Úvod do theorie grup [2. rozšířené vydání]

10. O význačných druzích grupoidů

In: Otakar Borůvka (author): Úvod do theorie grup [2. rozšířené vydání]. (Czech). Praha: Přírodovědecké vydavatelství, 1952. pp. 89--101.

Persistent URL: http://dml.cz/dmlcz/401416

10. O VÝZNAČNÝCH DRUZÍCH GRUPOIDŮ.

10.1. Úvodem.

Ačkoli některé význačné druhy grupoidů, o kterých pojednáme, jsou charakterisovány zvláštními vlastnostmi násobení a výklad o nich se přimyká k odst. 5, přistoupíme k němu teprve nyní, abychom zdůraznili, že předcházející úvahy platí pro všechny grupoidy bez ohledu na nějaké jejich zvláštní vlastnosti. Pro naše další úvahy jsou důležité zejména grupoidy asociativní, dále t. zv. grupoidy s jednoznačným dělením a grupoidy s jednotkou.

10.2. Asociativní grupoidy neboli pologrupy.

10.2.1. *Definice.* Pojem asociativního grupoidu $\mathfrak{G}$ jsme již vymezili v odst. 6.7.2, a to vlastností, že *každá uspořádaná trojice prvků v $\mathfrak{G}$ má jenom jeden součin*, t. j. že pro každé tři prvky $a_1, a_2, a_3 \in \mathfrak{G}$ platí rovnost $a_1(a_2a_3) = (a_1a_2)a_3$. *Asociativní grupoidy se nazývají také pologrupy.*

10.2.2. *Základní věta o pologrupách.* Nyní ukážeme, že *každý asociativní grupoid $\mathfrak{G}$ se vyznačuje tím, že každá uspořádaná skupina několika prvků v $\mathfrak{G}$ má jenom jeden součin*, t. j. pro $a_1, \ldots, a_n \in \mathfrak{G}$ $(n \geqq 2)$ značí symbol $a_1 \ldots a_n$ právě jeden prvek v $\mathfrak{G}$.

Za tím účelem uvažujme o libovolném asociativním grupoidu $\mathfrak{G}$. K důkazu použijeme methody úplné indukce. Naše tvrzení je správné, když $n = 2$, neboť v tom případě plyne bezprostředně z definice násobení v $\mathfrak{G}$. Zbývá tedy ukázat, že platí-li tvrzení o každé uspořádané skupině nejvýše $n - 1$ prvků v $\mathfrak{G}$, kde n značí některé přirozené číslo > 2, pak platí také o každé uspořádané skupině n prvků v $\mathfrak{G}$. Nechť tedy $a_1, \ldots, a_n$ značí libovolné prvky grupoidu $\mathfrak{G}$ a předpokládejme, že každá uspořádaná skupina nejvýše $n - 1$ prvků v $\mathfrak{G}$ má jenom jeden součin. Pak každý symbol

$$a_1,\ a_2 \ldots a_n,\ a_1a_2,\ a_3 \ldots a_n,\ \ldots,\ a_1 \ldots a_{n-1},\ a_n$$

značí zcela určitý prvek grupoidu $\mathfrak{G}$, neboť podle našeho předpokladu je na př. jenom jeden součin $a_2 \ldots a_n$ uspořádané skupiny $n - 1$ prvků $a_2, \ldots, a_n \in \mathfrak{G}$. Máme ukázat, že všechny prvky

$$a_1(a_2 \ldots a_n),\ (a_1a_2)(a_3 \ldots a_n),\ \ldots,\ (a_1 \ldots a_{n-1})\, a_n \tag{1}$$

jsou identické. Za tím účelem si všimněme, že každý z těchto prvků je součinem $(a_1 \dots a_k) . (a_{k+1} \dots a_n)$ uspořádané dvojice prvků $a_1 \dots a_k$, $a_{k+1} \dots a_n \in \mathfrak{G}$, při čemž k značí některé číslo $1, \dots, n - 1$. Důkaz bude proveden, když zjistíme, že každý prvek (1) jest identický na př. s prvním z nich, t. j. že při každém $k = 1, \dots, n - 1$ platí rovnost

$$(a_1 \dots a_k)(a_{k+1} \dots a_n) = a_1(a_2 \dots a_n). \tag{2}$$

Když $k = 1$, je tato rovnost samozřejmá, a proto se můžeme omezit na případ $k > 1$. V tomto případě jest $a_1 \dots a_k$ součin uspořádané skupiny alespoň dvou a nejvýše $n - 1$ prvků $a_1, \dots, a_k$ a je tedy podle našeho předpokladu identický s prvkem $a_1(a_2 \dots a_k)$, takže vychází rovnost $(a_1 \dots a_k)(a_{k+1} \dots a_n) = (a_1(a_2 \dots a_k))(a_{k+1} \dots a_n)$. Protože grupoid $\mathfrak{G}$ jest asociativní, je prvek na pravé straně této rovnosti identický s prvkem $a_1((a_2 \dots a_k)(a_{k+1} \dots a_n))$, t. j. s prvkem $a_1(a_2 \dots a_n)$ a vychází (2).

Podobný výsledek platí ovšem o uspořádaných skupinách podmnožin v $\mathfrak{G}$.

