \cap b\mathfrak{B}$ je levou třídou každého prvku v něm ležícího vzhledem k podgrupě $\mathfrak{A} \cap \mathfrak{B}$; každá levá třída $c(\mathfrak{A} \cap \mathfrak{B})$ je průnikem levých tříd $c\mathfrak{A}$, $c\mathfrak{B}$ (odst. **12.2.6**). Tím je důkaz proveden.

12.3.5. *Doplňkové levé rozklady.*

Nechť v grupě $\mathfrak{G}$ jsou dány dvě *vzájemně zaměnitelné* podgrupy $\mathfrak{A}$, $\mathfrak{B}$.

Ukážeme, že *levé rozklady $\mathfrak{G}/_l\mathfrak{A}$, $\mathfrak{G}/_l\mathfrak{B}$ jimi vytvořené jsou doplňkové.*

Vskutku, podle věty **12.3.3** je nejmenší společný zákryt těchto rozkladů rozklad $\mathfrak{G}/_l\mathfrak{A}\mathfrak{B}$. Budiž $c\mathfrak{A}\mathfrak{B} \in \mathfrak{G}/_l\mathfrak{A}\mathfrak{B}$ libovolná třída. Každá třída rozkladu $\mathfrak{G}/_l\mathfrak{A}$ ležící v $c\mathfrak{A}\mathfrak{B}$ je $cb\mathfrak{A}$, kde $b \in \mathfrak{B}$ značí vhodný prvek; podobně každá třída rozkladu $\mathfrak{G}/_l\mathfrak{B}$ ležící v $c\mathfrak{A}\mathfrak{B}$ je $ca\mathfrak{B}$, kde $a \in \mathfrak{A}$ značí vhodný prvek. Máme ukázat, že každé dvě levé třídy $cb\mathfrak{A}$, $ca\mathfrak{B}$, ležící v $c\mathfrak{A}\mathfrak{B}$, jsou incidentní, t. j. že existují prvky $a_1 \in \mathfrak{A}$, $b_1 \in \mathfrak{B}$ vyhovující rovnosti $ba_1 = ab_1$. To je snadné: Protože podgrupy $\mathfrak{A}, \mathfrak{B}$ jsou vzájemně zaměnitelné, existují prvky $a_1 \in \mathfrak{A}$, $b_1 \in \mathfrak{B}$, které hoví vztahu $a^{-1}b = b_1a_1^{-1}$ a tyto prvky splňují hořejší rovnost. Tím je důkaz proveden.

12.3.6. *Vztah mezi levými a pravými rozklady.*

Budiž $\mathfrak{A}$ libovolná podgrupa v grupě $\mathfrak{G}$.

Snadno ukážeme, že *rozklady* $\mathfrak{G}/_l\mathfrak{A}$, $\mathfrak{G}/_p\mathfrak{A}$ *jsou ekvivalentní množiny*. Za tím účelem stačí ovšem zjistit, že existuje prosté zobrazení rozkladu $\mathfrak{G}/_l\mathfrak{A}$ na rozklad $\mathfrak{G}/_p\mathfrak{A}$. V každém prvku $\bar{a}$ rozkladu $\mathfrak{G}/_l\mathfrak{A}$ zvolme libovolný prvek $a \in \mathfrak{G}$, takže $\bar{a} = a\mathfrak{A}$, a přiřaďme k němu prvek $\mathfrak{A}a^{-1}$ rozkladu $\mathfrak{G}/_p\mathfrak{A}$. Tím definujeme jisté zobrazení rozkladu $\mathfrak{G}/_l\mathfrak{A}$ do rozkladu $\mathfrak{G}/_p\mathfrak{A}$ a (protože každý prvek v $\mathfrak{G}$ jest inversní vzhledem k některému prvku v $\mathfrak{G}$) dokonce *na* rozklad $\mathfrak{G}/_p\mathfrak{A}$ a stačí zjistiti, že toto zobrazení jest prosté. Jsou-li některé prvky $a\mathfrak{A}$, $b\mathfrak{A} \in \mathfrak{G}/_l\mathfrak{A}$ zobrazeny na týž prvek $\mathfrak{A}a^{-1} = \mathfrak{A}b^{-1}$, pak (podle věty analogické k větě **12.2.3**) platí vztah $a^{-1}b \in \mathfrak{A}$ a odtud podle věty **12.2.3** plyne, že prvky $a\mathfrak{A}$, $b\mathfrak{A}$ jsou identické, a tím jest dokázáno, že naše zobrazení je prosté.

