3. kapitola. Množiny se dvěma operacemi

In: Karel Hruša (author): Polynomy v moderní algebře. (Czech). Praha: Mladá fronta, 1970. pp. 29–54.

Persistent URL: http://dml.cz/dmlcz/403714

3. kapitola

MNOŽINY SE DVĚMA OPERACEMI

Největší důležitost pro nás budou mít množiny, v nichž jsou definovány dvě operace. Jednu z těchto operací budeme nazývat sčítání a druhou násobení.

Definice 7. Nechť jsou v množině M definovány operace $\oplus$ a $\odot$, které mají tyto vlastnosti:

1. Pro každé $[x, y] \in M \times M$ existuje $x \oplus y \in M$ i $x \odot y \in M$.
2. Obě operace jsou komutativní a asociativní.
3. Operace $\odot$ je distributivní vzhledem k operaci $\oplus$.

Pak se operace $\oplus$ nazývá *sčítání* a operace $\odot$ se nazývá *násobení* v množině M.

Neutrální prvek sčítání se nazývá *nulový prvek* a neutrální prvek násobení se nazývá *jednotkový prvek*. Inverzní prvek sčítání se jmenuje *opačný prvek* a inverzní prvek násobení se jmenuje *převrácený prvek*.

Množina M, v níž je definováno sčítání a násobení, se nazývá *polookruh*.

Pro takto definované operace jsme zavedli symboly $\oplus$ a $\odot$, aby nám to připomínalo běžně užívané symboly $+$ a $.$ pro sčítání a násobení čísel. Uvedené operace však nemusí mít se sčítáním a násobením čísel nic společného.

Polookruh může být grupou vzhledem k sčítání $\oplus$, může být také grupou vzhledem k násobení $\odot$, ale nemusí tomu

tak být, protože nemusí obsahovat ani nulový prvek, ani jednotkový prvek a také ke každému prvku polookruhu nemusí existovat ani opačný prvek, ani převrácený prvek. O existenci těchto prvků se v definici 7 nic nepředpokládá.

Požadavky uvedené v definici 7 můžeme rozepsat takto: Pro každé $x \in \mathsf{M}$, pro každé $y \in \mathsf{M}$ a pro každé $z \in \mathsf{M}$ je

$$x \oplus y = y \oplus x, \qquad x \odot y = y \odot x,$$
$$(x \oplus y) \oplus z = x \oplus (y \oplus z), \qquad (x \odot y) \odot z = x \odot (y \odot z),$$
$$(x \oplus y) \odot z = (x \odot z) \oplus (y \odot z).$$

Pro úplnost můžeme poznamenat, že se v některých knihách komutativnost a asociativnost násobení nepředpokládá a pak se polookruh, v němž je násobení komutativní, označuje názvem komutativní polookruh a polookruh, v němž je násobení asociativní, názvem asociativní polookruh. My se však budeme zabývat pouze polookruhy, které jsou komutativní a asociativní, a nebudeme si proto zbytečně komplikovat názvosloví.

Příklad 12. Množina N_0 všech přirozených čísel (včetně nuly) s obyčejným sčítáním a násobením, jak je známe ze školy, je polookruh, neboť ke každé dvojici $[x, y] \in \mathsf{N}_0 \times \mathsf{N}_0$ jsou definována čísla $x + y \in \mathsf{N}_0$, $xy \in \mathsf{N}_0$ a pro libovolná čísla x, y, z množiny N_0 je

$$x + y = y + x, \qquad xy = yx,$$
$$(x + y) + z = x + (y + z), \qquad (xy)z = x(yz),$$
$$(x + y)z = xz + yz.$$

Nulovým prvkem je tu číslo 0 a jednotkovým prvkem je číslo 1, neboť pro každé $x \in \mathsf{N}_0$ je

$$x + 0 = 0 + x = x, \quad x.1 = 1.x = x.$$

Opačný prvek existuje pouze k číslu 0 a je jím zase číslo 0; převrácený prvek existuje pouze k číslu 1 a je jím zase

číslo 1. Také množina N všech přirozených čísel (bez nuly) je polookruh. Ten však nemá nulový prvek; jednotkovým prvkem je opět číslo 1. Rovněž množina S všech sudých přirozených čísel (bez nuly) je polookruh; v něm však neexistuje ani nulový, ani jednotkový prvek. Také množina C všech celých čísel, množina Q všech racionálních čísel, množina R všech reálných čísel a množina K všech komplexních čísel jsou polookruhy. Ve všech těchto polookruzích je nulovým prvkem číslo 0 a jednotkovým prvkem číslo 1.

Ukážeme si ještě dva příklady polookruhů, v nichž jsou operace $\oplus$ a $\odot$ definovány jinak než obvykle.

Příklad 13. Budiž L množina všech lichých kladných čísel. V množině L budeme definovat operace $\oplus$ a $\odot$ takto:

$$x \oplus y = x + y + 1, \quad x \odot y = \tfrac{1}{2}(x + 1)(y + 1) - 1.$$

Máme ukázat, že množina L s takto definovaným sčítáním a násobením je polookruh.

Ke každé dvojici $[x, y] \in \mathsf{L} \times \mathsf{L}$ přísluší čísla $x \oplus y$, $x \odot y$, která patří také do L. To je zřejmé, neboť součet $x + y$ dvou lichých čísel je sudé číslo a $x \oplus y = x + y + 1$ je tedy liché číslo; čísla $x + 1$, $y + 1$ jsou obě sudá, jejich součin je násobek čtyř a polovina tohoto součinu je násobek dvou, takže číslo $x \odot y = \frac{1}{2}(x + 1)(y + 1) - 1$ je liché. Jsou-li dále čísla x, y kladná, jsou i čísla $x \oplus y$, $x \odot y$ kladná a patří tedy do L.

Operace $\oplus$ a $\odot$ mají i další vlastnosti uvedené v definici 7.

a) Komutativnost: Platí

$$x \oplus y = x + y + 1, \quad y \oplus x = y + x + 1.$$

Odtud však je vidět, že pro každá dvě čísla x, y množiny L je $x \oplus y = y \oplus x$. Podobně

$$x \circ y = \tfrac{1}{2}(x+1)(y+1) - 1,$$
$$y \circ x = \tfrac{1}{2}(y+1)(x+1) - 1,$$

takže pro každá dvě čísla x, y množiny L je $x \circ y = y \circ x$.