10.2.3. *Důsledky základní věty o pologrupách.*

10.2.3.1. *Jednoznačnost složené permutace.*

Výsledek, který jsme právě dokázali, má důležité použití při skládání několika permutací nějaké (konečné nebo nekonečné) množiny prvků. Nechť $\mathbf{p}_1, \dots, \mathbf{p}_n$ $(n \geqq 2)$ značí libovolné permutace nějaké množiny H. Co rozumíme permutací složenou z permutací $\mathbf{p}_1, \dots, \mathbf{p}_n$ (v tomto pořadí)? V případě $n = 2$ je to, jak víme, složené zobrazení $\mathbf{p}_2\mathbf{p}_1$. V případě $n = 3$ definujeme pojem složené permutace z permutací $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$ takto: Permutací složenou z permutací $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3$ rozumíme kteroukoli z permutací $\mathbf{p}_3(\mathbf{p}_2\mathbf{p}_1)$, $(\mathbf{p}_3\mathbf{p}_2)\mathbf{p}_1$ a označujeme ji symbolem $\mathbf{p}_3\mathbf{p}_2\mathbf{p}_1$; symbol $\mathbf{p}_3\mathbf{p}_2\mathbf{p}_1$ má tedy význam jednak permutace složené z permutací $\mathbf{p}_2\mathbf{p}_1$, $\mathbf{p}_3$, jednak permutace složené z permutací $\mathbf{p}_1$, $\mathbf{p}_3\mathbf{p}_2$. V případě $n = 4$ definujeme permutaci složenou z permutací $\mathbf{p}_1, \mathbf{p}_2, \mathbf{p}_3, \mathbf{p}_4$ takto: Je to kterákoli z permutací $\mathbf{p}_4(\mathbf{p}_3\mathbf{p}_2\mathbf{p}_1)$, $(\mathbf{p}_4\mathbf{p}_3)(\mathbf{p}_2\mathbf{p}_1)$, $(\mathbf{p}_4\mathbf{p}_3\mathbf{p}_2)\mathbf{p}_1$ a označuje se symbolem $\mathbf{p}_4\mathbf{p}_3\mathbf{p}_2\mathbf{p}_1$. Symbol $\mathbf{p}_4\mathbf{p}_3\mathbf{p}_2\mathbf{p}_1$ má tedy význam kterékoli z těchto permutací množiny H: $\mathbf{p}_4(\mathbf{p}_3(\mathbf{p}_2\mathbf{p}_1))$, $\mathbf{p}_4((\mathbf{p}_3\mathbf{p}_2)\mathbf{p}_1)$, $(\mathbf{p}_4\mathbf{p}_3)(\mathbf{p}_2\mathbf{p}_1)$, $(\mathbf{p}_4(\mathbf{p}_3\mathbf{p}_2))\mathbf{p}_1$, $((\mathbf{p}_4\mathbf{p}_3)\mathbf{p}_2)\mathbf{p}_1$.

Obecně, pro $n \geqq 2$, definujeme permutaci složenou z permutací $\mathbf{p}_1, \dots, \mathbf{p}_n$ takto: Je to kterákoli z permutací

$$p_n(p_{n-1} \cdots p_1), (p_n p_{n-1})(p_{n-2} \cdots p_1), \ldots, (p_n \cdots p_2)p_1,$$

při čemž symbol v každé závorce značí libovolnou permutaci složenou z permutací v něm vyznačených, a to v pořadí od pravého konce symbolu k levému. Permutaci složenou z permutací $p_1, \ldots, p_n$ označujeme symbolem $p_n \ldots p_1$. Podle této definice má tedy symbol $p_n \ldots p_1$ význam součinu uspořádané skupiny n prvků $p_1, \ldots, p_n$ z grupoidu, jehož pole se skládá ze všech permutací množiny H a násobení je definováno skládáním permutací. Protože o skládání permutací platí asociativní zákon (viz **4.5.3**), je tento grupoid asociativní a z hořejšího výsledku plyne, že *jest jenom jedna permutace* $p_n \ldots p_1$ *složená z permutací* $p_1, \ldots, p_n$. Tuto větu vyjadřujeme také výrokem, že při stejném pořadí permutací nezávisí složená permutace na způsobu složení. Podle tohoto výsledku obdržíme tedy obraz $p_n \ldots p_1 x$ libovolného prvku $x \in H$ na př. podle vzorce

$$p_n \cdots p_1 x = p_n(p_{n-1}(\cdots (p_2(p_1 x)) \ldots)),$$

t. j. tím způsobem, že určíme nejprve obraz $p_1 x$ prvku x v permutaci p_1, pak obraz $p_2(p_1 x)$ prvku $p_1 x$ v permutaci p_2, atd. a konečně obraz $p_n(p_{n-1}(\cdots (p_2(p_1 x)) \ldots))$ prvku $p_{n-1}(\ldots (p_2(p_1 x))\ldots)$ v permutaci p_n. Odtud je také bezprostředně patrno, že když permutace $p_1, \ldots, p_n$ nechávají některý prvek $x \in H$ beze změny, pak totéž platí o složené permutaci $p_n \ldots p_1$.

10.2.3.2. *Složení permutace z permutací cyklických.*]

Použijme těchto výsledků k několika poznámkám o permutacích konečné množiny. Předpokládejme, že se množina H skládá z konečného počtu (≥ 1) prvků.

