KAPITOLA XII

OKRUHY

§ 1. Ideály. Faktorové okruhy

V této kapitole budeme studovat vlastnosti algebraických struktur se dvěma binárními operacemi, zejména okruhů. Navážeme na pojmy zavedené v kapitole II, ve druhé části paragrafu 4 a budeme postupovat obdobně jako v kapitole X při vyšetřování vlastností grup.

Při studiu grup hrají významnou úlohu normální podgrupy, které nám umožňují jednak vytvářet nové grupy — faktorové grupy, jednak charakterizovat všechny homomorfní obrazy grup. V obdobné roli vystupují v teorii okruhů takzvané ideály. Tak jako normální podgrupy jsou speciálními případy podgrup, jsou rovněž ideály jisté podokruhy daného okruhu. Na rozdíl od grup se však při vyšetřování ideálů omezíme — pokud nebude výslovně stanoven opak — na okruhy komutativní.

Definice. *Nechť $(O, +, \cdot)$ je okruh. Podokruh $A \subseteq O$ se nazývá* ideál *v okruhu O, právě když platí*

$$(1) \qquad (\forall a \in A)\,(\forall x \in O)\; ax \in A.$$

Uvedeme několik poznámek k této definici.

Je ihned zřejmé, že v každém okruhu O existují tyto dva ideály: nulový ideál, obsahující pouze nulový prvek okruhu O, a okruh O sám. Tyto ideály se nazývají triviální ideály v O.

Je-li A ideál v okruhu O, je grupa $(A, +)$ zřejmě (normální) podgrupou v aditivní grupě $(O, +)$ okruhu O. To podle věty 2, kap. X, § 1 nastane, právě když

$$(2) \qquad (\forall a, b \in A)\; a - b \in A.$$

Lze proto vyslovit následující tvrzení.

Lemma 1. *Podmnožina A okruhu O je ideálem v O právě tehdy, když je neprázdná a platí pro ni podmínky* (1) *a* (2).

Na rozdíl od situace v grupách, kde každá podgrupa komutativní grupy G je normální podgrupou v G, nemusí libovolný podokruh komutativního okruhu být

jeho ideálem. Například v okruhu racionálních čísel $(\mathbf{Q}, +, \cdot)$ tvoří celá čísla podokruh $(\mathbf{Z}, +, \cdot)$. Ten však není ideálem v $\mathbf{Q}$, neboť nesplňuje podmínku (1): stačí volit třeba $a = 3$, $x = \frac{1}{2}$, pak $3 \in \mathbf{Z}$ a $3 \cdot \frac{1}{2} = \frac{3}{2} \notin \mathbf{Z}$.

Pojem ideálu lze zavést i v případě, když výchozí okruh není komutativní. Podmínka (1) se pak nahrazuje podmínkou

$$(1') \qquad (\forall a \in A)\,(\forall x \in O)\;(ax \in A \wedge xa \in A)$$

a hovoříme potom o oboustranném ideálu v O. Obdobně lze zavést i pojem levého a pravého ideálu v O.

Ihned z definice ideálu lze odvodit následující tvrzení analogické větě 4 z kap. II, § 3.

Věta 1. *Průnik libovolného neprázdného systému ideálu v okruhu O je opět ideál v O.*

Tato věta umožňuje zavést pojem ideálu generovaného danou množinou prvků z O.

Definice. *Nechť $(O, +, \cdot)$ je (komutativní) okruh, M libovolná podmnožina množiny O. Potom průnik všech ideálů v O, které obsahují množinu M, je ideál v O, který se nazývá* ideálem generovaným množinou *M a značí se $[M]$. Množina M se nazývá* systém generátorů ideálu *$[M]$ a její prvky* generátory *tohoto ideálu.*

Pokud je množina M konečná, například $M = \{a, b\}$, budeme místo $[\{a, b\}]$ psát pouze $[a, b]$.

Prázdná množina generuje zřejmě v libovolném okruhu nulový ideál O.

Pokud M je libovolná podmnožina okruhu O, je obvykle — pokud nemáme přehled o všech ideálech v O — obtížné sestrojit $[M]$ podle definice. Proto postupujeme obdobným způsobem jako u grup (viz kap. X, § 1) a hledáme (ve smyslu množinové inkluze $\subseteq$) nejmenší ideál v O obsahující množinu M. Připojujeme proto k M další prvky z O tak, abychom obdrželi ideál (přičemž dbáme na to, abychom M rozšířili co nejméně). K tomuto postupu je často výhodné užít následující tvrzení, jež plyne ihned z vlastností (1) a (2) ideálu.