b) Asociativnost: Platí

$$(x \oplus y) \oplus z = (x + y + 1) + z + 1,$$
$$x \oplus (y \oplus z) = x + (y + z + 1) + 1,$$

takže pro každá tři čísla x, y, z množiny L je $(x \oplus y) \oplus z = x \oplus (y \oplus z)$. Podobně

$$(x \circ y) \circ z = \tfrac{1}{2}\left(\tfrac{1}{2}(x+1)(y+1) - 1 + 1\right)(z+1) - 1,$$
$$x \circ (y \circ z) = \tfrac{1}{2}(x+1)\left(\tfrac{1}{2}(y+1)(z+1) - 1 + 1\right) - 1$$

a odtud po velmi snadné úpravě vyplývá, že pro každ tři čísla x, y, z množiny L je $(x \circ y) \circ z = x \circ (y \circ z)$.

c) Distributivnost operace $\circ$ vzhledem k operaci $\oplus$: Platí

$$(x \oplus y) \circ z = \tfrac{1}{2}(x + y + 1 + 1)(z+1) - 1,$$
$$(x \circ z) \oplus (y \circ z) = \tfrac{1}{2}(x+1)(z+1) - 1 + \tfrac{1}{2}(y+1)(z+1) - 1 + 1.$$

Lehko ověříme, že obě tato čísla jsou si rovna, takže pro každá tři čísla x, y, z množiny L je $(x \oplus y) \circ z = (x \circ z) \oplus (y \circ z)$.

Je tedy vskutku operace $\oplus$ sčítání a operace $\circ$ násobení v množině L. Podle naší definice je tedy např. $3 \oplus 5 = 9$, $5 \oplus 5 = 11$, $3 \circ 5 = 11$, $5 \circ 5 = 17$ atd.

Nulový prvek v polookruhu L neexistuje, neboť neexistuje takové $n \in \mathsf{L}$, aby pro všecka $x \in \mathsf{L}$ bylo $x \oplus n = x$, čili

$$x + n + 1 = x.$$

Jednotkovým prvkem polookruhu L je číslo 1, neboť podmínku $x \circ n = x$, neboli

$$\tfrac{1}{2}(x+1)(n+1) - 1 = x,$$

můžeme upravit na tvar

$$(x + 1)(n - 1) = 0,$$

což platí pro $n = 1$ a pro každé $x \in \mathsf{L}$.

Možná, že by čtenáře zajímalo, jaký rozumný smysl můžeme dát operacím $\oplus$ a $\odot$ v množině L. Poněvadž je číslo 1 jednotkový prvek polookruhu L, hraje číslo 1 v polookruhu L tutéž úlohu jako číslo 1 v polookruhu N všech přirozených čísel (bez nuly). Poněvadž dále $1 \oplus 1 = 1 + 1 + 1 = 3$, má číslo 3 v polookruhu L tutéž úlohu jako číslo $1 + 1 = 2$ v polookruhu N. Z toho, že $3 \oplus 1 = 3 + 1 + 1 = 5$, soudíme, že číslu $5 \in \mathsf{L}$ odpovídá číslo $2 + 1 = 3 \in \mathsf{N}$ atd. Matematickou indukcí se dá dokázat, že každé číslo $x = 2u - 1 \in \mathsf{L}$ odpovídá číslu $u \in \mathsf{N}$. Obdobně číslo $y = 2v - 1 \in \mathsf{L}$ odpovídá číslu $v \in \mathsf{N}$. Pak také číslo

$$x \oplus y = x + y + 1 = 2u - 1 + 2v - 1 + 1 = 2(u + v) - 1 \in \mathsf{L}$$

odpovídá číslu $u + v \in \mathsf{N}$ a číslo

$$x \odot y = \tfrac{1}{2}(x + 1)(y + 1) - 1 = \tfrac{1}{2}(2u - 1 + 1)(2v - 1 + 1) - 1 = 2uv - 1 \in \mathsf{L}$$

odpovídá číslu $uv \in \mathsf{N}$. Množina L tedy vznikne z množiny N pouhým přejmenováním prvků: místo $u \in \mathsf{N}$ píšeme $2u - 1 \in \mathsf{L}$. Obě množiny se liší pouze označením svých prvků. Kdyby se byl historický vývoj matematiky odehrál tak, že by se k zapisování přirozených čísel užívalo pouze znaků, jimiž dnes zapisujeme prvky množiny L, museli bychom počítat podle pravidel platných v polookruhu L. Pak by výpočty $3 \oplus 5 = 9$, $5 \oplus 5 = 11$, $3 \odot 5 = 11$, $5 \odot 5 = 17$ znamenaly totéž jako naše obvyklé výpočty $2 + 3 = 5$, $3 + 3 = 6$, $2.3 = 6$, $3.3 = 9$ atd. Nahlédneme to například z tabulky

N	1	2	3	4	5	6	7	8	9	10	...
L	1	3	5	7	9	11	13	15	17	19	...

v níž jsou pod sebou uvedeny ty prvky množin N a L, které si navzájem odpovídají. Podle ní můžeme každý výpočet v množině N „přeložit" do množiny L tak, že prvky množiny N nahradíme odpovídajícími prvky množiny L a operace $+$ a $\cdot$ v množině N operacemi $\oplus$ a $\odot$ v množině L. Má tedy výpočet $2 + 3 = 5$ v množině N týž význam jako výpočet $3 \oplus 5 = 9$ v množině L apod.

Úmluva. V dalším textu budeme zapisovat sčítání v polookruhu M znakem $+$ a násobení znakem $\cdot$ (popř. budeme znak násobení vůbec vynechávat). Nulový prvek budeme označovat znakem 0 a jednotkový prvek znakem 1. Opačný prvek k prvku a budeme označovat $-a$ a převrácený prvek k prvku a budeme označovat a^{-1}.

Tohoto označení budeme užívat i tehdy, nebude-li mít sčítání a násobení v polookruhu M nic společného se sčítáním a násobením čísel. Kdyby však mohlo nastat nedorozumění, vrátíme se k dosavadním znakům $\oplus$ a $\odot$.

Příklad 14. Budiž M množina skládající se z prvků 0, 1, tj. $M = \{0, 1\}$. V množině M budeme definovat sčítání a násobení takto:

$$0 + 0 = 0,\ 0 + 1 = 1 + 0 = 1 + 1 = 1,$$
$$0.0 = 0.1 = 1.0 = 0,\ 1.1 = 1.$$

Abychom mohli tvrdit, že množina M s takto definovaným sčítáním a násobením je polookruh, musíme ověřit, že jsou splněny všecky požadavky z definice 7.