Především ukážeme, že *libovolná permutace množiny H je složena z konečného počtu cyklických permutací, jejichž cykly nemají společných prvků.*

Za tím účelem uvažujme o libovolné permutaci p množiny H. Jak jsme vyložili v odst. **4.4.5**, je permutace p vytvořena konečným počtem ryzích cyklických permutací $p_{\bar{a}}, \ldots, p_{\bar{m}}$, t. j. existuje rozklad $\bar{H} = \{\bar{a}, \ldots, \bar{m}\}$ množiny H takový, že každý jeho prvek $\bar{a}, \ldots, \bar{m}$ je v permutaci p invariantní a částečné permutace $p_{\bar{a}}, \ldots, p_{\bar{m}}$ jsou ryzí cyklické permutace prvků $\bar{a}, \ldots, \bar{m}$. Nechť $\bar{x}$ značí libovolný prvek v $\bar{H}$

a $\boldsymbol{q}_{\bar{x}}$ cyklickou permutaci množiny H, která je definována tím, že zobrazuje každý prvek $x \in \bar{x}$ na prvek $\boldsymbol{p}_{\bar{x}}x$ a všechny ostatní prvky množiny H, jsou-li jaké, nechává beze změny. Podle této definice má tedy cyklická permutace $\boldsymbol{q}_{\bar{x}}$ týž cyklus jako ryzí cyklická permutace $\boldsymbol{p}_{\bar{x}}$, můžeme tedy obě permutace $\boldsymbol{q}_{\bar{x}}, \boldsymbol{p}_{\bar{x}}$ vyjádřiti tímtéž zjednodušeným symbolem. Naše tvrzení bude dokázáno, zjistíme-li, že permutace $\boldsymbol{p}$ je složena z cyklických permutací $\boldsymbol{q}_{\bar{a}}, \ldots, \boldsymbol{q}_{\bar{m}}$, t. j. že $\boldsymbol{p} = \boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}$.

Nechť x značí libovolný prvek v H a $\bar{x}$ onen prvek rozkladu $\overline{\overline{H}}$, který jej obsahuje, takže permutace $\boldsymbol{q}_{\bar{x}}$ zobrazuje prvek x na prvek $\boldsymbol{q}_{\bar{x}}x$, ale všechny ostatní permutace $\boldsymbol{q}_{\bar{a}}, \ldots, \boldsymbol{q}_{\bar{m}}$, jsou-li jaké, nechávají prvek x beze změny. Protože při stejném pořadí permutací složená permutace nezávisí na způsobu složení, máme $\boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}x = (\boldsymbol{q}_{\bar{m}} \ldots)\, \boldsymbol{q}_{\bar{x}}(\ldots \boldsymbol{q}_{\bar{a}})\, x$, při čemž ovšem v případě $\bar{x} = \bar{m}$ vypustíme na pravé straně symbol složené permutace v první závorce a v případě $\bar{x} = \bar{a}$ symbol v druhé. Když $\bar{x} \neq \bar{a}$, máme $(\ldots \boldsymbol{q}_{\bar{a}})\, x = x$, neboť všechny permutace, z nichž $\ldots \boldsymbol{q}_{\bar{a}}$ je složena, nechávají prvek x beze změny. Máme tedy především $\boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}x = (\boldsymbol{q}_{\bar{m}} \ldots)\, \boldsymbol{q}_{\bar{x}}x$. Podobně zjistíme, že prvek na pravé straně této rovnosti je $\boldsymbol{q}_{\bar{x}}x$, takže vychází $\boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}x = \boldsymbol{q}_{\bar{x}}x$. Podle definice permutace $\boldsymbol{q}_{\bar{x}}$ je $\boldsymbol{q}_{\bar{x}}x = \boldsymbol{p}_{\bar{x}}x$ a dále podle definice permutace $\boldsymbol{p}_{\bar{x}}$ platí $\boldsymbol{p}_{\bar{x}}x = \boldsymbol{p}x$. Tím jsme došli k rovnosti $\boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}x = \boldsymbol{p}x$ a důkaz je proveden.

Všimněme si, že ve vzorci $\boldsymbol{p} = \boldsymbol{q}_{\bar{m}} \ldots \boldsymbol{q}_{\bar{a}}$ můžeme pořadí permutací $\boldsymbol{q}_{\bar{a}}, \ldots, \boldsymbol{q}_{\bar{m}}$ libovolně změniti, neboť při každém uspořádání permutací $\boldsymbol{q}_{\bar{a}}, \ldots, \boldsymbol{q}_{\bar{m}}$ můžeme zvoliti takové označení prvků rozkladu $\overline{\overline{H}}$, že tento vzorec zůstane beze změny.

Když máme nějaké permutace $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ $(n \geqq 2)$ množiny H vyjádřeny dvouřádkovými nebo zjednodušenými symboly, vyjadřujeme složenou permutaci $\boldsymbol{p}_n \ldots \boldsymbol{p}_1$ tím, že symboly permutací $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_n$ napíšeme vedle sebe v opačném pořádku vzhledem k tomuto. Podle této úmluvy a podle způsobu vyjádření libovolné permutace ryzími cyklickými permutacemi (viz odst. **4.4.5**), můžeme chápati na př. vzorec $\begin{pmatrix} a\,b\,c\,d \\ d\,c\,b\,a \end{pmatrix} = (a, d)(b, c)$ v tom smyslu, že permutace množiny $\{a, b, c, d\}$, vyjádřená symbolem na levé straně, je složena z cyklických permutací (b, c), (a, d), nebo v tom smyslu, že je vytvořena ryzími cyklickými permutacemi (a, d), (b, c).

