II. Grupoidy.

5. O násobení v množině.

Východiskem k našim dalším úvahám jest pojem násobení v množině, který v jistém smyslu zobecňuje pojem zobrazení množiny do sebe. Jako v kapitole I., tak i všude v dalším, značí písmeno G nějakou neprázdnou množinu.

Násobením v množině G rozumíme nějaké pravidlo, jímž jest ke každé uspořádané dvojici prvků $a, b \in G$ jednoznačně přiřazen opět některý prvek $c \in G$. Tento prvek c se nazývá *součin* prvku a s prvkem b a značí se symbolem $a.b$ anebo kratčeji ab. Z těchto definic jest zřejmé, že slovo násobení jest jenom název pro nějaké pravidlo, podrobněji popsané v naší definici, a že v konkretních případech nemusí míti nic společného s pojmem aritmetického násobení, které známe z obecné školy; podobná poznámka platí ovšem o součinu a o symbolech $a.b$, ab. V jakém smyslu zobecňuje pojem násobení v množině G pojem zobrazení množiny G do sebe, na to odpověď plyne snadno z porovnání obou definic: Každé zobrazení množiny G do sebe přiřazuje jednoznačně ke každému prvku v G opět nějaký prvek v G; každé násobení v množině G přiřazuje jednoznačně ke každé uspořádané dvojici prvků v G opět nějaký prvek v G. K naší definici násobení v množině připojme ještě několik poznámek! Jestliže jest dáno násobení v množině G, pak jest zejména jednoznačně určen součin každého prvku $a \in G$ opět s prvkem a; místo aa píšeme někdy stručněji a^2. Násobení v množině G může míti zvláštní vlastnosti. Tak na příklad není naší definicí vyloučeno, že násobení přiřazuje k některým dvěma opačně uspořádaným dvojicím prvků v G dva různé prvky, takže se může státi, že součin některého prvku a s některým prvkem b jest různý od součinu prvku b s prvkem a, t. j. $ab \neq ba$. Jestliže pro některé dva prvky $a, b \in G$ platí rovnost $ab = ba$, pak se prvky a, b nazývají *zaměnitelné* anebo *komutativní;* jestliže každé dva prvky v G jsou zaměnitelné, pak se násobení nazývá *abelovské* anebo *komutativní*.

Násobení v množině může míti ovšem i jiné význačné vlastnosti a o některých, které jsou pro náš účel důležité, pojednáme později. Zde uvedeme tři příklady násobení, na něž v dalším výkladu častěji poukážeme.

[1] G jest množina všech celých čísel a násobení jest definováno takto: Součin libovolného prvku $a \in G$ s libovolným prvkem $b \in G$ jest číslo $a + b$. V tomto případě jest tedy násobením sečítání v obvyklém smyslu. Z rovnosti $a + b = b + a$, která platí pro každé dva prvky $a, b \in G$, plyne, že toto násobení jest abelovské.

[2] Nechť n jest libovolné přirozené číslo a G nějaká množina skládající se z přirozených čísel, která obsahuje všechna čísla $0, \ldots, n - 1$.

Násobení v množině G definujeme takto: Součin ab libovolného prvku $a \in G$ s libovolným prvkem $b \in G$ jest zbytek dělení čísla $a + b$ číslem n.*) Součin ab jest tedy vždy jedno z čísel $0, \ldots, n - 1$. Toto násobení nazýváme *sečítání vzhledem k modulu n*; jest zřejmé, že jest také abelovské.

[3] G jest množina všech permutací nějaké konečné množiny řádu n (≥ 1) a násobení jest definováno takto: Součin $\boldsymbol{p} \cdot \boldsymbol{q}$ libovolného prvku $\boldsymbol{p} \in G$ s libovolným prvkem $\boldsymbol{q} \in G$ jest složená permutace $\boldsymbol{qp}$. V tomto případě jest tedy násobení skládání permutací a z dřívějšího výkladu víme, že nemusí býti abelovské.

Když množina G jest konečná a její prvky jsme označili na př. písmeny $a, b, \ldots, m$ pak libovolné násobení v G můžeme popsati v t. zv. *multiplikační tabulce*, kterou sestavíme takto: Do prvního řádku a do prvního sloupce, které obvykle od ostatních oddělujeme vodorovnou a svislou čarou, napíšeme všechna písmena $a, b, \ldots, m$ a sice zpravidla v témže pořádku, v prvním řádku od leva do prava a v prvním sloupci od shora dolů. Napravo od každého písmene x v prvním sloupci a sice pod jednotlivá písmena $a, b, \ldots, m$ stojící v prvním řádku, napíšeme písmena označující jednotlivé součiny $xa, xb, \ldots, xm$. První řádek a první sloupec, oddělené od ostatních čarami, nazýváme *záhlaví* tabulky. Každá multiplikační tabulka má tedy kromě vodorovného a svislého záhlaví ještě právě tolik řádků a sloupců, kolik má množina G prvků. Když písmena $a, b, \ldots, m$ jsou v obou záhlavích napsána v témže pořádku, pak se násobení abelovské projeví v tabulce patrně tím, že tabulka jest souměrná vzhledem k hlavní úhlopříčně, t. j. v jejím libovolném j-tém řádku a v libovolném k-tém sloupci za oběma záhlavími jest týž prvek jako v k-tém řádku a j-tém sloupci.