Oba výkony jsou definovány pro všecky dvojice $[x,$

$y] \in \mathsf{M} \times \mathsf{M}$, jak je patrné z jejich zavedení. Také komutativnost sčítání i násobení odtud bezprostředně vyplývá. Asociativnost těchto operací ověříme tak, že vyšetříme postupně všecky případy, které mohou nastat:

$$(0 + 0) + 0 = 0 + 0 = 0, \quad 0 + (0 + 0) = 0 + 0 = 0,$$
$$(0 + 0) + 1 = 0 + 1 = 1, \quad 0 + (0 + 1) = 0 + 1 = 1,$$
$$(0 + 1) + 0 = 1 + 0 = 1, \quad 0 + (1 + 0) = 0 + 1 = 1,$$
$$(1 + 0) + 0 = 1 + 0 = 1, \quad 1 + (0 + 0) = 1 + 0 = 1,$$
$$(0 + 1) + 1 = 1 + 1 = 1, \quad 0 + (1 + 1) = 0 + 1 = 1,$$
$$(1 + 0) + 1 = 1 + 1 = 1, \quad 1 + (0 + 1) = 1 + 1 = 1,$$
$$(1 + 1) + 0 = 1 + 0 = 1, \quad 1 + (1 + 0) = 1 + 1 = 1,$$
$$(1 + 1) + 1 = 1 + 1 = 1, \quad 1 + (1 + 1) = 1 + 1 = 1.$$

Obdobně bychom ověřili i asociativnost násobení. Ještě je třeba ukázat, že násobení je distributivní vzhledem ke sčítání:

$$(0 + 0).0 = 0.0 = 0, \qquad 0.0 + 0.0 = 0 + 0 = 0,$$
$$(0 + 0).1 = 0.1 = 0, \qquad 0.1 + 0.1 = 0 + 0 = 0,$$
$$(0 + 1).0 = 1.0 = 0, \qquad 0.0 + 1.0 = 0 + 0 = 0,$$
$$(1 + 0).0 = 1.0 = 0, \qquad 1.0 + 0.0 = 0 + 0 = 0,$$
$$(0 + 1).1 = 1.1 = 1, \qquad 0.1 + 1.1 = 0 + 1 = 1,$$
$$(1 + 0).1 = 1.1 = 1, \qquad 1.1 + 0.1 = 1 + 0 = 1,$$
$$(1 + 1).0 = 1.0 = 0, \qquad 1.0 + 1.0 = 0 + 0 = 0,$$
$$(1 + 1).1 = 1.1 = 1, \qquad 1.1 + 1.1 = 1 + 1 = 1.$$

Uvedený postup jsme mohli poněkud zkrátit, neboť tu jde o komutativní operace a není třeba znovu provádět výpočty, které vzniknou pouhou záměnou prvků; úspora takto vzniklá však je jen nepatrná. To tedy znamená, že množina M je opravdu polookruh, v němž je operace $+$ sčítání a operace $.$ násobení. (Bylo by možné také ukázat, že v polookruhu M je sčítání distributivní vzhledem k násobení, ale to nás v tomto okamžiku nezajímá.)

Prvek 0 je nulovým prvkem polookruhu M, neboť

$$0 + 0 = 0, \quad 1 + 0 = 0 + 1 = 1,$$

a prvek 1 je jeho jednotkovým prvkem, protože

$$0.1 = 1.0 = 0, \quad 1.1 = 1.$$

Opačný prvek existuje pouze k prvku 0 a tímto opačným prvkem je zase prvek 0, neboť $0 + 0 = 0$, takže $-0 = 0$. Převrácený prvek existuje pouze k prvku 1 a tímto převráceným prvkem je zase prvek 1, neboť $1.1 = 1$, takže $1^{-1} = 1$. K prvku 1 neexistuje opačný prvek a k prvku 0 neexistuje převrácený prvek, protože neexistuje žádné $x \in M$ tak, aby $1 + x = 0$, popř. $0.x = 1$.

Čtenář se asi ptá, jaký smysl má toto podivné počítání. Označme Z nějakou množinu výroků (pravdivých i nepravdivých), která má tu vlastnost, že ke každým dvěma výrokům **A**, **B** z množiny Z patří do Z i jejich alternativa **A nebo B** a konjunkce **A a zároveň B**. Množinu Z můžeme rozložit do dvou tříd: do jedné, kterou označíme symbolem 0, zařadíme všecky nepravdivé výroky z množiny Z a do druhé, kterou označíme symbolem 1, zařadíme všecky pravdivé výroky z množiny Z. Označme dále $M = \{0, 1\}$. Patří-li výrok **A** do třídy $x \in M$ a výrok **B** do třídy $y \in M$, patří výrok **A nebo B** do třídy $x + y \in M$ a výrok **A a zároveň B** do třídy $xy \in M$. Uvedené definice sčítání a násobení v množině M nejsou nic jiného než pravidla známá z logiky:

Jsou-li dva výroky nepravdivé, je i jejich alternativa nepravdivá,
je-li aspoň jeden ze dvou výroků pravdivý, je jejich alternativa pravdivá;
je-li aspoň jeden ze dvou výroků nepravdivý, je jejich konjunkce nepravdivá,
jsou-li dva výroky pravdivé, je jejich konjunkce pravdivá.

Zavedené počítání nám dovoluje zcela mechanicky rozhodnout o pravdivosti či nepravdivosti každého výroku zce-

la libovolně složeného z alternativy a konjunkce výroků.

Ukažme si to na této úloze: Jednoho cestovatele zajali divoši a uvěznili ho v místnosti se dvěma východy pod dozorem dvou strážců. Náčelník kmene řekl zajatci: „Jeden východ vede na svobodu a druhý na smrt. Tvoji strážci vědí, kam který východ vede, a můžeš se jich na to zeptat. Smíš však položit jen jedinou otázku a jen jedinému z nich a nesmíš se ptát, co by řekl ten druhý. Ale upozorňuji tě, že jeden ze strážců mluví vždycky pravdu a druhý stále lže.“ Cestovatel chvíli přemýšlel, pak vyslovil otázku a na základě odpovědi, kterou dostal, spolehlivě rozhodl, který východ vede na svobodu. Jak zněla ta otázka?

Vžijme se do situace ubohého cestovatele. Zajímá ho pravdivost dvou výroků:

A: Tento východ vede na svobodu.
B: Ty mluvíš pravdu.

Z těchto výroků musí sestavit takový složený výrok **X**, aby kladná odpověď na otázku: „Je pravda, že **X**?“ znamenala, že výrok **A** je pravdivý, a aby záporná odpověď znamenala, že výrok **A** je nepravdivý, a to bez ohledu na pravdivost či nepravdivost výroku **B**. Sestaví-li všecky možnosti, které mohou nastat, do přehledné tabulky, dostane:

A	B	X*	X
1	1	1	1
1	0	1	0
0	1	0	0
0	0	0	1

Ve sloupcích označených **A**, **B** jsou zapsány pravdivostní třídy, do nichž patří výroky **A**, **B**, ve sloupci označeném **X*** je uvedena odpověď, kterou cestovatel dostane (znak 1 značí „ano", znak 0 značí „ne") a ve sloupci nadepsaném **X** je uvedena skutečná pravdivostní třída, do níž patří výrok **X**. Kromě výroků **A**, **B** zavedeme ještě dva další výroky, které jsou jejich negacemi:

A′: Tento východ vede na smrt.
B′: Ty lžeš.