10.3. Grupoidy s jednoznačným dělením neboli quasigrupy.

10.3.1. *Definice. Když se nějaký grupoid* $\mathfrak{G}$ *vyznačuje tím, že ke každým dvěma prvkům* $a, b \in \mathfrak{G}$ *existují prvky* $x, y \in \mathfrak{G}$ *splňující rovnosti*

$$ax = b, \; ya = b,$$

nazývá se $\mathfrak{G}$ *grupoid s dělením.*

Když existuje jediný prvek $x \in \mathfrak{G}$ *a jediný prvek* $y \in \mathfrak{G}$ *s touto vlastností, nazývá se* $\mathfrak{G}$ *grupoid s jednoznačným dělením.*

V literatuře se pro grupoid s jednoznačným dělením vyskytuje také název *quasigrupa.*

10.3.2. Je zřejmé, že *když* $\mathfrak{G}$ *je grupoid s dělením, platí rovnost* $\mathfrak{G}\mathfrak{G} = \mathfrak{G}$.

10.3.3. *Pravidla o krácení.* Všimněme si, že pro každý grupoid s jednoznačným dělením $\mathfrak{G}$ platí t. zv. *pravidla o krácení:*

Když pro některé prvky $a, x, y \in \mathfrak{G}$ *platí rovnost* $ax = ay$ *nebo* $xa = ya$, pak $x = y$.

Když v nějakém konečném grupoidu $\mathfrak{G}$ *platí pravidla o krácení, pak* $\mathfrak{G}$ *je grupoid s jednoznačným dělením.*

10.3.4. *Poznámka o multiplikační tabulce.*

Multiplikační tabulka každého konečného grupoidu s jednoznačným dělením $\mathfrak{G}$ má tuto charakteristickou vlastnost: V každém řádku a v každém sloupci se vyskytnou napravo od svislého a pod vodorovným záhlavím symboly *všech* prvků grupoidu $\mathfrak{G}$. Neboť jestliže se na př. v některém řádku $[a]$ (t. j. napravo od písmena a ve svislém záhlaví) nevyskytnou symboly všech prvků grupoidu $\mathfrak{G}$, pak se v řádku $[a]$ a v některých dvou různých sloupcích $[x_1]$, $[x_2]$ (t. j. pod symboly x_1, x_2 ve vodorovném záhlaví) vyskytne symbol téhož prvku b, a to znamená, že platí rovnosti $ax_1 = ax_2 = b$, které odporují pravidlům o krácení. Jestliže se naopak v každém řádku $[a]$ vyskytne symbol b každého prvku grupoidu $\mathfrak{G}$ v některém sloupci $[x]$ a současně se v každém sloupci $[a]$ vyskytne b v některém řádku $[y]$, pak mají rovnice $ax = b$, $ya = b$ jediné řešení: $x \in \mathfrak{G}$, $y \in \mathfrak{G}$, a tedy $\mathfrak{G}$ je grupoid s jednoznačným dělením.

10.3.5. *Příklady.* Na př. grupoidy $\mathfrak{Z}$, $\mathfrak{Z}_n$, $\mathfrak{S}_n$ ($n \geqq 1$) jsou quasigrupy: Ke každým dvěma prvkům $a, b \in \mathfrak{Z}$ existuje jediný prvek $x \in \mathfrak{Z}$ a jediný prvek $y \in \mathfrak{Z}$ takový, že $a + x = b$, $y + a = b$, a to $x = -a + b$, $y = b - a$. Podobně existuje ke každým dvěma prvkům $a, b \in \mathfrak{Z}_n$ jediný prvek $x \in \mathfrak{Z}_n$ a jediný prvek $y \in \mathfrak{Z}_n$ takový, že zbytek dělení čísla $a + x$ číslem n je b a zbytek dělení čísla $y + a$ číslem n je b, a to $x = y = -a + b$ ($= n - a + b$), když $-a + b \geqq 0$ ($-a + b < 0$). Ke každým dvěma permutacím $\boldsymbol{p}, \boldsymbol{q} \in \mathfrak{S}_n$ existuje jediná permutace $\boldsymbol{x} \in \mathfrak{S}_n$ a jediná permutace $\boldsymbol{y} \in \mathfrak{S}_n$ taková, že $\boldsymbol{p} \,.\, \boldsymbol{x} = \boldsymbol{q}$, $\boldsymbol{y} \,.\, \boldsymbol{p} = \boldsymbol{q}$ neboli $\boldsymbol{x} = \boldsymbol{q}\boldsymbol{p}^{-1}$, $\boldsymbol{y} = \boldsymbol{p}^{-1}\boldsymbol{q}$, při čemž $\boldsymbol{q}\boldsymbol{p}^{-1}$ značí permutaci složenou z permutace inversní $\boldsymbol{p}^{-1}$ vzhledem k $\boldsymbol{p}$ a z $\boldsymbol{q}$, a podobně $\boldsymbol{p}^{-1}\boldsymbol{q}$.

10.4. Grupoidy s jednotkou.

10.4.1. *Definice. Když se některý prvek, označme jej $\underline{1}$, v nějakém grupoidu $\mathfrak{G}$ vyznačuje tím, že součin prvku $\underline{1}$ s libovolným prvkem $a \in \mathfrak{G}$ je prvek a a podobně součin libovolného prvku $a \in \mathfrak{G}$ s prvkem $\underline{1}$ je rovněž prvek a, pak se prvek $\underline{1}$ nazývá jednotkový neboli jednotka grupoidu $\mathfrak{G}$.*

Jednotka $\underline{1} \in \mathfrak{G}$ je tedy charakterisována rovnostmi $\underline{1}a = a\underline{1} = a$, které platí pro každý prvek $a \in \mathfrak{G}$.