Lemma 2. *Jsou-li $a_1, a_2, \ldots, a_k$ libovolné prvky z ideálu A v okruhu O, je i každá jejich lineární kombinace s koeficienty z O prvkem ideálu A, tj.*

$$(3) \qquad (\forall x_1, x_2, \ldots, x_k \in O)\; a_1x_1 + a_2x_2 + \ldots + a_kx_k \in A.$$

Příklad 1. V okruhu celých čísel $\mathbf{Z}$ máme určit ideál $A = [96, 14]$. Pomocí lemmatu 2 se snažíme v tomto ideálu nalézt nenulové číslo s co nejmenší absolutní hodnotou. Musí být

$$1 . 96 + (-6) . 14 = 12 \in A,$$

a tedy též

$$1 . 14 + (-1) . 12 = 2 \in A.$$

Podle (1) obsahuje A všechny celočíselné násobky čísla 2, tj. všechna sudá čísla. Protože podle lemmatu 1 množina všech sudých čísel tvoří zřejmě ideál v $\mathbf{Z}$, je

$$A = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}.$$

Poznamenejme, že obdobně jako u grup může mít týž ideál různé systémy generátorů. Tak třeba ideál A z příkladu 1 je zřejmě generován též číslem 2, tj. $A = [2]$, a lze snadno nahlédnout, že také například $A = [6, 8, -10]$.

Pokud okruh O je okruh s jednotkovým prvkem, lze lemma 2 „zdokonalit" tímto způsobem:

Věta 2. *Nechť O je okruh s jednotkovým prvkem a nechť*

$$M = \{a_1, a_2, \ldots, a_k\} \subseteq O.$$

Pak ideál $[M]$ se skládá právě ze všech prvků tvaru (3), *tj.* $[M] = A$, *kde*

$$A = \{a_1x_1 + a_2x_2 + \ldots + a_kx_k\,;\, x_1, x_2, \ldots, x_k \in O\}.$$

Poznamenejme, že větu 2 lze snadno zobecnit i pro případ nekonečné množiny M. Množina $[M]$ je pak totožná s množinou všech lineárních kombinací s koeficienty z O prvků libovolné konečné podmnožiny množiny M (viz cvičení 5).

Důkaz věty 2. Podle lemmatu 2 je každý prvek tvaru (3) prvkem ideálu $[M]$. Zbývá tedy ukázat, že A je ideál obsahující všechny prvky množiny M. Podle lemmatu 1 stačí pro A ověřit podmínky (1) a (2). Je však ihned vidět, že pro libovolné prvky

$$a = a_1x_1 + \ldots + a_kx_k, \quad b = a_1y_1 + \ldots + a_ky_k \in A$$

(takové, že $x_1, \ldots, x_k, y_1, \ldots, y_k \in O$) a pro libovolné $x \in O$ jsou prvky

$$ax = a_1(x_1x) + \ldots + a_k(x_kx),$$
$$a - b = a_1(x_1 - y_1) + \ldots + a_k(x_k - y_k)$$

rovněž tvaru (3), takže $ax \in A$ i $a - b \in A$.

Pro libovolný index i takový, že $1 \leqq i \leqq k$, stačí volit

$$x_1 = \ldots = x_{i-1} = x_{i+1} = \ldots = x_k = 0, \quad x_i = 1$$

a potom zřejmě

$$a_i = a_1x_1 + \ldots + a_kx_k \in A.$$

Tím je věta 2 dokázána.

Užití věty 2 si ukážeme na příkladech.

Příklad 2. V okruhu $\mathbf{Z}[x]$ polynomů jedné neurčité s celočíselnými koeficienty máme sestrojit ideál $[x, 2]$. Podle věty 2 (neboť v $\mathbf{Z}[x]$ existuje jednotkový prvek) se tento ideál skládá ze všech prvků tvaru

$$x \,.\, f_1(x) + 2 \,.\, f_2(x), \quad \text{kde} \quad f_1(x),\ f_2(x) \in \mathbf{Z}[x].$$

Tedy $[x, 2]$ je množina všech polynomů

$$a_0 + a_1x + \ldots + a_nx^n \in \mathbf{Z}[x],$$

jejichž člen a_0 je sudé číslo. Ideál $[x, 2]$ je tudíž vlastní podmnožina v $\mathbf{Z}[x]$.