Potom úloze vyhovuje tento výrok **X**:

(**A a zároveň B**) **nebo** (**A**′ **a zároveň B**′).

Označíme-li pravdivostní třídy výroků **A**, **B**, **A**′, **B**′, **X** po řadě písmeny a, b, a', b', x, pak

$$x = ab + a'b';$$

přitom pro $a = 1$ je $a' = 0$, pro $a = 0$ je $a' = 1$, pro $b = 1$ je $b' = 0$ a pro $b = 0$ je $b' = 1$. Lehko se přesvědčíme, že takto vypočtená třída x splňuje podmínky vyjádřené výše uvedenou tabulkou. Otázka, kterou cestovatel položí, zní tedy takto: „Je pravda, že tento východ vede na svobodu a ty přitom mluvíš pravdu nebo že vede na smrt a ty přitom lžeš?"*)

Podle věty 1 existuje v každém polookruhu M nejvýše jeden nulový prvek 0 a podle věty 2 existuje ke každému prvku $a \in \mathsf{M}$ nejvýše jeden opačný prvek $-a \in \mathsf{M}$. Mezi všemi polookruhy jsou nejdůležitější takové, v nichž existu-

*) Podmínku, že se nesmí ptát žádného ze strážců na to, co by řekl druhý strážce, položil náčelník cestovateli proto, aby mu zabránil položit otázku: „Co by mi odpověděl tvůj kamarád, kdybych se ho zeptal, vede-li tento východ na svobodu?" Odpověď na tuto otázku totiž vyjadřuje negaci skutečného stavu bez ohledu na to, kterému strážci byla položena, neboť jeden z nich — lhostejno který — mluví pravdu a druhý lže.

je právě jeden nulový prvek a v nichž ke každému prvku existuje právě jeden opačný prvek, tj. polookruhy, které jsou vzhledem ke sčítání (komutativními) grupami.

Definice 8. Polookruh M, který je (komutativní) grupou vzhledem k sčítání, se nazývá *okruh*. Tato grupa se jmenuje *aditivní grupa okruhu* M.

Podle věty 3 existuje ke každým dvěma prvkům a, b okruhu M právě jeden prvek $x \in M$, pro který platí

$$a + x = b$$

a v důsledku komutativnosti sčítání také $x + a = b$. Tento prvek můžeme podle téže věty vyjádřit v tvaru

$$x = b + (-a),$$

kde $-a$ je opačný prvek k prvku a.

Definice 9. Prvek x, pro který platí

$$a + x = b,$$

označujeme názvem *rozdíl* prvků b, a (v tomto pořádku) a píšeme $x = b - a$.

Operace, která k prvkům b, a množiny M přiřazuje nejvýše jeden rozdíl $b - a \in M$, nazývá se *odčítání*.

Z věty 3 tedy vyplývá, že ke každým dvěma prvkům b, a okruhu M existuje jediný rozdíl $b - a \in M$ a že

$$b - a = b + (-a),$$

takže rozdíl prvků b, a můžeme nahradit součtem prvku b a opačného prvku $-a$. Je-li $b = 0$, plyne odtud

$$0 - a = 0 + (-a) = -a;$$

můžeme tedy opačný prvek $-a$ považovat za rozdíl $0 - a$. Je-li $b = a$, pak

$$a - a = a + (-a) = 0;$$

rozdílem dvou sobě rovných prvků tedy je nulový prvek 0.

Na základě věty 4 můžeme říci toto: Existuje-li ke každým dvěma prvkům b, a polookruhu M i rozdíl $b - a \in \mathsf{M}$, pak polookruh M je okruh, tj. je to grupa vzhledem k sčítání.

Jestliže polookruh není okruh, může se stát, že k některým jeho prvkům b, a rozdíl $b - a$ neexistuje, popř. není určen jednoznačně.

Příklad 15. Množina C všech celých čísel je okruh, neboť ke každým dvěma jeho prvkům b, a existuje rozdíl $b - a \in \mathsf{C}$. Tento rozdíl je jediný a platí

$$b - a = b + (-a).$$

Obdobné tvrzení můžeme vyslovit i o množině Q všech racionálních čísel, o množině R všech reálných čísel i o množině K všech komplexních čísel. Naproti tomu množina N_0 všech přirozených čísel (včetně nuly) není okruh a v něm existuje rozdíl $b - a$ pouze tehdy, je-li $b \geqq a$, ale v případě $b < a$ rozdíl $b - a$ neexistuje. Ani množina $\mathsf{M} = \{0, 1\}$ z příkladu 14 není okruh; je sice $0 - 0 = 0$, $1 - 0 = 1$, ale rozdíl $0 - 1$ neexistuje, protože neexistuje žádné $x \in \mathsf{M}$, pro které by bylo $1 + x = 0$, a rozdíl $1 - 1$ není v množině M určen jednoznačně, protože podmínku $1 + x = 1$ splňuje $x = 0$ i $x = 1$.

Věta 5. Pro každý prvek x okruhu M platí

$$0.x = 0;$$

přitom 0 je nulový prvek okruhu M.

Důkaz. Zvolme některý prvek $a \in M$. Podle definice nulového prvku je

$$a + 0 = a.$$

Odtud na základě distributivnosti násobení vzhledem k sčítání vyplývá, že pro každé $x \in M$ je

$$ax = (a + 0)x = ax + 0.x,$$

takže

$$0.x = ax - ax = 0.$$

To tedy znamená, že součin dvou prvků okruhu M, z nichž aspoň jeden je nulový, je roven tomuto nulovému prvku. Nesmíme se však nechat svést k ukvapenému závěru, že také obráceně z rovnosti

$$xy = 0$$

vyplývá, že musí být buď $x = 0$, nebo $y = 0$. Existují okruhy, v nichž $xy = 0$ přesto, že $x \neq 0$ i $y \neq 0$. Dříve však, než uvedeme příklad takového okruhu, vyslovíme definici:

Definice 10. Prvky $x \neq 0, y \neq 0$, pro něž je

$$xy = 0,$$

nazývají se *dělitelé nuly*.