12.4. Obal a průsek podgrupy s levým (pravým) rozkladem.

12.4.1. Nechť $\mathfrak{A} \subset \mathfrak{B}$, $\mathfrak{C}$ značí podgrupy v $\mathfrak{G}$ a předpokládejme, že podgrupy $\mathfrak{A}$, $\mathfrak{C}$ jsou vzájemně zaměnitelné. Za tohoto předpokladu jsou (podle **11.7.6**) vzájemně zaměnitelné i obě podgrupy $\mathfrak{C} \cap \mathfrak{B}$, $\mathfrak{A}$, takže existuje podgrupa $(\mathfrak{C} \cap \mathfrak{B})\mathfrak{A}$. Uvažujme nyní o *obalu* $\mathfrak{C} \sqsubset \mathfrak{B}/_l\mathfrak{A}$ *podgrupy* $\mathfrak{C}$ *v rozkladu* $\mathfrak{B}/_l\mathfrak{A}$ a o *průseku* $\mathfrak{B}/_l\mathfrak{A} \sqcap \mathfrak{C}$ *rozkladu* $\mathfrak{B}/_l\mathfrak{A}$ *s podgrupou* $\mathfrak{C}$. Ukážeme, že platí tyto rovnosti:

$$1.\quad \mathfrak{C} \sqsubset \mathfrak{B}/_l\mathfrak{A} = (\mathfrak{C} \cap \mathfrak{B})\mathfrak{A}/_l\mathfrak{A};$$

$$2.\quad \mathfrak{B}/_l\mathfrak{A} \sqcap \mathfrak{C} = (\mathfrak{C} \cap \mathfrak{B})/_l(\mathfrak{C} \cap \mathfrak{A}).$$

Abychom ukázali, že platí rovnost **1**, ukážeme, že každý prvek rozkladu na pravé straně je prvkem rozkladu na levé straně a naopak, každý prvek rozkladu na levé straně je prvkem rozkladu na pravé straně. Na pravé straně rovnosti **1** máme levý rozklad podgrupy $(\mathfrak{C} \cap \mathfrak{B})\mathfrak{A}$ vytvořený podgrupou $\mathfrak{A}$. Každý prvek $\bar{a}$ tohoto rozkladu je tedy $x\mathfrak{A}$, kde $x \in (\mathfrak{C} \cap \mathfrak{B})\mathfrak{A}$, takže x je součin ba jistého prvku $b \in \mathfrak{C} \cap \mathfrak{B}$ s jistým prvkem $a \in \mathfrak{A}$. Odtud plyne $\bar{a} = (ba)\mathfrak{A} = b(a\mathfrak{A}) = b\mathfrak{A}$, neboť podle věty **12.2.2** máme $a\mathfrak{A} = A$. Protože $b \in \mathfrak{B}$, $\mathfrak{A} \subset \mathfrak{B}$, je $b\mathfrak{A} \in \mathfrak{B}/_l\mathfrak{A}$, a protože $b \in \mathfrak{C}$, je $b\mathfrak{A}$ incidentní s $\mathfrak{C}$. Vychází tedy vztah $\bar{a} \in \mathfrak{C} \sqsubset \mathfrak{B}/_l\mathfrak{A}$ a tím je provedena první část našeho důkazu. Nechť nyní $\bar{a}$ značí libovolný prvek v $\mathfrak{C} \sqsubset \mathfrak{B}/_l\mathfrak{A}$, takže $\bar{a} = b\mathfrak{A}$, kde b značí jistý prvek v $\mathfrak{B}$, a dále $b\mathfrak{A}$ jest incidentní s $\mathfrak{C}$, t. j. existuje prvek $c \in \mathfrak{C}$ takový, že $c \in b\mathfrak{A}$. Ze vztahu $c \in b\mathfrak{A}$ plyne podle vět **12.2.1** a **12.2.4** rovnost $\bar{a} = c\mathfrak{A}$ a odtud plyne dále $c \in \mathfrak{B}$, neboť $\bar{a} \subset \mathfrak{B}$. Máme tedy vztah $c \in \mathfrak{C} \cap \mathfrak{B}$ a tedy také $c = c\underline{1} \in (\mathfrak{C} \cap \mathfrak{B})\mathfrak{A}$. Odtud a ze vztahu $\mathfrak{A} \subset (\mathfrak{C} \cap \mathfrak{B})\mathfrak{A}$ vychází $\bar{a} \in (\mathfrak{C} \cap \mathfrak{B})\mathfrak{A}/_l\mathfrak{A}$ a tím je náš důkaz ukončen.