Snadno ukážeme, že *každý grupoid může míti nejvýše jednu jednotku.* Značí-li totiž $\underline{1}$, x jednotky libovolného grupoidu $\mathfrak{G}$, pak jest jednak $\underline{1}x = x$ (neboť $\underline{1}a = a$ pro každý prvek $a \in \mathfrak{G}$) a jednak $\underline{1}x = \underline{1}$ (neboť $ax = a$ pro každý prvek $a \in \mathfrak{G}$). Odtud plyne $\underline{1} = x$.

Když nějaký grupoid $\mathfrak{G}$ má jednotku, pak jej nazýváme *grupoid s jednotkou.*

10.4.2. *Poznámka o multiplikační tabulce.* Všimněme si, že multiplikační tabulka libovolného konečného grupoidu s jednotkou má tuto charakteristickou vlastnost: Onen řádek, na jehož začátku ve svislém záhlaví tabulky je vyznačena jednotka, obsahuje na dalších místech tytéž symboly a ve stejném pořádku jako vodorovné záhlaví tabulky. Podobně onen sloupec, na jehož začátku ve vodorovném záhlaví je vyznačena jednotka, obsahuje na dalších místech tytéž symboly a ve stejném pořádku jako svislé záhlaví.

10.4.3. *Příklady.* Příklady grupoidů s jednotkou jsou grupoidy $\mathfrak{Z}$, $\mathfrak{Z}_n$, $\mathfrak{S}_n$ ($n \geq 1$). Jednotkou grupoidu $\mathfrak{Z}$ je 0, neboť pro každý prvek $a \in \mathfrak{Z}$ platí rovnosti $0 + a = a + 0 = a$. Rovněž jednotkou grupoidu $\mathfrak{Z}_n$ je 0, neboť pro každý prvek $a \in \mathfrak{Z}_n$ dají čísla $0 + a$, $a + 0$ dělením číslem n zbytek a. Jednotkou grupoidu $\mathfrak{S}_n$ jest identická permutace $\boldsymbol{e}$ množiny H, neboť pro každý prvek $\boldsymbol{p} \in \mathfrak{S}_n$ máme $\boldsymbol{pe} = \boldsymbol{ep} = \boldsymbol{p}$. Naproti tomu na př. grupoid popsaný ve cvič. **8.8.3** nemá jednotku.

10.5. Další význačné grupoidy. Grupy.

Některé grupoidy mohou míti dvě nebo i všechny tři hořejší vlastnosti současně. Podle toho mluvíme pak o asociativních grupoidech s jednotkou neboli o pologrupách s jednotkou, o quasigrupách s jednotkou a o asociativních quasigrupách.

Quasigrupa s jednotkou se nazývá lupa. Pokud jde o asociativní quasigrupy, snadno ukážeme, že když *nějaký grupoid jest asociativní quasigrupa, pak nutně má jednotku*, t. j. když má obě první vlastnosti, pak má nutně i třetí.

Vskutku, nechť $\mathfrak{G}$ značí nějakou asociativní quasigrupu. Zvolme v $\mathfrak{G}$ libovolný prvek a. Protože $\mathfrak{G}$ je quasigrupa, existuje prvek $e_p \in \mathfrak{G}$, takový, že $ae_p = a$. O prvku e_p ukážeme, že jest jednotkou grupoidu $\mathfrak{G}$. Nechť b značí libovolný prvek v $\mathfrak{G}$. Protože $\mathfrak{G}$ je quasigrupa, existuje prvek $y \in \mathfrak{G}$ takový, že $ya = b$, a protože $\mathfrak{G}$ je asociativní, platí rovnosti $be_p = (ya)\, e_p = y(ae_p) = ya = b$. Vychází tedy $be_p = b$. Podobně zjistíme, že pro prvek $e_l \in \mathfrak{G}$ definovaný rovností $e_l a = a$ platí $e_l b = b$. Poněvadž jednak $e_l e_p = e_l$ (neboť $be_p = b$ pro každý prvek $b \in \mathfrak{G}$) a jednak $e_l e_p = e_p$ (neboť $e_l b = b$ pro každý prvek $b \in \mathfrak{G}$), vidíme, že $e_l = e_p$ a že prvek e_p skutečně má charakteristické vlastnosti jednotky grupoidu $\mathfrak{G}$. Všimněme si, že jsme při tomto důkazu nepoužili předpokladu, že dělení v $\mathfrak{G}$ jest jednoznačné.

Asociativní quasigrupy se obvykle nazývají grupy. Naši větu možno tedy vyjádřit tím, že každá grupa má jednotku. Na př. $\mathfrak{Z}$, $\mathfrak{Z}_n$, $\mathfrak{S}_n$ ($n \geq 1$) jsou grupy. Poznamenejme, že *se grupa $\mathfrak{S}_n$ nazývá symetrická permutační grupa stupně n.*

Všechny zmíněné druhy grupoidů mohou míti ovšem ještě další vlastnosti, na př. mohou býti abelovské; v tom případě mluvíme na př. o abelovských asociativních grupoidech s jednotkou, atp.

10.6. Svazy.

Tuto kapitolu zakončíme krátkým výkladem o t. zv. svazech, jejichž pojem se k předcházejícím úvahám úzce přimyká. V podstatě jsou svazy dvojice *soumístných*, t. j. na témže poli definovaných, grupoidů se zvláštními vlastnostmi, při čemž jejich násobení jsou vázána jistými zákony. Theorie svazů zaujímá v moderní matematice významné místo nejenom pro svou obsažnost a formální půvab, nýbrž zejména proto, že s jednotícího hlediska popisuje vlastnosti nejrozmanitějších útvarů, které se vyskytují v různých oborech matematiky jako realisace svazů.