Příklad 16. Budiž C množina všech celých čísel a $m > 1$ přirozené číslo, které budeme nazývat *modul*. Dělíme-li libovolné číslo $x \in C$ modulem m, dostaneme neúplný podíl q a zbytek r, přičemž

$$x = mq + r, \quad 0 \leqq r < m,$$

kde q, r jsou čísla z množiny C. Uvedenými podmínkami jsou čísla q, r stanovena jednoznačně. Všech možných zbytků je celkem m; jsou to čísla

$$0, 1, 2, 3, \ldots, m - 1.$$

Všecka celá čísla, která při dělení modulem m dávají týž zbytek r, tvoří množinu, kterou budeme nazývat *zbytková třída podle modulu m*. Všech zbytkových tříd podle modulu m je právě tolik, kolik je různých zbytků, tj. m, a každé celé číslo patří právě do jedné z nich. Zbytkovou třídu, do níž patří číslo x, budeme označovat $\{x\}$; tento symbol znamená množinu všech celých čísel, která při dělení modulem m dávají týž zbytek jako číslo x. Dává-li číslo x při dělení modulem m zbytek r, pak čísla x_1, x_2 patří do třídy $\{x\}$ právě tehdy, existují-li taková celá čísla q_1, q_2, že

$$x_1 = mq_1 + r, \; x_2 = mq_2 + r,$$

a to nastane právě tehdy, když

$$x_1 - x_2 = m(q_1 - q_2) = mq,$$

kde q je celé číslo, čili když je jejich rozdíl násobkem modulu m.

Vezmeme-li nyní dvě zbytkové třídy $\{x\}$, $\{y\}$ a zvolíme-li libovolná čísla $x_1 \in \{x\}$, $x_2 \in \{x\}$, $y_1 \in \{y\}$, $y_2 \in \{y\}$, pak podle toho, co už víme, jsou rozdíly $x_1 - x_2$, $y_1 - y_2$ násobky modulu m, tj.

$$x_1 - x_2 = mq, \; y_1 - y_2 = mq',$$

kde q, q' jsou vhodná celá čísla. Odtud vychází

$$(x_1 + y_1) - (x_2 + y_2) = (x_1 - x_2) + (y_1 - y_2) = \\ = mq + mq' = m(q + q'),$$

takže čísla $x_1 + y_1$, $x_2 + y_2$ patří také do téže zbytkové třídy podle modulu m. Podobně dostaneme

$$(x_1 - y_1) - (x_2 - y_2) = (x_1 - x_2) - (y_1 - y_2) = \\ = mq - mq' = m(q - q'),$$

a proto i čísla $x_1 - y_1$, $x_2 - y_2$ patří do téže zbytkové třídy podle modulu m. A konečně

$$x_1y_1 - x_2y_2 = (x_1 - x_2)y_1 + x_2(y_1 - y_2) =$$
$$= mqy_1 + x_2mq' = m(qy_1 + q'x_2),$$

a to znamená, že čísla x_1y_1, x_2y_2 patří rovněž do téže zbytkové třídy podle modulu m.

Odtud plyne: Zvolíme-li zbytkové třídy $\{x\}$, $\{y\}$ a vybereme-li zcela libovolně v každé z těchto tříd po jednom čísle, pak zbytkové třídy, do nichž patří součet, rozdíl a součin těchto vybraných čísel, závisí jen na volbě zbytkových tříd $\{x\}$, $\{y\}$ a nezávisí na tom, která čísla z tříd $\{x\}$, $\{y\}$ jsme zvolili k výpočtu. Součty $x_1 + y_1$, $x_2 + y_2$ patří ovšem do téže třídy jako součet $x + y$, tj. do třídy $\{x + y\}$, a podobná tvrzení platí i o rozdílu a součinu.

To nám umožní definovat v množině C_m všech zbytkových tříd podle modulu m operace takto:

$\{x\} + \{y\} = \{x + y\}$, $\{x\} - \{y\} = \{x - y\}$, $\{x\}\{y\} = \{xy\}$.

Můžeme říci, že součtem zbytkových tříd $\{x\}$, $\{y\}$ podle modulu m rozumíme tu zbytkovou třídu podle modulu m, do níž patří součet $x + y$, a podobně můžeme interpretovat i další napsané definice operací. Sčítání a násobení tříd má vlastnosti požadované v definici 7, jak se dá snadno ověřit. To tedy znamená, že množina C_m s uvedeným sčítáním a násobením je polookruh. Poněvadž dále ke každým dvěma zbytkovým třídám podle modulu m existuje i jejich rozdíl, je množina C_m s uvedenými operacemi dokonce okruh; říkáme mu *okruh zbytkových tříd podle modulu m.*

Nulovým prvkem je třída $\{0\}$, neboť pro každou třídu $\{x\}$ je

$$\{x\} + \{0\} = \{x + 0\} = \{x\}.$$

Všimněme si nyní dělitelů nuly, tj. ptejme se, za jakých podmínek může v okruhu C_m být

$$\{x\}\{y\} = \{0\}.$$

To lze přepsat v tvaru

$$\{xy\} = \{0\},$$

který říká, že číslo xy musí patřit do třídy $\{0\}$, tj. musí dávat při dělení modulem m zbytek 0 a musí tedy být násobkem modulu m, takže

$$xy = mq,$$

kde q je vhodné celé číslo. Mohou nastat dva případy:

a) Je-li m prvočíslo, pak aspoň jedno z čísel x, y musí být násobkem čísla m,*) a to znamená, že buď $\{x\} = \{0\}$, nebo $\{y\} = \{0\}$.V okruhu zbytkových tříd podle prvočíselného modulu tedy neexistují dělitelé nuly.

b) Je-li však m složené číslo, tj. je-li $m = m_1 m_2$, kde $1 < m_1 < m$, $1 < m_2 < m$, může se stát, že číslo x je násobkem čísla m_1 a číslo y násobkem čísla m_2 a žádné z nich není násobkem modulu m. Pak $\{x\} \neq \{0\}$, $\{y\} \neq \{0\}$, a přitom $\{x\}\{y\} = \{0\}$, takže obě třídy jsou děliteli nuly.

Okruh C_2 zbytkových tříd podle modulu 2 obsahuje dvě třídy $\{0\}$, $\{1\}$. Třídu $\{0\}$ tvoří všecka sudá čísla a třídu $\{1\}$ všecka lichá čísla. Sčítání a násobení v okruhu C_2 je definováno takto:

$$\{0\} + \{0\} = \{0\},\ \{0\} + \{1\} = \{1\} + \{0\} = \{1\},$$

$$\{1\} + \{1\} = \{0\},$$

$$\{0\}\{0\} = \{0\}\{1\} = \{1\}\{0\} = \{0\},\ \{1\}\{1\} = \{1\}.$$

Tyto rovnosti ovšem neznamenají nic jiného než známá pravidla: Součet dvou sudých čísel je sudé číslo, součet dvou čísel, z nichž jedno je sudé a druhé liché, je liché číslo atd. Poněvadž je číslo 2 prvočíslo, neexistují v okruhu C_2 dělitelé nuly. Prvek $\{0\}$ je nulovým prvkem a prvek $\{1\}$ jednotkovým prvkem okruhu C_2, takže $-\{0\} = \{0\}$, $-\{1\} = \{1\}$, $\{1\}^{-1} = \{1\}$, ale převrácený prvek k prvku $\{0\}$ neexistuje.