Při důkazu rovnosti 2 budeme postupovati podobně. Každý prvek $\bar{a}$ na pravé straně rovnosti 2 jest $a(\mathfrak{C} \cap \mathfrak{A}) = a\mathfrak{C} \cap a\mathfrak{A}$, kde $a \in \mathfrak{C} \cap \mathfrak{B}$. Ze vztahu $a \in \mathfrak{C}$ plyne rovnost $a\mathfrak{C} = C$, kde C je pole podgrupy $\mathfrak{C}$, a protože $a \in \mathfrak{B}$, $\mathfrak{A} \subset \mathfrak{B}$, máme $a\mathfrak{A} \in \mathfrak{B}/_l\mathfrak{A}$. Odtud vychází $\bar{a} = \mathfrak{C} \cap a\mathfrak{A} \in \mathfrak{B}/_l\mathfrak{A} \sqcap \mathfrak{C}$ a tím je provedena první část důkazu. Nechť nyní $\bar{a}$ značí libovolný prvek rozkladu $\mathfrak{B}/_l\mathfrak{A} \sqcap \mathfrak{C}$, takže $\bar{a} = \mathfrak{C} \cap b\mathfrak{A}$, kde b je jistý prvek v $\mathfrak{B}$. Podle definice průseku rozkladu s množinou, není $\bar{a}$ prázdná množina, a tedy existuje prvek $a \in \mathfrak{C} \cap b\mathfrak{A}$. Protože $a \in \mathfrak{C}$, platí rovnost $C = a\mathfrak{C}$, a protože $a \in b\mathfrak{A}$, je $b\mathfrak{A} = a\mathfrak{A}$ a tedy máme $\bar{a} = a\mathfrak{C} \cap a\mathfrak{A} = a(\mathfrak{C} \cap \mathfrak{A})$. Uvážíme-li, že ze vztahů $b \in \mathfrak{B}$, $\mathfrak{A} \subset \mathfrak{B}$ plyne $b\mathfrak{A} \subset \mathfrak{B}$, vidíme, že $a \in \mathfrak{C} \cap \mathfrak{B}$, a vychází $\bar{a} \in (\mathfrak{C} \cap \mathfrak{B})/_l(\mathfrak{C} \cap \mathfrak{A})$ — a tím je důkaz ukončen.

12.4.2. Všimněme si zvláštního případu, že podgrupa $\mathfrak{B}$ splývá s grupou $\mathfrak{G}$. Pak $\mathfrak{C} \cap \mathfrak{B} = \mathfrak{C}$ a z hořejších vzorců plynou tyto rovnosti:

$$\mathfrak{C} \sqsubset \mathfrak{G}/_l\mathfrak{A} = \mathfrak{C}\mathfrak{A}/_l\mathfrak{A}, \qquad \mathfrak{G}/_l\mathfrak{A} \sqcap \mathfrak{C} = \mathfrak{C}/_l(\mathfrak{C} \cap \mathfrak{A}).$$

12.4.3. *Poznámka.* Podobnými úsudky se dá ukázat, že pro *pravé rozklady* platí analogické vzorce:

$$1.\ \mathfrak{C} \sqsubset \mathfrak{B}/_p\mathfrak{A} = \mathfrak{A}(\mathfrak{C} \cap \mathfrak{B})/_p\mathfrak{A},$$
$$2.\ \mathfrak{B}/_p\mathfrak{A} \sqcap \mathfrak{C} = (\mathfrak{C} \cap \mathfrak{B})/_p(\mathfrak{C} \cap \mathfrak{A}),$$

a jejich zvláštní případy:

$$\mathfrak{C} \sqsubset \mathfrak{G}/_p\mathfrak{A} = \mathfrak{A}\mathfrak{C}/_p\mathfrak{A}, \qquad \mathfrak{G}/_p\mathfrak{A} \sqcap \mathfrak{C} = \mathfrak{C}/_p(\mathfrak{C} \cap \mathfrak{A}).$$

Zopakujme si, že $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ značí podgrupy v grupě $\mathfrak{G}$ a že podgrupa $\mathfrak{A}$ leží v $\mathfrak{B}$ a je zaměnitelná s $\mathfrak{C}$.