Příklad 3. Hledejme ideál $[x, 2]$ v okruhu $\mathbf{Z}_5[x]$ polynomů jedné neurčité nad tělesem $(\mathbf{Z}_5, +, \cdot)$, kde $\mathbf{Z}_5 = \{0, 1, 2, 3, 4\}$ a operace v $\mathbf{Z}_5$ jsou popsány tabulkami 14a, b, takže $(\mathbf{Z}_5, +)$ je izomorfní s faktorovou grupou $\mathbf{Z}/[5]$ v grupě $(\mathbf{Z}, +)$.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Tab. 14a

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tab. 14b

Ideál $[x, 2]$ se podle věty 2 skládá z polynomů tvaru

$$x \,.\, g_1(x) + 2 \,.\, g_2(x), \quad \text{kde} \quad g_1(x),\ g_2(x) \in \mathbf{Z}_5[x]. \tag{4}$$

Protože $\mathbf{Z}_5$ je těleso, existuje prvek $2^{-1} = 3 \in \mathbf{Z}_5$. Volíme-li tedy speciálně v (4) $g_1(x) = 0$, $g_2(x) = 3$, je

$$x \,.\, g_1(x) + 2 \,.\, g_2(x) = x \,.\, 0 + 2 \,.\, 3 = 1.$$

Tedy ideál $[x, 2]$ obsahuje jednotkový prvek 1 okruhu $\mathbf{Z}_5[x]$, takže podle lemmatu 2

$$[x, 2] = [1] = \mathbf{Z}_5[x].$$

Obdobou cyklických podgrup jsou v teorii okruhů takzvané hlavní ideály, které nyní zavedeme.

Definice. *Ideál A v okruhu O se nazývá* hlavní ideál *v O, právě když má alespoň jeden systém generátorů, který je jednoprvková množina.*

Příklad 4. a) Pro ideál A z příkladu 1 platí $A=[2]$ a tedy je hlavním ideálem v $\mathbf{Z}$.

b) Rovněž ideál $[x, 2]$ z příkladu 3 je hlavní ideál v $\mathbf{Z}_5[x]$, neboť má vedle $\{x, 2\}$ též systém generátorů $\{1\}$.

c) Ukážeme, že ideál $[x, 2]$ z příkladu 2 není hlavní ideál v $\mathbf{Z}[x]$.

Předpokládejme opak, tj. že $[x, 2]$ je hlavní ideál v $\mathbf{Z}[x]$. Pak musí existovat polynom $p(x)\in\mathbf{Z}[x]$ tak, že $[x, 2]=[p(x)]$. Protože $2\in[p(x)]$, existuje podle věty 2 polynom $g(x)\in\mathbf{Z}[x]$ takový, že

$$2=p(x).g(x).$$

Podle věty o stupni součinu polynomů (viz věta 1, kap. XI, § 1) musí mít oba polynomy $p(x)$ a $g(x)$ stupeň 0, takže jsou vlastně celočíselné konstanty, jejichž součin je roven 2. Tedy

$$p(x)=\pm 2 \vee p(x)=\pm 1.$$

Kdyby platilo $p(x)=\pm 2$, byl by každý prvek z $[p(x)]$ násobkem čísla 2, avšak $x\in[p(x)]$ a nemá zřejmě tento tvar. Nemůže však platit ani $p(x)=\pm 1$, neboť pak by byl ideál $[x, 2]$ roven celému okruhu $\mathbf{Z}[x]$, což nenastane, jak jsme viděli v příkladu 2.

Tedy náš předpoklad, že $[x, 2]$ je hlavní ideál v $\mathbf{Z}[x]$, vedl ve všech případech ke sporu, takže $[x, 2]$ hlavní ideál v $\mathbf{Z}[x]$ není.

Právě ukončený příklad dokazuje existenci ideálů, které nejsou hlavní. Přesto však existují okruhy, které nemají jiné ideály než hlavní. Takový okruh, jehož každý ideál je hlavní, se nazývá okruh hlavních ideálů.

Triviálním příkladem okruhu hlavních ideálů je libovolné těleso T. Nechť A je ideál v T; jestliže A neobsahuje žádný nenulový prvek, je A nulový ideál, takže $A=[0]$. Obsahuje-li A alespoň jeden nenulový prvek a, musí podle (1)

$$a.a^{-1}=1\in A,$$

takže $A=[1]=T$. Tedy všechny ideály v T jsou hlavní.