Jako příklad uvedeme multiplikační tabulky pro násobení v množině G všech permutací nějaké množiny H, která se skládá z $n = 1, 2, 3$ prvků, při čemž násobení jest skládání permutací, jak jsme je popsali v hořejším příkladě [3]. Protože všech permutací množiny H a tedy prvků množiny G jest $n! = 1, 2, 6$, mají tyto multiplikační tabulky, kromě obou záhlaví, $n! = 1, 2, 6$ řádků a sloupců.

---

*) Nechť n jest libovolné přirozené číslo. Ze střední školy víme, že ke každému celému číslu x můžeme jednoznačně přiřaditi a sice dělením čísla x číslem n, jisté celé číslo q a dále jisté celé číslo r hovící nerovnostem $0 \leqq r \leqq n - 1$, tak, že $x = qn + r$; číslo q se nazývá *podíl* a číslo r *zbytek* dělení čísla x číslem n. V dalších úvahách použijeme častěji této věty: *Když se dvě celá čísla x, y liší jenom o celý násobek čísla n*, t. j. když $x - y = nk$, kde k značí nějaké celé číslo, *pak jejich zbytky dělení r, s číslem n jsou stejné.* Z rovnic $x - y = nk$, $x = nq' + r$, $y = nq'' + s$ plyne totiž $n(k - q' + q'') = r - s$ a protože platí nerovnosti $0 \leqq r, s \leqq n - 1$, jest tato rovnice splněna jenom když $r = s$.

$n = 1$. Množina G se skládá z identické permutace $\boldsymbol{e}$. Označíme-li onen prvek, z něhož se množina H skládá, písmenem a, jest symbol této permutace $\begin{pmatrix} a \\ a \end{pmatrix}$ a multiplikační tabulka jest tato:

	e
e	***e***

$n = 2$. Množina G se skládá ze dvou permutací. Označíme-li prvky množiny H písmeny a, b, jsou symboly těchto permutací $\begin{pmatrix} a\,b \\ a\,b \end{pmatrix}, \begin{pmatrix} a\,b \\ b\,a \end{pmatrix}$. První z nich jest identická permutace $\boldsymbol{e}$, druhou označíme na př. $\boldsymbol{a}$. Permutace složené jsou: $\boldsymbol{ee} = \boldsymbol{e}$, $\boldsymbol{ae} = \boldsymbol{a}$, $\boldsymbol{ea} = \boldsymbol{a}$, $\boldsymbol{aa} = \boldsymbol{e}$, a odtud vychází tato multiplikační tabulka:

	e	***a***
e	***e***	***a***
a	***a***	***e***

$n = 3$. Množina G se skládá ze šesti permutací. Označíme-li prvky množiny H písmeny a, b, c, jsou symboly těchto permutací

$$\begin{pmatrix} a\,b\,c \\ a\,b\,c \end{pmatrix}, \begin{pmatrix} a\,b\,c \\ b\,c\,a \end{pmatrix}, \begin{pmatrix} a\,b\,c \\ c\,a\,b \end{pmatrix}, \begin{pmatrix} a\,b\,c \\ a\,c\,b \end{pmatrix}, \begin{pmatrix} a\,b\,c \\ c\,b\,a \end{pmatrix}, \begin{pmatrix} a\,b\,c \\ b\,a\,c \end{pmatrix}.$$

První z nich jest identická permutace $\boldsymbol{e}$, ostatní označíme popořádku $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, \boldsymbol{d}, \boldsymbol{f}$. Permutace složené jsou:

$$\begin{array}{llllll}
\boldsymbol{ee} = \boldsymbol{e}, & \boldsymbol{ae} = \boldsymbol{a}, & \boldsymbol{be} = \boldsymbol{b}, & \boldsymbol{ce} = \boldsymbol{c}, & \boldsymbol{de} = \boldsymbol{d}, & \boldsymbol{fe} = \boldsymbol{f}; \\
\boldsymbol{ea} = \boldsymbol{a}, & \boldsymbol{aa} = \boldsymbol{b}, & \boldsymbol{ba} = \boldsymbol{e}, & \boldsymbol{ca} = \boldsymbol{d}, & \boldsymbol{da} = \boldsymbol{f}, & \boldsymbol{fa} = \boldsymbol{c}; \\
\boldsymbol{eb} = \boldsymbol{b}, & \boldsymbol{ab} = \boldsymbol{e}, & \boldsymbol{bb} = \boldsymbol{a}, & \boldsymbol{cb} = \boldsymbol{f}, & \boldsymbol{db} = \boldsymbol{c}, & \boldsymbol{fb} = \boldsymbol{d}; \\
\boldsymbol{ec} = \boldsymbol{c}, & \boldsymbol{ac} = \boldsymbol{f}, & \boldsymbol{bc} = \boldsymbol{d}, & \boldsymbol{cc} = \boldsymbol{e}, & \boldsymbol{dc} = \boldsymbol{b}, & \boldsymbol{fc} = \boldsymbol{a}; \\
\boldsymbol{ed} = \boldsymbol{d}, & \boldsymbol{ad} = \boldsymbol{c}, & \boldsymbol{bd} = \boldsymbol{f}, & \boldsymbol{cd} = \boldsymbol{a}, & \boldsymbol{dd} = \boldsymbol{e}, & \boldsymbol{fd} = \boldsymbol{b}; \\
\boldsymbol{ef} = \boldsymbol{f}, & \boldsymbol{af} = \boldsymbol{d}, & \boldsymbol{bf} = \boldsymbol{c}, & \boldsymbol{cf} = \boldsymbol{b}, & \boldsymbol{df} = \boldsymbol{a}, & \boldsymbol{ff} = \boldsymbol{e},
\end{array}$$

