22. Důsledky vlastností rozkladů vytvořených podgrupami

22.1. Lagrangeova věta

Budiž $\mathfrak{A} \subset \mathfrak{G}$ libovolná podgrupa v $\mathfrak{G}$. Všimněme si důsledků plynoucích z existence a vlastností levého (popř. pravého) rozkladu grupy $\mathfrak{G}$ vzhledem k podgrupě $\mathfrak{A}$.

Předpokládejme, 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 proto podle (**20.2.**5) se každý prvek levého rozkladu vytvořeného podgrupou $\mathfrak{A}$ 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 se v literatuře nazývá *Lagrangeova věta* a v teorii konečných grup je považován za jeden z nejdůležitějších. Číslo q, tj. 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 např., 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 ($N = 0$).

Příklad. Uvažujme o grupě $\mathfrak{S}_3$ a její prvky označme písmeny $\underline{1}, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{f}$, podobně jako v **11.4**. Z multiplikační tabulky grupy $\mathfrak{S}_3$, uvedené v odst. **11.4** vidíme, že prvky $\underline{1}, \boldsymbol{f}$ tvoří podgrupu v $\mathfrak{S}_3$. Tuto podgrupu označíme $\mathfrak{A}$.

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

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

Pravé třídy jsou:

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

Levý rozklad grupy $\mathfrak{S}_3$ vytvořený podgrupou $\mathfrak{A}$ se tedy skládá z prvků $\{\underline{1}, \boldsymbol{f}\}$, $\{\boldsymbol{a}, \boldsymbol{c}\}$, $\{\boldsymbol{b}, \boldsymbol{d}\}$, zatímco pravý rozklad má prvky $\{\underline{1}, \boldsymbol{f}\}$, $\{\boldsymbol{a}, \boldsymbol{d}\}$, $\{\boldsymbol{b}, \boldsymbol{c}\}$. 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 $\mathfrak{A}$.

22.2. Vztahy mezi vzájemně zaměnitelnými podgrupami

Výsledek odvozený v odst. **21.6** a vlastnosti doplňkových rozkladů (**5**) vedou k řadě důsledků pro vzájemně zaměnitelné podgrupy. Spokojíme se jenom s několika výsledky a přenecháváme čtenáři v tomto směru další iniciativu. Je účelné podotknout, že vzorce, které přitom obdržíme, dají se většinou jednoduše ověřit přímo. Naše metoda se však vyznačuje nejen tím, že tyto vzorce odkrývá, nýbrž i dovoluje hlubší pohled na jejich strukturu.

1) *Buďte $\mathfrak{A} \supset \mathfrak{B}$, $\mathfrak{D}$ libovolné podgrupy v $\mathfrak{G}$ a předpokládejme, že podgrupy $\mathfrak{B}, \mathfrak{D}$ jsou vzájemně zaměnitelné. Pak také podgrupy $\mathfrak{B}, \mathfrak{A} \cap \mathfrak{D}$ jsou vzájemně zaměnitelné a platí vzorec*

$$\mathfrak{A} \cap \mathfrak{D}\mathfrak{B} = (\mathfrak{A} \cap \mathfrak{D})\,\mathfrak{B}\,. \tag{1}$$

Vskutku, podle **21.6** jsou rozklady $\mathfrak{G}/_l\mathfrak{B}$, $\mathfrak{G}/_l\mathfrak{D}$ doplňkové. Z předpokladu $\mathfrak{A} \supset \mathfrak{B}$ máme $\mathfrak{G}/_l\mathfrak{A} \geqq \mathfrak{G}/_l\mathfrak{B}$ (**21.3**). Podle **5.3** je rozklad $\mathfrak{G}/_l\mathfrak{B}$ doplňkový k rozkladu $(\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{D})$ a podle **21.4** máme: $(\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{D}) = \mathfrak{G}/_l(\mathfrak{A} \cap \mathfrak{D})$. Vidíme, že rozklady $\mathfrak{G}/_l\mathfrak{B}$, $\mathfrak{G}/_l(\mathfrak{A} \cap \mathfrak{D})$ jsou doplňkové; z **21.6** soudíme, že podgrupy $\mathfrak{B}$, $\mathfrak{A} \cap \mathfrak{D}$ jsou vzájemně zaměnitelné.