Nechť jsou na množině G dána *dvě násobení*. Abychom je v úvahách mohli snadno odlišit, zvolíme jedno z nich libovolně a nazveme je *horní*, kdežto druhé nazveme *dolní*. Součin libovolného prvku $a \in G$ s libovolným prvkem $b \in G$ v horním (dolním) násobení nazýváme *spojení* (*průnik*) *prvku* a *s prvkem* b a označujeme jej symbolem $a \smile b$ ($a \frown b$). Grupoid, jehož polem je množina G a násobení je horní (dolní) násobení, nazýváme *horní* (*dolní*) *grupoid*.

10.6.1. *Definice svazu. Dvojice horního a dolního grupoidu se nazývá svaz na poli* G, stručněji: *svaz, když pro každé prvky* $a, b, c \in G$ *platí tyto rovnosti:*

a. $a \smile b = b \smile a,$	**a′.** $a \frown b = b \frown a,$
b. $a \smile a = a,$	**b′.** $a \frown a = a,$
c. $a \smile (b \smile c) = (a \smile b) \smile c,$	**c′.** $a \frown (b \frown c) = (a \frown b) \frown c,$
d. $a \smile (a \frown b) = a;$	**d′.** $a \frown (a \smile b) = a.$

Každý z obou grupoidů svazu je tedy abelovský (**a**, **a′**) a asociativní (**c**, **c′**) a všechny jeho prvky jsou rovnomocné (**b**, **b′**). Násobení obou grupoidů spolu souvisí podle vzorců **d**, **d′**; tyto vzorce vyjadřují t. zv. *absorptivní zákony svazu.*

10.6.2. *Příklady svazů:*

[1] G je množina všech přirozených čísel $1, 2, 3 \ldots$; $a \smile b$ je nejmenší společný násobek a $a \frown b$ největší společný dělitel čísla a a čísla b.

[2] G je množina všech částí nějaké množiny. $A \smile B$ je součet a $A \frown B$ průnik části A a části B.

[3] G je množina všech rozkladů nějaké množiny. $\bar{A} \smile \bar{B}$ je nejmenší společný zákryt $[\bar{A}, \bar{B}]$ a $\bar{A} \frown \bar{B}$ největší společné zjemnění $(\bar{A}, \bar{B})$ rozkladu $\bar{A}$ a rozkladu $\bar{B}$.

10.6.3. *Základní částečná uspořádání svazu.* Budiž Γ svaz na poli G. Nechť $a, b, c \in G$ jsou libovolné prvky.

10.6.3.1. Především si všimněme, že *oba vztahy*

$$a \smile b = b, \quad b \frown a = a \tag{h}$$

platí současně, t. j. když platí jeden, platí i druhý.

Vskutku, z platnosti prvního vztahu plyne podle **10.6.1 a′,d′**:

$$b \frown a = (a \smile b) \frown a = a \frown (a \smile b) = a;$$

podobně z platnosti druhého plyne podle **10.6.1 a,d**:

$$a \smile b = (b \frown a) \smile b = b \smile (b \frown a) = b.$$

Když ke každému prvku $a \in G$ přiřadíme každý prvek $b \in G$, který splňuje rovnosti (h), obdržíme zobecněné zobrazení množiny G na sebe; označíme je $\boldsymbol{h}$.

Zobrazení $\boldsymbol{h}$ *je antisymetrická kongruence na* G. Vskutku, ze vzorců **10.6.1b, b′** vidíme, že je reflexivní. Přihlížejíce k vzorci **10.6.1c**, soudíme, že ze vztahů $a \smile b = b, b \smile c = c$ následuje: $a \smile c = a \smile (b \smile c) = (a \smile b) \smile c = b \smile c = c$; z toho vidíme, že zobrazení $\boldsymbol{h}$ je transitivní. Je to tedy kongruence na G. Konečně z rovností $a \smile b = b$, $b \smile a = a$ plyne, podle **10.6.1a**, že $a = b$.

Zjistili jsme, že kongruence $\boldsymbol{h}$ je antisymetrická, jinými slovy, že zobrazení $\boldsymbol{h}$ je částečné uspořádání množiny G. Nazýváme je *horní částečné uspořádání svazu* Γ.

Připomeňme, že následující symboly mají týž obsah: $a \leqq b$ $(\boldsymbol{h})$, $a \smile b = b$, $b \frown a = a$.

Obdobné úvahy platí, když vyměníme úlohy horního a dolního grupoidu. Potom máme tyto výsledky:

Oba vztahy

$$b \smile a = a, \quad a \frown b = b \tag{d}$$

platí současně.

Když ke každému prvku $a \in G$ *přiřadíme každý prvek* $b \in G$, *který splňuje rovnosti* (d), *obdržíme na* G *jistou antisymetrickou kongruenci* $\boldsymbol{d}$. *Nazýváme ji dolní částečné uspořádání svazu* Γ.

Vidíme, že následující symboly mají týž obsah: $a \leqq b$ ($\boldsymbol{d}$), $b \smile a = a$, $a \frown b = b$.

Horní a dolní částečné uspořádání svazu Γ nazýváme souhrnně *základní částečná uspořádání.*

Základní částečná uspořádání svazu Γ jsou vzájemně inversní, takže $\boldsymbol{d} = \boldsymbol{h}^{-1}$, $\boldsymbol{h} = \boldsymbol{d}^{-1}$. To plyne z toho, že v kongruenci $\boldsymbol{h}$ je každý prvek $b \in G$ obrazem všech prvků $a \in G$, které hoví rovnostem (h), a právě tyto prvky jsou obrazy prvku b v kongruenci $\boldsymbol{d}$, jak vidíme ze vzorců (d).