*) Používáme tu známé věty: je-li součin xy dvou celých čísel násobkem prvočísla m, pak aspoň jedno z čísel x, y je násobkem prvočísla m, tj. buď $x = mq_1$, nebo $y = mq_2$, kde q_1, q_2 jsou celá čísla.

Ukážeme ještě příklad okruhu C_6 zbytkových tříd podle modulu 6. Tento okruh má šest prvků, jejichž sčítání a násobení je dáno následujícími tabulkami.

$\{x\} + \{y\}$

$\{x\}$ \ $\{y\}$	{0}	{1}	{2}	{3}	{4}	{5}
{0}	{0}	{1}	{2}	{3}	{4}	{5}
{1}	{1}	{2}	{3}	{4}	{5}	{0}
{2}	{2}	{3}	{4}	{5}	{0}	{1}
{3}	{3}	{4}	{5}	{0}	{1}	{2}
{4}	{4}	{5}	{0}	{1}	{2}	{3}
{5}	{5}	{0}	{1}	{2}	{3}	{4}

$\{x\}\{y\}$

$\{x\}$ \ $\{y\}$	{0}	{1}	{2}	{3}	{4}	{5}
{0}	{0}	{0}	{0}	{0}	{0}	{0}
{1}	{0}	{1}	{2}	{3}	{4}	{5}
{2}	{0}	{2}	{4}	{0}	{2}	{4}
{3}	{0}	{3}	{0}	{3}	{0}	{3}
{4}	{0}	{4}	{2}	{0}	{4}	{2}
{5}	{0}	{5}	{4}	{3}	{2}	{1}

Odtud je vidět, že v okruhu C_6 zbytkových tříd podle modulu 6 je $\{2\}\{3\} = \{0\}$, $\{3\}\{4\} = \{0\}$, takže třídy $\{2\}$, $\{3\}$, $\{4\}$ jsou dělitelé nuly v tomto okruhu. Také v okruhu C_6 je prvek $\{0\}$ nulovým prvkem a prvek $\{1\}$ jednotkovým prvkem; proto $-\{0\} = \{0\}$, $-\{1\} = \{5\}$, $-\{2\} = \{4\}$, $-\{3\} = \{3\}$, $-\{4\} = \{2\}$, $-\{5\} = \{1\}$, $\{1\}^{-1} = \{1\}$, $\{5\}^{-1} = \{5\}$ a převrácené prvky k prvkům $\{0\}$, $\{2\}$, $\{3\}$, $\{4\}$ neexistují. Z toho je vidět, že v okruhu může podmínku $a = -a$ splňovat i jiný prvek než nulový a podmínku $a = a^{-1}$ i jiný prvek než jednotkový.

Příklad 17. Máme zjistit, pro která celá čísla n je číslo $3n^2 + 2n + 7$ násobkem pěti. Úlohu můžeme formulovat tak, že se ptáme, je-li možné, aby číslo $3n^2 + 2n + 7$ patřilo do zbytkové třídy $\{0\}$ podle modulu 5, čili aby $\{3n^2 + 2n + 7\} = \{0\}$. Podle pravidel o počítání v okruhu C_5 zbytkových tříd podle modulu 5 je

$$\{3n^2 + 2n + 7\} = \{3\}\{n\}^2 + \{2\}\{n\} + \{2\}.$$

Dosadíme-li sem za $\{n\}$ postupně všecky zbytkové třídy podle modulu 5, dostaneme

$$\{3\}\{0\}^2 + \{2\}\{0\} + \{2\} = \{0\} + \{0\} + \{2\} = \{2\},$$
$$\{3\}\{1\}^2 + \{2\}\{1\} + \{2\} = \{3\} + \{2\} + \{2\} = \{2\},$$
$$\{3\}\{2\}^2 + \{2\}\{2\} + \{2\} = \{2\} + \{4\} + \{2\} = \{3\},$$
$$\{3\}\{3\}^2 + \{2\}\{3\} + \{2\} = \{2\} + \{1\} + \{2\} = \{0\},$$
$$\{3\}\{4\}^2 + \{2\}\{4\} + \{2\} = \{3\} + \{3\} + \{2\} = \{3\}.$$

Odtud je vidět, že úlohu řeší všecka celá čísla $n \in \{3\}$, tj. všecka čísla $n = 5k + 3$, kde k je celé číslo.

Příklad 18. Značí-li písmeno n libovolné celé číslo, máme dokázat, že z čísel $n^3 - 1$, n^3, $n^3 + 1$ je právě jedno násobkem sedmi. Budeme vyšetřovat, do které zbytkové třídy podle modulu 7 patří čísla $n^3 - 1$, n^3, $n^3 + 1$. Poněvadž

$$\{n^3 - 1\} = \{n\}^3 - \{1\}, \{n^3\} = \{n\}^3, \{n^3 + 1\} = \{n\}^3 + \{1\},$$

stačí za $\{n\}$ brát postupně všecky zbytkové třídy podle modulu 7:

$$\{0\}^3 = \{0\}, \{0\}^3 - \{1\} = \{6\}, \{0\}^3 + \{1\} = \{1\},$$
$$\{1\}^3 = \{1\}, \{1\}^3 - \{1\} = \{0\}, \{1\}^3 + \{1\} = \{2\},$$
$$\{2\}^3 = \{1\}, \{2\}^3 - \{1\} = \{0\}, \{2\}^3 + \{1\} = \{2\},$$
$$\{3\}^3 = \{6\}, \{3\}^3 - \{1\} = \{5\}, \{3\}^3 + \{1\} = \{0\},$$
$$\{4\}^3 = \{1\}, \{4\}^3 - \{1\} = \{0\}, \{4\}^3 + \{1\} = \{2\},$$
$$\{5\}^3 = \{6\}, \{5\}^3 - \{1\} = \{5\}, \{5\}^3 + \{1\} = \{0\},$$
$$\{6\}^3 = \{6\}, \{6\}^3 - \{1\} = \{5\}, \{6\}^3 + \{1\} = \{0\}.$$

Patří-li tedy číslo n do zbytkové třídy $\{0\}$, je číslo n^3 násobkem sedmi; patří-li číslo n do některé ze zbytkových tříd $\{1\}$, $\{2\}$, $\{4\}$, je číslo $n^3 - 1$ násobkem sedmi; patří-li číslo n do některé ze zbytkových tříd $\{3\}$, $\{5\}$, $\{6\}$, je číslo $n^3 + 1$ násobkem sedmi.

Definice 11. Okruh, v němž neexistují dělitelé nuly, se nazývá *obor integrity*.