Podle **5.4** je rozklad $\mathfrak{G}/_l\mathfrak{D}$ modulární vzhledem k rozkladům $\mathfrak{G}/_l\mathfrak{A}$, $\mathfrak{G}/_l\mathfrak{B}$, takže

$$(\mathfrak{G}/_l\mathfrak{A}, [\mathfrak{G}/_l\mathfrak{B}, \mathfrak{G}/_l\mathfrak{D}]) = [\mathfrak{G}/_l\mathfrak{B}, (\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{D})]\,.$$

Odtud vzhledem k **21.4** a **21.5** plyne

$$(\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{D}\mathfrak{B}) = [\mathfrak{G}/_l\mathfrak{B}, \mathfrak{G}/_l(\mathfrak{A} \cap \mathfrak{D})]\,,$$

a tedy též

$$\mathfrak{G}/_l(\mathfrak{A} \cap \mathfrak{D}\mathfrak{B}) = \mathfrak{G}/_l(\mathfrak{A} \cap \mathfrak{D})\,\mathfrak{B}\,.$$

Vidíme, že levá třída tohoto rozkladu, obsahující jednotku $\underline{1}$ grupy $\mathfrak{G}$, je polem podgrupy $\mathfrak{A} \cap \mathfrak{D})\,\mathfrak{B}$ a současně polem podgrupy $(\mathfrak{A} \cap \mathfrak{D})\,\mathfrak{B}$. Odtud vychází hořejší vzorec.

2) *Buďte $\mathfrak{A} \supset \mathfrak{B}$, $\mathfrak{C} \supset \mathfrak{D}$ libovolné podgrupy v $\mathfrak{G}$ a předpokládejme, že podgrupy $\mathfrak{B}, \mathfrak{D}$ jsou vzájemně zaměnitelné. Pak také podgrupy $\mathfrak{B}, \mathfrak{A} \cap \mathfrak{D}$ jsou vzájemně zaměnitelné a též podgrupy $\mathfrak{D}, \mathfrak{C} \cap \mathfrak{B}$. Současně i podgrupy $\mathfrak{A} \cap \mathfrak{D}, \mathfrak{C} \cap \mathfrak{B}$ mají touž vlastnost a platí vzorec*

$$\mathfrak{A} \cap \mathfrak{C} \cap \mathfrak{D}\mathfrak{B} = (\mathfrak{A} \cap \mathfrak{D})\,(\mathfrak{C} \cap \mathfrak{B})\,. \tag{2}$$

Vskutku, první část tohoto tvrzení plyne bezprostředně z hořejší věty. Dále platí (podle **5.6.1**)

(3) $$((\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{C}), [\mathfrak{G}/_l\mathfrak{B}, \mathfrak{G}/_l\mathfrak{D}]) = [(\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{D}), (\mathfrak{G}/_l\mathfrak{C}, \mathfrak{G}/_l\mathfrak{B})]$$

a rozklady $(\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{D})$, $(\mathfrak{G}/_l\mathfrak{C}, \mathfrak{G}/_l\mathfrak{B})$, tj. $\mathfrak{G}/_l(\mathfrak{A} \cap \mathfrak{D})$, $\mathfrak{G}/_l(\mathfrak{C} \cap \mathfrak{B})$ jsou doplňkové. Z toho soudíme (**21.6**), že podgrupy $\mathfrak{A} \cap \mathfrak{D}$, $\mathfrak{C} \cap \mathfrak{B}$ jsou vzájemně zaměnitelné, takže ze vzorce (3) vychází (2).

3) *V situaci popsané ve větě* 2 *platí též tyto vzorce*:

(4) $$(\mathfrak{A} \cap \mathfrak{D})\,\mathfrak{B} \cap \mathfrak{C} = (\mathfrak{C} \cap \mathfrak{B})\,\mathfrak{D} \cap \mathfrak{A} = (\mathfrak{A} \cap \mathfrak{D})\,(\mathfrak{C} \cap \mathfrak{B}).$$

Důkaz. Víme, že rozklady $\mathfrak{G}/_l\mathfrak{B}$, $\mathfrak{G}/_l\mathfrak{D}$ jsou doplňkové; mimoto platí vztahy: $\mathfrak{G}/_l\mathfrak{A} \geqq \mathfrak{G}/_l\mathfrak{B}$, $\mathfrak{G}/_l\mathfrak{C} \geqq \mathfrak{G}/_l\mathfrak{D}$. Připomeňme, že pole podgrup $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{D}$ jsou prvky příslušných levých rozkladů obsahující jednotku $\underline{1}$ grupy $\mathfrak{G}$.