12.5. Lagrangeova věta.

12.5.1. Všimněme si nyní důsledku existence levého nebo pravého rozkladu vytvořeného podgrupou $\mathfrak{A}$ v případě, že grupa $\mathfrak{G}$ je konečná.

Označme písmenem N řád grupy $\mathfrak{G}$, takže N je počet prvků v $\mathfrak{G}$, a písmenem n řád podgrupy $\mathfrak{A}$, takže n je počet prvků v $\mathfrak{A}$. Jedním prvkem levého rozkladu vytvořeného podgrupou $\mathfrak{A}$ je pole A podgrupy $\mathfrak{A}$. Tento prvek levého rozkladu se tedy skládá z n prvků grupy $\mathfrak{G}$ a tedy (podle věty 12.2.5) každý prvek levého rozkladu vytvořeného podgrupou $\mathfrak{A}$ se skládá z n prvků grupy $\mathfrak{G}$. Odtud plyne rovnost $N = qn$, kde q značí počet prvků levého rozkladu vytvořeného podgrupou $\mathfrak{A}$. Tímto způsobem jsme došli k důležitému výsledku:

Řád každé podgrupy $\mathfrak{A}$ v libovolné konečné grupě $\mathfrak{G}$ je dělitelem řádu grupy $\mathfrak{G}$.

Tento výsledek bývá v literatuře označován jako *Lagrangeova věta* a v theorii konečných grup je považován za jeden z nejdůležitějších. Číslo q, t. j. tedy počet prvků rozkladu $\mathfrak{G}/_l\mathfrak{A}$ a současně i podíl řádu grupy $\mathfrak{G}$ a řádu podgrupy $\mathfrak{A}$, se nazývá *index podgrupy $\mathfrak{A}$ v grupě $\mathfrak{G}$*. Protože rozklady $\mathfrak{G}/_l\mathfrak{A}$, $\mathfrak{G}/_p\mathfrak{A}$ jsou ekvivalentní množiny, udává index podgrupy $\mathfrak{A}$ v grupě $\mathfrak{G}$ současně počet prvků rozkladu $\mathfrak{G}/_p\mathfrak{A}$. Důsledkem Lagrangeovy věty je na př., že *libovolná konečná grupa, jejíž řád je nějaké prvočíslo, neobsahuje žádnou vlastní podgrupu, která by byla různá od nejmenší podgrupy.*

Všimněme si, že tvrzení Lagrangeovy věty platí, i když grupa $\mathfrak{G}$ je nekonečná ($N = 0$).

12.5.2. *Příklad.* Uvažujme o grupě $\mathfrak{S}_3$ a její prvky označme písmeny $\underline{1}$, $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{f}$, podobně jako v odst. 5.4.2. Z multiplikační tabulky grupy $\mathfrak{S}_3$, uvedené v odst. 5.4.2, vidíme, že prvky 1, $\mathbf{f}$ tvoří podgrupu v $\mathfrak{S}_3$; tuto podgrupu označíme $\mathfrak{A}$.

Levé třídy jednotlivých prvků v $\mathfrak{S}_3$ vzhledem k $\mathfrak{A}$ jsou:

$$\underline{1}\mathfrak{A} = \mathbf{f}\mathfrak{A} = \{\underline{1}, \mathbf{f}\}; \ \mathbf{a}\mathfrak{A} = \mathbf{c}\mathfrak{A} = \{\mathbf{a}, \mathbf{c}\}; \ \mathbf{b}\mathfrak{A} = \mathbf{d}\mathfrak{A} = \{\mathbf{b}, \mathbf{d}\}.$$

Pravé třídy jsou:

$$\mathfrak{A}\underline{1} = \mathfrak{A}\mathbf{f} = \{\underline{1}, \mathbf{f}\}; \ \mathfrak{A}\mathbf{a} = \mathfrak{A}\mathbf{d} = \{\mathbf{a}, \mathbf{d}\}; \ \mathfrak{A}\mathbf{b} = \mathfrak{A}\mathbf{c} = \{\mathbf{b}, \mathbf{c}\}.$$

