II. GRUPOIDY

11. Násobení v množinách

11.1. Základní pojmy

Násobením neboli *binární operací* v množině G rozumíme vztah mezi prvky množiny G, který se vyznačuje tím, že ke každé dvoučlenné posloupnosti prvků $a, b \in G$ je přiřazen právě jeden prvek $c \in G$; jinými slovy vztah, jímž je každá dvoučlenná posloupnost prvků a, b v množině G zobrazena právě na jeden prvek c téže množiny G. Tento prvek c se nazývá *součin prvku a s prvkem b* nebo též *součin z prvků a a b*, a značí se symbolem: $a \, . \, b$ kratčeji ab; máme tedy $c = ab$. Přitom a (b) je *první* (*druhý*) *činitel* neboli *faktor* součinu c.

Z těchto definic je zřejmé, že slovo násobení je jenom názvem pro vztah mezi prvky množiny G, který byl podrobněji popsán v hořejší definici, a že v konkrétních případech nemusí mít nic společného s obvyklým aritmetickým násobením; obdobná poznámka platí též 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 dvoučlenné posloupnosti prvků v G opět nějaký prvek v G.

Je zřejmé, že násobení v množině G můžeme též definovat jako zobrazení kartézského čtverce $G \times G$ (**1.8**) do množiny G. Pak se součiny jeví jako obrazy jednotlivých prvků tohoto kartézského čtverce. Teorie grupoidů, která, jak uvidíme, je založena na pojmu násobení v množině, se dá tímto způsobem podřadit obecné teorii o zobrazování množin. Naše další úvahy jsou však založeny na hořejším pojmu násobení, protože vývin teorie grupoidů na základě tohoto pojmu je bez podrobnějšího studia vlastností kartézských čtverců pro naše účely jednodušší. Nicméně doporučujeme čtenáři, aby další úvahy promýšlel i ze zmíněného hlediska zobrazování množin.

neboť se mu přitom naskytne hodně příležitostí k samostatným pohledům na jednotlivé situace.

Je-li dáno násobení v množině G, pak je zejména jednoznačně určen součin každého prvku $a \in G$ opět s prvkem a; místo aa píšeme někdy stručněji a^2.

11.2. Násobení komutativní (abelovské)

Násobení v množině G může mít 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 stát, že součin některého prvku a s některým prvkem b je různý od součinu prvku b s prvkem a, tj. $ab \neq ba$.

Jestliže pro některé dva prvky $a, b \in G$ platí rovnost $ab = ba$, pak se prvky a, b nazývají *vzájemně zaměnitelné* neboli *vzájemně komutativní*; jestliže každé dva prvky v G jsou vzájemně zaměnitelné, pak se násobení nazývá *komutativní* neboli *abelovské*.

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

11.3. Příklady násobení v množině

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

b) Nechť je n libovolné přirozené číslo a G nějaká množina skládající se z celých nezáporných 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 $b \in G$ je zbytek dělení čísla $a + b$ číslem n. Součin ab je tedy vždy jedno z čísel $0, \ldots, n - 1$. Toto násobení nazýváme *sečítání vzhledem k modulu n*; je zřejmé, že je rovněž abelovské.

c) Nechť je G množina všech permutací nějaké konečné množiny řádu n ($\geqq 1$) a násobení budiž definováno takto: Součin $\boldsymbol{p} \,.\, \boldsymbol{q}$ libovolného prvku $\boldsymbol{p} \in G$ s libovolným prvkem $\boldsymbol{q} \in G$ je složená permutace $\boldsymbol{qp}$. V tomto případě je tedy násobení skládání permutací. Z dřívějšího výkladu (**8.7.2**) víme, že nemusí být abelovské.

d) Nechť je G množina všech rozkladů nějaké množiny a násobení budiž definováno takto: Součin $\bar{A}, \bar{B}$ libovolného prvku $\bar{A} \in G$ s libovolným prvkem $\bar{B} \in G$ je rozklad $[\bar{A}, \bar{B}]$, popř. $(\bar{A}, \bar{B})$. Obě násobení jsou abelovská, jak plyne z **3.4** a **3.5**.

11.4. Multiplikační tabulka

1. *Popis multiplikační tabulky.* Když je množina G konečná a její prvky jsme označili např. písmeny $a, b, \ldots, m$, pak libovolné násobení v G můžeme popsat v tzv. *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 to zpravidla v témž pořadí, v prvním řádku odleva doprava a v prvním sloupci od shora dolů. Napravo od každého písmene x v prvním sloupci, a to 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 tolik sloupců, kolik má množina G prvků. Jsou-li písmena $a, b, \ldots, m$ v obou záhlavích napsána v témž pořádku, pak se násobení abelovské projeví v tabulce patrně tím, že tabulka je souměrná vzhledem k hlavní úhlopříčně, tj. v jejím libovolném j-tém řádku a v libovolném k-tém sloupci za oběma záhlavími je týž prvek jako v k-tém řádku a j-tým sloupci.