Příklad 19. Množina C všech celých čísel, množina Q všech racionálních čísel, množina R všech reálných čísel i množina K všech komplexních čísel jsou obory integrity, neboť jsou to okruhy, v nichž je podmínka $xy = 0$ splněna jen tehdy, když buď $x = 0$, nebo $y = 0$. Množina S všech sudých čísel (kladných, záporných i nuly) je rovněž obor integrity. Také každý okruh C_p zbytkových tříd podle prvočíselného modulu p je obor integrity. Oborem integrity není například množina N_0 všech přirozených čísel (včetně nuly), neboť to není okruh, nebo okruh C_m zbytkových tříd podle složeného modulu m, neboť v něm existují dělitelé nuly.

V oboru integrity platí tato věta:

Věta 6. Jsou-li x, y prvky oboru integrity a je-li $a \neq 0$, pak z rovnosti

$$ax = ay$$

vyplývá rovnost

$$x = y.$$

Důkaz. Rovnost $ax = ay$ můžeme přepsat v tvaru $ax - ay = 0$ a tu zase podle cvič. 22e) na str. 52 v tvaru $a(x - y) = 0$. Poněvadž jde o obor integrity, v němž neexistují dělitelé nuly, a poněvadž podle předpokladu je $a \neq 0$, musí být $x - y = 0$, čili $x = y$.

Věta 6 neplatí v okruhu, který není oborem integrity, neboť tam se může stát, že prvek a je dělitelem nuly, a pak může být $a(x - y) = 0$, i když $x - y \neq 0$.

Větu 6 často formulujeme v tvaru: V oboru integrity lze rovnost „krátit" nenulovým prvkem tohoto oboru integrity.

Vraťme se však zase k polookruhům. Podle věty 1 existuje v každém polookruhu M nejvýše jeden jednotkový prvek 1 a podle věty 2 existuje ke každému $a \in M$ nejvýše jeden převrácený prvek $a^{-1} \in M$. Zvláštní pozornost si zasluhují polookruhy, v nichž existuje právě jeden jednotkový prvek a v nichž ke každému nenulovému prvku existuje právě jeden převrácený prvek, tj. polookruhy, jejichž nenulové prvky tvoří vzhledem k násobení (komutativní) grupu. Přitom ovšem do pojmu polookruhu zahrnujeme i okruhy.

Definice 12. Tvoří-li všecky nenulové prvky polookruhu M (komutativní) grupu M′ vzhledem k násobení, nazývá se tato grupa *multiplikativní grupa polookruhu* M. Okruh, jehož nenulové prvky tvoří multiplikativní grupu, nazývá se *těleso*.

Multiplikativní grupu polookruhu M budeme označovat M'.

Podle věty 3 existuje ke každým dvěma prvkům a, b multiplikativní grupy M' polookruhu M právě jeden prvek $x \in M'$, pro který platí

$$ax = b$$

a v důsledku komutativnosti násobení také

$$xa = b.$$

Tento prvek můžeme podle téže věty vyjádřit v tvaru

$$x = ba^{-1},$$

kde a^{-1} je převrácený prvek k prvku a.

Definice 13. Prvek x, pro který platí

$$ax = b,$$

označujeme názvem *podíl* prvků b, a (v tomto pořádku) a píšeme

$$x = \frac{b}{a} \text{ nebo také } x = b : a.$$

Operace, která k prvkům b, a polookruhu M přiřazuje nejvýše jeden podíl $\frac{b}{a} \in M$, nazývá se *dělení*.

Z věty 3 tedy vyplývá, že ke každým dvěma prvkům b, a multiplikativní grupy M' polookruhu M existuje jediný podíl $\frac{b}{a} \in M'$ a že

$$\frac{b}{a} = ba^{-1},$$

takže podíl prvků b, a můžeme nahradit součinem prvku b a převráceného prvku a^{-1}. Je-li $b = 1$, plyne odtud

$$\frac{1}{a} = 1.a^{-1} = a^{-1};$$

můžeme tedy převrácený prvek a^{-1} považovat za podíl $\frac{1}{a}$. Je-li $b = a$, pak

$$\frac{a}{a} = a.a^{-1} = 1;$$

podílem dvou sobě rovných prvků tedy je jednotkový prvek 1.

Je-li M obor integrity a je-li $b = 0$, pak pro každé $a \neq 0$ je $\frac{0}{a} = 0$, neboť podmínku $ax = 0$ v oboru integrity splňuje jediný prvek $x = 0$. Avšak i v mnohých polookruzích, které nejsou obory integrity, je $\frac{0}{a} = 0$ pro každé $a \neq 0$. Naproti tomu pro $a = 0$ podíl $\frac{b}{0}$ nedefinujeme v žádném polookruhu pro žádné b.

Je-li M těleso, pak z předcházejících úvah vyplývá, že v něm existuje podíl $\frac{b}{a}$ kterýchkoli dvou prvků b, $a \neq 0$. Je-li $a = 0$, podíl $\frac{b}{a}$ neexistuje.

Na základě věty 4 můžeme říci toto: Existuje-li ke každým dvěma prvkům b, $a \neq 0$, polookruhu M podíl $\frac{b}{a}$, pak nenulové prvky polookruhu M tvoří multiplikativní grupu, a je-li M okruh, je to těleso. Každé těleso tedy obsahuje dvě grupy: jednak aditivní grupu, kterou tvoří

všecky jeho prvky bez výjimky, jednak multiplikativní grupu, kterou tvoří všecky jeho nenulové prvky. Každé těleso T obsahuje nulový prvek 0 a jednotkový prvek 1, přičemž $0 \neq 1$; kdyby bylo $0 = 1$, pak by pro každé $x \in T$ bylo $x = x.1 = x.0 = 0$ a multiplikativní grupa by neexistovala, neboť těleso T by v tomto případě obsahovalo jediný prvek 0 a po jeho vynechání bychom dostali prázdnou množinu, která však nemůže být grupou.

Příklad 20. Množina Q všech racionálních čísel, množina R všech reálných čísel i množina K všech komplexních čísel s obvykle definovaným sčítáním a násobením jsou tělesa, neboť jsou to aditivní grupy a všechny jejich nenulové prvky tvoří multiplikativní grupu. Množiny Q' všech nenulových racionálních čísel, R' všech nenulových reálných čísel a K' všech nenulových komplexních čísel nejsou tělesa; jsou to sice multiplikativní grupy, ale nejsou to aditivní grupy, neboť v nich chybí nulový prvek 0. Totéž platí i o množině Q^+ všech kladných racionálních čísel a o množině R^+ všech kladných (reálných) čísel. Množina C všech celých čísel rovněž není těleso; je to sice aditivní grupa, ale po vynechání nulového prvku z ní nevznikne multiplikativní grupa. Množina C_7 všech zbytkových tříd pole modulu 7 je těleso, neboť je to aditivní grupa a vynecháním nulového prvku $\{0\}$ vznikne multiplikativní grupa (viz cvič. 27 na str. 53). Totéž platí pro každou množinu C_p všech zbytkových tříd podle prvočíselného modulu p. Naproti tomu množina C_8 všech zbytkových tříd podle modulu 8 není těleso, neboť po vynechání nulového prvku $\{0\}$ nevznikne multiplikativní grupa (viz cvič. 28 na str. 53). Totéž platí o každé množině C_m zbytkových tříd podle složeného modulu m.