Levý rozklad grupy $\mathfrak{S}_3$ vytvořený podgrupou $\mathfrak{A}$ se tedy skládá z prvků: $\{\underline{1}, \mathbf{f}\}$, $\{\mathbf{a}, \mathbf{c}\}$, $\{\mathbf{b}, \mathbf{d}\}$ a pravý rozklad se skládá z prvků: $\{\underline{1}, \mathbf{f}\}$, $\{\mathbf{a}, \mathbf{d}\}$, $\{\mathbf{b}, \mathbf{c}\}$. Všimněme si, že tyto dva rozklady jsou různé. Řád grupy $\mathfrak{S}_3$ je 6, řád podgrupy $\mathfrak{A}$ je 2, index podgrupy $\mathfrak{A}$ v $\mathfrak{S}_3$ je $6 : 2 = 3 =$ počet prvků levého a současně i pravého rozkladu grupy $\mathfrak{S}_3$ vytvořeného podgrupou $\mathfrak{A}$.

12.6. Cvičení.

12.6.1. Když grupa $\mathfrak{G}$ jest abelovská, pak levá třída libovolného prvku $a \in \mathfrak{G}$ vzhledem k nějaké podgrupě $\mathfrak{A} \subset \mathfrak{G}$ je současně pravou třídou prvku a vzhledem k $\mathfrak{A}$; odtud plyne rovnost levého a pravého rozkladu grupy $\mathfrak{G}$ vytvořeného podgrupou $\mathfrak{A}$.

12.6.2. Levý (a současně pravý) rozklad grupy $\mathfrak{Z}$, vytvořený podgrupou skládající se ze všech násobků libovolného přirozeného čísla n, je rozklad $\overline{Z}_n$, o němž jsme uvažovali v odst. 8.3.

12.6.3. Řád každé grupy, jejíž prvky jsou permutace nějaké konečné množiny řádu n, je dělitelem čísla $n!$.

12.6.4. Počet prvků v libovolné konečné abelovské grupě řádu N, které jsou samy k sobě inversní, je dělitelem čísla N.

12.6.5. Nechť $\mathfrak{A}$ značí libovolnou podgrupu a B libovolnou podmnožinu v nějaké grupě $\mathfrak{G}$. Ukažte, že: 1. součet všech levých (pravych) tříd vzhledem k $\mathfrak{A}$, které jsou incidentní s B, je $B\mathfrak{A}$ ($\mathfrak{A}B$); 2. součet všech levých tříd vzhledem k $\mathfrak{A}$, které jsou incidentní s některou pravou třídou $\mathfrak{A}a$, je týž, jako součet všech pravých tříd vzhledem k $\mathfrak{A}$ incidentních s levou třídou $a\mathfrak{A}$.

13. O INVARIANTNÍCH PODGRUPÁCH.

13.1. Definice.

Když nějaká podgrupa $\mathfrak{A}$ v grupě $\mathfrak{G}$ se vyznačuje vlastností, že levá a pravá třída každého prvku $a \in \mathfrak{G}$ vzhledem k podgrupě $\mathfrak{A}$ splývají, když tedy pro každý prvek $a \in \mathfrak{G}$ platí rovnost $a\mathfrak{A} = \mathfrak{A}a$, *pak pravíme, že $\mathfrak{A}$ jest invariantní nebo normální podgrupa v grupě $\mathfrak{G}$.* V tomto případě ovšem *levý a pravý rozklad grupy $\mathfrak{G}$ vytvořený podgrupou $\mathfrak{A}$ splývají v jeden t. zv. rozklad grupy $\mathfrak{G}$ vytvořený podgrupou $\mathfrak{A}$.*

13.2. Vlastnosti invariantních podgrup.

13.2.1. Všimněme si nyní vlastností invariantních podgrup. V každé grupě $\mathfrak{G}$ existují alespoň dvě invariantní podgrupy, a to nejmenší podgrupa $\mathfrak{E}$, skládající se z jediného prvku 1, a největší podgrupa $\mathfrak{G}$. V grupách mohou existovati podgrupy, které nejsou invariantní; na př. podgrupa $\mathfrak{A}$ v grupě $\mathfrak{S}_3$, skládající se z obou permutací $\underline{1}$, $\boldsymbol{f}$ (označení