Použijeme nyní výsledku z odst. **5.5**, podle něhož jsou rozklady

$$\mathfrak{A}/_l\mathfrak{B} = \mathfrak{A} \sqsubset \mathfrak{G}/_l\mathfrak{B}\ (= \mathfrak{G}/_l\mathfrak{B} \sqcap \mathfrak{A}), \quad \mathfrak{C}/_l\mathfrak{D} = \mathfrak{C} \sqsubset \mathfrak{G}/_l\mathfrak{D}\,(= \mathfrak{G}/_l\mathfrak{D} \sqcap \mathfrak{C})$$

adjungované vzhledem k $\mathfrak{B}, \mathfrak{D}$. Platí tedy rovnost:

(5) $$\mathbf{s}(\mathfrak{D} \sqsubset \mathfrak{A}/_l\mathfrak{B} \sqcap \mathfrak{C}) = \mathbf{s}(\mathfrak{B} \sqsubset \mathfrak{C}/_l\mathfrak{D} \sqcap \mathfrak{A}).$$

Podle **2.6.5**a) máme vztahy

$$\mathfrak{D} \sqsubset \mathfrak{A}/_l\mathfrak{B} \sqcap \mathfrak{C} = (\mathfrak{D} \sqsubset \mathfrak{A}/_l\mathfrak{B}) \sqcap \mathfrak{C} = \mathfrak{D} \sqsubset (\mathfrak{A}/_l\mathfrak{B} \sqcap \mathfrak{C}),$$
$$\mathfrak{B} \sqsubset \mathfrak{C}/_l\mathfrak{D} \sqcap \mathfrak{A} = (\mathfrak{B} \sqsubset \mathfrak{C}/_l\mathfrak{D}) \sqcap \mathfrak{A} = \mathfrak{B} \sqsubset (\mathfrak{C}/_l\mathfrak{D} \sqcap \mathfrak{A}),$$

a poznatky z odst. **21.2.1** vedou k vzorcům

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

Tak docházíme k vztahům

$$\mathbf{s}(\mathfrak{D} \sqsubset \mathfrak{A}/_l\mathfrak{B} \sqcap \mathfrak{C}) = (\mathfrak{A} \cap \mathfrak{D})\,\mathfrak{B} \cap \mathfrak{C} = (\mathfrak{A} \cap \mathfrak{D})(\mathfrak{C} \cap \mathfrak{B}),$$
$$\mathbf{s}(\mathfrak{B} \sqsubset \mathfrak{C}/_l\mathfrak{D} \sqcap \mathfrak{A}) = (\mathfrak{C} \cap \mathfrak{B})\,\mathfrak{D} \cap \mathfrak{A} = (\mathfrak{C} \cap \mathfrak{B})(\mathfrak{A} \cap \mathfrak{D}),$$

které spolu s (5) dávají vzorce (4).

22.3. Modulární svazy podgrup a rozkladů vytvořených podgrupami

Vezměme v úvahu libovolný neprázdný systém O podgrup v grupě $\mathfrak{G}$. Předpokládáme, že každé dvě podgrupy obsažené v systému O jsou vzájemně zaměnitelné a že tento systém je vzhledem k průnikům a součinům dvojic podgrup uzavřený. Posledně uvedený postulát o uzavřenosti systému O má tento smysl: Pro každé dvě podgrupy $\mathfrak{A}, \mathfrak{B} \in O$ patří jejich průnik i součin rovněž do systému O, tedy $\mathfrak{A} \cap \mathfrak{B}$, $\mathfrak{A}\mathfrak{B} \in O$.

Ke každé dvojčlenné posloupnosti podgrup $\mathfrak{A}, \mathfrak{B} \in O$ přiřaďme jednou průnik $\mathfrak{A} \cap \mathfrak{B}$ a podruhé součin $\mathfrak{A}\mathfrak{B}$ podgrup $\mathfrak{A}, \mathfrak{B}$. Tím máme definována dvě násobení v systému O a tedy dvojici soumístných grupoidů na poli O. Každý z obou grupoidů je abelovský (**1.6**), asociativní (**1.10**.4; **18.1**.1) a skládá se vesměs z prvků idempotentních (**1.10**.1; **15.6**.4). Mimoto vidíme, že násobení v obou grupoidech souvisí podle vzorců: $\mathfrak{A}(\mathfrak{A} \cap \mathfrak{B}) = \mathfrak{A}$, $\mathfrak{A} \cap \mathfrak{A}\mathfrak{B} = \mathfrak{A}$. Tím je zjištěno, že hořejší dvojice grupoidů je svazem, např. Ω.