Věta 7. V tělese neexistují dělitelé nuly.

Důkaz. Nechť pro prvky x, y tělesa T je

$$xy = 0,$$

kde 0 je nulový prvek. Je-li $y = 0$, nejsou prvky x, y dělitelé nuly. Je-li $y \neq 0$, existuje k němu převrácený prvek y^{-1}. Pak

$$x = x.1 = x(yy^{-1}) = (xy)y^{-1} = 0.y^{-1} = 0,$$

takže x, y nejsou dělitelé nuly ani v tomto případě.

To však znamená, že každé těleso je také oborem integrity a že tedy okruh, který není oborem integrity, nemůže být tělesem.

Cvičení. 21. Za předpokladu, že existují napsané symboly, dokažte následující rovnosti pro prvky x, y libovolného polookruhu:

$$\text{a) } -(x+y) = (-x) + (-y),$$

$$\text{b) } -(x-y) = (-x) + y,$$

$$\text{c) } x(-y) = (-x)y = -(xy), \quad \text{d) } (-x)(-y) = xy.$$

22. Za předpokladu, že jsou jednoznačně definovány napsané symboly, dokažte následující rovnosti pro prvky x, y, z libovolného polookruhu:

$$\text{a) } (x+y) - z = x + (y-z),$$

$$\text{b) } x - (y+z) = (x-y) - z,$$

$$\text{c) } x - (y-z) = (x-y) + z,$$

$$\text{d) } (x+z) - (y+z) = x - y, \quad \text{e) } x(y-z) = xy - xz.$$

23. Za předpokladu, že existují napsané symboly, dokažte následující rovnosti pro prvky x, y libovolného polookruhu:

$$\text{a) } (xy)^{-1} = x^{-1}y^{-1}, \quad \text{b) } (x:y)^{-1} = x^{-1}y, \quad \text{c) } (-x):y = x:(-y) = -(x:y), \quad \text{d) } (-x):(-y) = x:y.$$

24. Za předpokladu, že jsou jednoznačně definovány napsané symboly, dokažte následující rovnosti pro prvky x, y, z libovolného polookruhu:

a) $(xy) : z = x.(y : z)$, b) $x : (yz) = (x : y) : z$,

c) $x : (y : z) = (x : y).z$, d) $(xz) : (yz) = x : y$.

25. Za předpokladu, že jsou jednoznačně definovány napsané symboly, dokažte následující rovnosti pro prvky x, y, u, v libovolného polookruhu:

a) $\frac{x}{u} = \frac{y}{v}$, právě když $vx = uy$, b) $\frac{x}{u} + \frac{y}{v} = \frac{vx + uy}{uv}$,

c) $\frac{x}{u} - \frac{y}{v} = \frac{vx - uy}{uv}$, d) $\frac{x}{u}.\frac{y}{v} = \frac{xy}{uv}$, e) $\frac{x}{u} : \frac{y}{v} = \frac{x}{u}.\frac{v}{y} = \frac{vx}{uy}$.

26. Ověřte, že operace definované vzorci $\{x\} + \{y\} = \{x + y\}$, $\{x\} - \{y\} = \{x - y\}$, $\{x\}\{y\} = \{xy\}$ v množině C_m všech zbytkových tříd podle modulu m (viz str. 43) jsou opravdu sčítání, odčítání a násobení.

27. V tělese C_7 zbytkových tříd podle modulu 7 najděte a) nulový prvek, b) jednotkový prvek, c) ke každému prvku opačný prvek, d) ke každému nenulovému prvku převrácený prvek a ověřte tak, že C_7 je těleso.

28. Pokuste se o totéž v okruhu C_8 zbytkových tříd podle modulu 8 a ukažte, že C_8 není těleso.

29. Dokažte, že číslo $n^2 + n + 2$ není pro žádné celé číslo n násobkem patnácti.

30. Nechť množina M je komutativní grupa vzhledem k operaci $\oplus$ (sčítání). Definujeme-li v množině M další operaci $\odot$ vzorcem $x \odot y = 0$ pro každé $x \in M$ a pro každé $y \in M$, je operace $\odot$ násobení. Dokažte.

31. V intervalu $N = \langle 0, 10 \rangle$ jsou dány operace max (sčítání) a min (násobení) — viz cvič. 8 na str. 14. Najděte nulový a jednotkový prvek tohoto polookruhu. Je tento polookruh okruhem?

32. V množině M všech podmnožin množiny Z jsou dány operace $\cup$ (sčítání) a $\cap$ (násobení) — viz cvič. 9 na str. 14. Najděte nulový a jednotkový prvek tohoto polookruhu. Je polookruh M okruhem?

33. V množině N všech přirozených čísel (bez nuly) jsou dány operace: největší společný dělitel (sčítání) a nejmenší společný násobek (násobení) — viz cvič. 10 na str. 14. Vyšetřte existenci nulového a jednotkového prvku tohoto polookruhu.

34. V množině C všech celých čísel jsou dány operace $\oplus$ (sčítání) a $\odot$ (násobení) vzorci: $x \oplus y = x + y + 1$, $x \odot y = xy + x + y$. Ukažte, že množina C s takto definovanými operacemi je obor intengrity. Najděte jeho nulový a jednotkový prvek.

35. Opakujte cvič. 34 pro množinu Q všech racionálních čísel a pro operace $\oplus$ a $\odot$ dané vzorci: $x \oplus y = x + y - 1$, $x \odot y = x + y - xy$. Je množina Q s operacemi $\oplus$ a $\odot$ těleso? Který je jeho nulový a jednotkový prvek?

36. Jak je třeba definovat sčítání a násobení v množině M, která má právě dva různé prvky, aby vznikl obor integrity s jednotkovým prvkem? Je tento obor integrity těleso?

37. Jak je třeba definovat sčítání a násobení v množině M, která má právě tři různé prvky, aby vznikl obor integrity s jednotkovým prvkem? Je tento obor integrity těleso?

38. Řešte obdobnou úlohu pro množinu M, která má právě čtyři navzájem různé prvky.

39. Ukažte, že jednoprvková množina $M = \{0\}$, v níž je definováno sčítání $0 + 0 = 0$ a násobení $0.0 = 0$, je obor integrity. Proč to není těleso?

40. Jsou-li a, b racionální čísla, pak množina M všech čísel tvaru $a + b\sqrt{2}$, v níž je definováno sčítání a násobení obvyklým způsobem, je těleso. Dokažte.