Všimněme si, že symboly $a \leqq b$ ($\boldsymbol{h}$) a $b \leqq a$ ($\boldsymbol{d}$) mají týž obsah. Na př. na svazu popsaném v odst. **10.6.2** [1] obdržíme horní (dolní) částečné uspořádání tím, že ke každému přirozenému číslu přiřadíme každý jeho kladný násobek (dělitele); na svazu [2] tím, že ke každé množině $A \in G$ přiřadíme každou její nadmnožinu (podmnožinu) $B \in G$; na svazu [3] tím, že ke každému rozkladu $\bar{A} \in G$ přiřadíme každý jeho zákryt (zjemnění) $\bar{B} \in G$.

10.6.3.2. *Vzhledem k hornímu (dolnímu) částečnému uspořádání svazu je prvek $a \smile b$ horní (dolní) a prvek $a \frown b$ dolní (horní) hranicí prvků a, b.*

Protože horní a dolní částečné uspořádání jsou vzájemně inversní, stačí ukázat, že tvrzení je správné na př. v případě horního částečného uspořádání (odst. **3.9.1.3**).

Máme ukázat, že vzhledem ke kongruenci $\boldsymbol{h}$ platí vztahy $a \leqq a \smile b$ $b \leqq a \smile b$ a dále, že ze vztahů $a \leqq c$, $b \leqq c$ následuje $a \smile b \leqq c$.

Správnost vztahů $a \leqq a \smile b$, $b \leqq a \smile b$ plyne z rovností, které platí v důsledku vzorců **10.6.1c, b, a**:

$$a \smile (a \smile b) = (a \smile a) \smile b = a \smile b,$$

$$b \smile (a \smile b) = b \smile (b \smile a) = (b \smile b) \smile a = b \smile a = a \smile b.$$

Vztahy $a \leqq c$, $b \leqq c$ vyjadřují rovnosti

$$a \smile c = c, \; b \smile c = c,$$

z nichž následuje, podle **10.6.1c**,

$$(a \smile b) \smile c = a \smile (b \smile c) = a \smile c = c,$$

t. j. $a \smile b \leqq c$. Tím je důkaz proveden.

Vidíme tedy, že *vzhledem k hornímu (dolnímu) částečnému uspořádání svazu má každá dvojice prvků svazu horní i dolní hranici; horní hranicí je spojení (průnik) a dolní hranicí je průnik (spojení) obou prvků.*

10.6.4. *Poznámka k definici svazu.* Svaz jsme definovali jako dvojic soumístných grupoidů, které mají zvláštní vlastnosti a jejichž násobení jsou vázána jistými zákony. Potom jsme ukázali, že na každém svazu jsou jistá vzájemně inversní částečná uspořádání, vzhledem k nimž má každá dvojice prvků horní i dolní hranici; horní a dolní hranice jsou součiny obou prvků dvojice v grupoidech svazu.

Naopak lze definici svazu založit na pojmu antisymetrické kongruence. Když je na množině G dána libovolná antisymetrická kongruence, vzhledem k níž má každá dvojice prvků $a, b \in G$ horní hranici $a \smile b$ a dolní hranici $a \frown b$, můžeme na množině G definovat dvě násobení tím, že součin uspořádané dvojice prvků a, b je jednou $a \smile b$ a po druhé $a \frown b$. Dá se snadno ukázat, že dvojice grupoidů na poli G s těmito násobeními je svazem a výchozí antisymetrická kongruence je horním a kongruence k ní inversní dolním částečným uspořádáním tohoto svazu.

10.6.5. *Význačné druhy svazů.* Nechť Γ je svaz na poli G.

10.6.5.1. *Svazy s krajními prvky.* Když se některý prvek $O \in G$ vyznačuje tím, že pro každý prvek $a \in G$ platí $a \leqq O$ (**h**) [$a \leqq O$ (**d**)], pravíme o něm, že je *největší vzhledem k hornímu* (*dolnímu*) *částečnému uspořádání*; když se některý prvek $o \in G$ vyznačuje tím, že vždycky platí $o \leqq a$ (**h**) [$o \leqq a$ (**d**)], nazývá se *nejmenší vzhledem k hornímu* (*dolnímu*) *částečnému uspořádání*. Snadno vidíme, přihlížejíce k současné platnosti vztahů **10.6.3.1** (h) nebo (d), že *největší prvek vzhledem k hornímu* (*dolnímu*) *částečnému uspořádání je nejmenším* (*největším*) *vzhledem k částečnému uspořádání dolnímu* (*hornímu*). Rovněž je snadné nahlédnout, že ve svazu může býti vzhledem k témuž základnímu částečnému uspořádání nejvýše jeden největší a nejvýše jeden nejmenší prvek. Největší a nejmenší prvky vzhledem ke každému základnímu částečnému uspořádání svazu se nazývají *krajními prvky*.

Když ve svazu Γ oba krajní prvky vzhledem k oběma základním částečným uspořádáním existují, pravíme že Γ je svaz s krajními prvky.