Zvolme za horní (dolní) násobení ve svazu Ω např. ono, v němž je ke každé dvojčlenné posloupnosti podgrup $\mathfrak{A}, \mathfrak{B} \in \Omega$ přiřazen jejich součin $\mathfrak{A}\mathfrak{B}$ (průnik $\mathfrak{A} \cap \mathfrak{B}$), takže $\mathfrak{A} \cup \mathfrak{B} = \mathfrak{A}\mathfrak{B}$, $\mathfrak{A} \cap \mathfrak{B} = \mathfrak{A} \cap \mathfrak{B}$. V této situaci obdržíme horní (dolní) částečné uspořádání $\boldsymbol{h}$ (resp. $\boldsymbol{d}$) svazu Ω, když ke každé podgrupě $\mathfrak{A} \in \Omega$ přiřadíme všechny její nadgrupy (podgrupy) $\mathfrak{B} \in \Omega$. Ze vzorce **22.2**.1 vidíme, že každá trojčlenná posloupnost podgrup $\mathfrak{A}, \mathfrak{B}, \mathfrak{C} \in \Omega$, pro niž platí $\mathfrak{A} \leqq \mathfrak{C}$ $(\boldsymbol{h})$, splňuje horní modulární vztah. Tím je zjištěno, že svaz Ω je modulární.

Dále přiřaďme ke každé podgrupě $\mathfrak{A} \in \Omega$ levý rozklad $\mathfrak{G}/_l\mathfrak{A}$ grupy $\mathfrak{G}$ vzhledem k $\mathfrak{A}$ a označme příslušný systém levých rozkladů grupy $\mathfrak{G}$ symbolem O^*. Se zřetelem na **21.4**; **21.5** vidíme, že systém O^* je uzavřený vzhledem k operacím ( ), [ ], takže s každými dvěma levými rozklady $\mathfrak{G}/_l\mathfrak{A}$, $\mathfrak{G}/_l\mathfrak{B} \in O^*$ patří do systému též jejich největší společné zjemnění a nejmenší společný zákryt: $(\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{B})$, $[\mathfrak{G}/_l\mathfrak{A}, \mathfrak{G}/_l\mathfrak{B}] \in O^*$. V systému O^* můžeme definovat dvě násobení tím, že ke každé dvojčlenné posloupnosti levých rozkladů $\mathfrak{G}/_l\mathfrak{A}$, $\mathfrak{G}/_l\mathfrak{B} \in O^*$ přiřadíme jednou jejich největší společné zjemnění a podruhé nejmenší společný zákryt. Tímto způsobem obdržíme na poli O^* dvojici soumístných grupoidů Ω^* a opět se dá zjistit, že Ω^* představuje svaz.

Funkce $\boldsymbol{i}$, která ke každé podgrupě $\mathfrak{A} \in \Omega$ přiřazuje levý rozklad $\mathfrak{G}/_l\mathfrak{A} \in \Omega^*$, představuje zřejmě prosté zobrazení svazu Ω na svaz Ω^* a vyznačuje se tím, že pro každé podgrupy $\mathfrak{A}, \mathfrak{B} \in \Omega$ platí vztahy

$$\boldsymbol{i}(\mathfrak{A} \cap \mathfrak{B}) = \mathfrak{G}/_l(\mathfrak{A} \cap \mathfrak{B}), \quad \boldsymbol{i}\mathfrak{A}\mathfrak{B} = \mathfrak{G}/_l\mathfrak{A}\mathfrak{B},$$

tj.

$$\boldsymbol{i}(\mathfrak{A} \cap \mathfrak{B}) = \boldsymbol{i}\mathfrak{A} \cap \boldsymbol{i}\mathfrak{B}, \quad \boldsymbol{i}(\mathfrak{A} \cup \mathfrak{B}) = \boldsymbol{i}\mathfrak{A} \cup \boldsymbol{i}\mathfrak{B}.$$

Zobrazení $\boldsymbol{i}$ je tedy izomorfismus svazu Ω na svaz Ω^*. Protože svaz Ω je modulární, platí totéž o svazu Ω^* (**18.7**.14).

Došli jsme k tomuto výsledku:

Každý neprázdný systém podgrup v libovolné grupě $\mathfrak{G}$, jehož každé dva prvky jsou vzájemně zaměnitelné a systém sám je vzhledem k průnikům a součinům vždy dvou podgrup uzavřený, tvoří s násobeními, definovanými tvořením průniků a součinů, modulární svaz. Systém levých (pravých) rozkladů grupy $\mathfrak{G}$, vytvořených jednotlivými prvky tohoto svazu, je vzhledem k operacím ( ), [ ] uzavřený a tvoří s násobeními, definovanými těmito operacemi, rovněž modulární svaz, který je s oním izomorfní.

22.4. Cvičení

1. Řád každé grupy, která se skládá z permutací nějaké konečné množiny řádu n, je dělitelem čísla $n!$.

2. V každé konečné abelovské grupě řádu N je počet prvků, které jsou samy k sobě inverzní, dělitelem čísla N.