2. *Příklady multiplikačních tabulek.* Jako příklad uvedeme multiplikační tabulky pro násobení v množině G všech permutací nějaké množiny H, která se skládá z $n = 1, 2, 3$ prvků, přičemž násobení je skládání permutací, jak jsme je popsali v hořejším příkladě **11.3**c. Protože všech permutací množiny H, a tedy prvků množiny G, je $n! = 1, 2, 6$, mají tyto multiplikační tabulky, kromě obou záhlaví, $n! = 1, 2, 6$ řádků a týž počet sloupců.

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

	$\mathbf{e}$
$\mathbf{e}$	$\mathbf{e}$

Pro $n = 2$. 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 je identická permutace $\mathbf{e}$, druhou označíme např. $\boldsymbol{a}$. Permutace složené jsou: $\mathbf{ee} = \mathbf{e}$, $\boldsymbol{a}\mathbf{e} = \boldsymbol{a}$, $\mathbf{e}\boldsymbol{a} = \boldsymbol{a}$, $\boldsymbol{aa} = \mathbf{e}$, a odtud vychází tato multiplikační tabulka:

	$\mathbf{e}$	$\boldsymbol{a}$
$\mathbf{e}$	$\mathbf{e}$	$\boldsymbol{a}$
$\boldsymbol{a}$	$\boldsymbol{a}$	$\mathbf{e}$

Pro $n = 3$. 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 je identická permutace $\mathbf{e}$, ostatní označíme po pořádku $\mathbf{a}, \mathbf{b}, \mathbf{c}, \mathbf{d}, \mathbf{f}$. Permutace složené jsou:

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

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 jsme napsali v obou záhlavích symboly $\mathbf{e}, \mathbf{a}, \ldots, \mathbf{f}$ jednotlivých prvků množiny G v témž pořadí a vidíme, že v případech $n = 1, 2$ jsou hořejší tabulky souměrné vzhledem k hlavní úhlopříčně, kdežto v případě $n = 3$ je multiplikační tabulka nesouměrná. Odtud plyne, že naše násobení v množině G je v případech $n = 1, 2$ abelovské, ale v případě $n = 3$ abelovské není.

Příkladů násobení v množinách se dá uvést nepřehledné množství. Stačí vzít libovolnou abstraktní neprázdnou množinu G a ke každé posloupnosti prvků $a, b \in G$ jednoznačně přiřadit některý prvek v G. Když je množina G konečná, pak můžeme přiřazeni definovat 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 je multiplikační.

11.5. Cvičení

1. V množině všech euklidovských pohybů na přímce $\mathbf{f}[a]$ a rovněž v množině skládající se ze všech euklidovských pohybů na přímce, $\mathbf{f}[a]$, $\mathbf{g}[a]$ (**6.10.4**) můžeme definovat násobení skládáním pohybů, podobně jako v příkladě **11.3.c**). Podobný výsledek platí o množině všech euklidovských

pohybů v rovině $\mathbf{f}[\alpha; a, b]$ a o množině všech euklidovských pohybů v rovině $\mathbf{f}[\alpha; a, b]$, $\mathbf{g}[\alpha; a, b]$ (**6.10.5**).

2. V množině $2n$ permutací vrcholů pravidelného n-úhelníka v rovině ($n \geqq 3$), které jsme popsali ve cvič. **8.8**.4 můžeme definovat násobení skládáním permutací podobně jako v příkladě **11.3**.c). Sestavte pro toto násobení v případech $n = 4, 5, 6$ multiplikační tabulky.

3. V příkladě **11.3**.b se může množina G skládat právě jenom z čísel $0, \ldots, n - 1$. Sestavte pro tento případ, a to pro $n = 1, 2, 3, 4, 5$, multiplikační tabulky.

4. Když jsou přirozená čísla a, b menší nebo rovná nějakému přirozenému číslu $n \geqq 5$, pak počet prvočinitelů čísla $10a + b$ je $\leqq n$. Odtud plyne, že v množině G, která se skládá z čísel $1, 2, \ldots, n$, můžeme definovat násobení takto: Součin $a \,.\, b$ libovolného prvku $a \in G$ s libovolným prvkem $b \in G$ je počet prvočinitelů čísla $10a + b$. Přesvědčte se, že pro $n = 6$ je příslušná multiplikační tabulka 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 definovat násobení tím, že ke každé uspořádané dvojici podmnožin přiřadíme jejich součet. Můžeme násobení podobně definovat pomocí průniku?

6. Vymyslete sami příklady násobení v množinách.