Na př. svaz popsaný v odst. **10.6.2** [1] má vzhledem k hornímu částečnému uspořádání nejmenší prvek 1, ale nemá největšího prvku; vzhledem k dolnímu částečnému uspořádání má tedy největší prvek 1, ale nemá nejmenšího prvku. Svaz [2] je svaz s krajními prvky; největším (nejmenším) prvkem vzhledem k hornímu částečnému uspořádání je množina, z jejíchž částí se pole svazu skládá (prázdná množina). Rovněž [3] je svaz s krajními prvky; největším (nejmenším) prvkem svazu vzhledem k hornímu částečnému uspořádání je největší (nejmenší) rozklad na množině, z jejíchž rozkladů se svaz skládá.

10.6.5.2. *Svazy Dedekindovy neboli modulární. Když pro některé prvky $a, b, c \in G$, které se vyznačují tím, že $a \leq c$ (**h**), platí rovnost*

$$a \smile (b \frown c) = (a \smile b) \frown c,$$

pravíme, že uspořádaná trojice prvků a, b, c splňuje horní Dedekindův vztah; podobně, *když je $a \leq c$ (**d**) a platí rovnost*

$$a \frown (b \smile c) = (a \frown b) \smile c,$$

pravíme, že ona trojice splňuje dolní Dedekindův vztah.

Je zřejmé, že *když uspořádaná trojice prvků a, b, c splňuje horní (dolní) Dedekindův vztah, pak opačně uspořádaná trojice c, b, a splňuje dolní (horní) Dedekindův vztah.*

*Svaz Γ se nazývá Dedekindův neboli modulární, když každá uspořádaná trojice prvků $a, b, c \in G$, v níž je $a \leq c$ (**h**) [$a \leq c$ (**d**)] splňuje horní (dolní) Dedekindův vztah.*

Na př. svaz popsaný v odst. **10.6.2** [2] je Dedekindův, neboť pro každé tři části A, B, C libovolné množiny, které se vyznačují tím, že $A \subset C$, platí rovnost $A \vee (B \cap C) = (A \vee B) \cap C$ (viz **1.7.5**). Připomeňme, že současně má tento svaz krajní prvky (**10.6.5.1**).

10.7. Cvičení.

10.7.1. Když nějaká permutace p nějaké množiny je složena z permutací $p_1, \ldots, p_n$ ($n \geq 2$), pak inversní permutace p^{-1} je složena z permutací $p_n^{-1}, \ldots, p_1^{-1}$.

10.7.2. Každá cyklická permutace nějaké konečné množiny, jejíž cyklus je alespoň dvojčlenný, se dá složiti z několika transposic, a to podle vzorce: $(a, b, c, \ldots, k, l, m) = (a, b)(b, c) \ldots (k, l)(l, m)$.

10.7.3. Označme (kvůli přehlednosti dolejšího vzorce) prvky nějaké množiny H řádu n (≥ 2), číslicemi $1, \ldots, n$. Každá transposice $(i, i+j)$

množiny H se dá složit z několika transposic $(1, 2), (2, 3), \ldots, (n - 1, n)$, a to podle vzorce: $(i, i + j) = (i + j - 1, i + j) \ldots (i + 1, i + 2) (i, i + 1)(i + 1, i + 2) \ldots (i + j - 1, i + j)$. Každá permutace množiny H se dá složit z několika transposic $(1, 2), (2, 3), \ldots, (n - 1, n)$.

10.7.4. Když grupoid $\mathfrak{G}$ má jednotku, pak její obraz v každé deformaci $\boldsymbol{d}$ grupoidu $\mathfrak{G}$ do nějakého grupoidu $\mathfrak{G}^*$ je jednotkou obrazu $\boldsymbol{d}\mathfrak{G}$.

10.7.5. Každý faktoroid $\overline{\mathfrak{G}}$ na libovolném grupoidu s jednotkou $\mathfrak{G}$ má jednotku, a to onen prvek $\bar{a} \in \overline{\mathfrak{G}}$, který obsahuje jednotku grupoidu $\mathfrak{G}$, jest jednotkou faktoroidu $\overline{\mathfrak{G}}$.

10.7.6. Uveďte příklady grupoidů, které jsou jenom: 1. asociativní, 2. s jednoznačným dělením, 3. s jednotkou; a příklady grupoidů, které mají právě jenom vlastnosti 1, 3 a vlastnosti 2, 3.

10.7.7. Každý konečný asociativní grupoid je grupa, když pro něj platí pravidla o krácení.

10.7.8. Součin několika prvků $a_1, \ldots, a_n$ $(n \geqq 2)$ v libovolné pologrupě nezávisí na jejich uspořádání, když každé dva z prvků $a_1, \ldots, a_n$ jsou vzájemně zaměnitelné. V libovolné abelovské pologrupě nezávisí součin libovolné skupiny prvků na jejich uspořádání.

10.7.9. Vlastnosti horního a dolního grupoidu požadované v definici svazu (odst. **10.6.1**) nejsou nezávislé, neboť vlastnosti **b**, **b′** jsou důsledkem ostatních. Přesvědčte se o tom, aplikujíce rovnost **d′(d)** na prvky $a, b = a$ a rovnost **d(d′)** na prvky $a, b = a \smile a$ $(a, b = a \frown a)$.

10.7.10. Když se nějaký svaz skládá z rozkladů na množině G, z nichž každé dva jsou doplňkové, a když násobení jsou definována jako v př. **10.6.2** [3], pak je modulární.

10.7.11. Svaz je modulární tehdy a jen tehdy, když v něm každé tři prvky a, b, c splňují rovnost: $(a \smile b) \frown [c \smile (a \frown b)] = (a \frown b) \smile [c \frown (a \smile b)]$.