a vychází tato multiplikační tabulka:

	e	***a***	***b***	***c***	***d***	***f***
e	***e***	***a***	***b***	***c***	***d***	***f***
a	***a***	***b***	***e***	***d***	***f***	***c***
b	***b***	***e***	***a***	***f***	***c***	***d***
c	***c***	***f***	***d***	***e***	***b***	***a***
d	***d***	***c***	***f***	***a***	***e***	***b***
f	***f***	***d***	***c***	***b***	***a***	***e***

Ve všech těchto multiplikačních tabulkách napsali jsme v obou záhlavích symboly $\boldsymbol{e}, \boldsymbol{a}, \ldots, \boldsymbol{f}$ jednotlivých prvků množiny G v témže pořádku a vidíme, že v případech $n = 1, 2$ jsou hořejší tabulky souměrné vzhledem k hlavní úhlopříčně, kdežto v případě $n = 3$ jest multiplikační tabulka nesouměrná. Odtud plyne, že naše násobení v množině G jest v případech $n = 1, 2$ abelovské, ale v případě $n = 3$ abelovské není.

Příkladů násobení v množinách dá se uvésti nepřehledné množství. Stačí vzíti libovolnou abstraktní neprázdnou množinu G a ke každé uspořádané dvojici prvků $a, b \in G$ jednoznačně přiřaditi některý prvek v G. Když množina G jest konečná, pak můžeme přiřazení definovati v tabulce, v níž na jednotlivých místech, pod vodorovným záhlavím a napravo od svislého, napíšeme symboly některých prvků množiny G, které zvolíme podle libosti. Každá volba těchto prvků určuje pak jisté násobení, pro které naše tabulka jest multiplikační.

Cvičení. 1. V množině všech euklidovských pohybů na přímce $\boldsymbol{f}[a]$ a rovněž v množině skládající se ze všech euklidovských pohybů na přímce $\boldsymbol{f}[a]$, $\boldsymbol{g}[a]$ (v. cvič. 5. v odst. 3.) můžeme definovati násobení skládáním pohybů, podobně jako v hořejším příkladě [3]. Podobný výsledek platí o množině všech euklidovských pohybů v rovině $\boldsymbol{f}[\alpha; a, b]$ a o množině všech euklidovských pohybů v rovině $\boldsymbol{f}[\alpha; a, b]$, $\boldsymbol{g}[\alpha; a, b]$ (v. cvič. 6. v odst. 3.).

2. V množině $2n$ permutací vrcholů pravidelného n-úhelníka v rovině ($n \geqq 3$), které jsme popsali ve cvič. 4. v odst. 4., můžeme definovati násobení skládáním permutací podobně jako v hořejším příkladě [3]. Sestavte pro toto násobení v případech $n = 4, 5, 6$ multiplikační tabulky!

3. V hořejším příkladě [2] může se množina G skládati právě jenom z čísel $0, \ldots, n - 1$. Sestavte pro tento případ a sice pro $n = 1, 2, 3, 4, 5$ multiplikační tabulky!

4. Když přirozená čísla a, b jsou menší anebo rovna nějakému přirozenému číslu $n \geqq 5$, pak počet prvočísel, která dělí číslo $10a + b$, jest $\leqq n$. Odtud plyne, že v množině G, která se skládá z čísel $1, 2, \ldots, n$, můžeme definovati násobení takto: Součin $a . b$ libovolného prvku $a \in G$ s libovolným prvkem $b \in G$ jest počet prvočísel, která dělí číslo $10a + b$. Přesvědčte se, že pro $n = 6$ příslušná multiplikační tabulka jest tato:

	1	2	3	4	5	6
1	1	3	1	2	2	4
2	2	2	1	4	2	2
3	1	5	2	2	2	4
4	1	3	1	3	3	2
5	2	3	1	4	2	4
6	1	2	3	6	2	3

5. V systému všech podmnožin libovolné neprázdné množiny můžeme definovati násobení tím, že ke každé uspořádané dvojici podmnožin přiřadíme jejich součet. Můžeme násobení podobně definovati pomocí průniku?

6. Vymyslete sami příklady násobení v množinách!