S dalšími, méně triviálními příklady okruhů hlavních ideálů se setkáme v příští kapitole (v § 3).

Poznamenejme ještě, že v případě, když okruh O není okruh s jednotkovým prvkem, nemusí tvrzení věty 2 platit, jak uvidíme v následujícím příkladě.

Příklad 5. Označme $(\mathbf{S}, +, \cdot)$ okruh všech sudých celých čísel a vezměme ideál $A=[6]$ generovaný číslem $6\in\mathbf{S}$. Pak množina všech násobků čísla 6 prvky z $\mathbf{S}$ má zřejmě tvar

$$A=\{\ldots, -24, -12, 0, 12, 24, 36, \ldots\}$$

a nemůže být rovna ideálu $[6]$, neboť neobsahuje ani samo číslo 6.

Lze však formulovat pro libovolné okruhy větu analogickou větě 2. Uvedeme ji bez důkazu (viz též cvičení 6).

Věta 2'. *Nechť O je okruh, $M=\{a_1, a_2, \ldots, a_k\}\subseteq O$. Pak ideál $[M]$ se skládá právě ze všech prvků tvaru*

$$a_1x_1+a_2x_2+\ldots+a_kx_k+n_1\times a_1+n_2\times a_2+\ldots+n_k\times a_k,$$

kde $x_1, x_2, \ldots, x_k$ jsou libovolné prvky z O a $n_1, n_2, \ldots, n_k$ libovolná celá čísla ($\times$ značí tzv. přirozený násobek — viz kap. II, § 3).

Ve zbývající části tohoto paragrafu budeme studovat pojem faktorového okruhu. Libovolný ideál v okruhu O je podgrupou v aditivní grupě $(O, +)$ okruhu O a dokonce — vzhledem ke komutativnosti grupy $(O, +)$ — normální podgrupou. Můžeme tedy sestrojit faktorovou grupu (viz kap. X, § 3) $(O/A, +)$, jejíž prvky — rozkladové třídy grupy $(O, +)$ podle A — budou mít ve shodě s aditivním zápisem tvar

$$x+A, \quad \text{kde} \quad x\in O.$$

Připomeňme, že operace ve faktorové grupě O/A je definována tímto způsobem:

$$(\forall x, y\in O)\,(x+A)+(y+A)=(x+y)+A$$

a že nulovým prvkem v O/A je třída $0+A=A$.

Protože v okruhu O máme ještě k dispozici operaci násobení, můžeme ji využít k zavedení operace násobení i v množině O/A. Definujeme ji tímto předpisem:

$$(5)\qquad (\forall x, y\in O)\,(x+A).(y+A)=xy+A.$$

Abychom ověřili, že (5) skutečně definuje operaci v O/A, musíme ukázat, že výsledná třída $xy+A$ nezávisí na způsobu označení výchozích tříd $x+A$, $y+A$. Nechť tedy

$$x+A=x'+A,\ y+A=y'+A,\ x, x', y, y'\in O.$$

Pak podle lemmatu 5 z kap. X, § 2 existují prvky $a, b\in A$ tak, že

$$x'-x=a,\ y'-y=b \quad \text{neboli} \quad x'=x+a,\ y'=y+b.$$

Z vlastností (1) a (2) ideálu a z (5) potom snadno odvodíme

$$(x'+A)\,(y'+A)=x'y'+A=(x+a)\,(y+b)+A=$$
$$=xy+xb+ay+ab+A=xy+A=(x+a)\,(y+A).$$

Tedy formulí (5) je skutečně definována operace v O/A, takže můžeme mluvit o struktuře $(O/A, +, \cdot)$.

Věta 3. *Nechť A je ideál v okruhu O, pak struktura $(O/A, +, \cdot)$ je okruh (s nulovým prvkem A); je-li O okruh s jednotkovým prvkem, má i $(O/A, +, \cdot)$ jednotkový prvek (jímž je třída $1+A$).*

Důkaz. Protože $(O/A, +)$ je komutativní grupa (viz věta 1, kap. X, § 3), stačí dokázat, že $(O/A, \cdot)$ je komutativní pologrupa a že struktura $(O/A, +, \cdot)$ je $(+, \cdot)$-distributivní.

Asociativnost struktury $(O/A, \cdot)$ ověříme snadno tímto způsobem: pro libovolné třídy $x+A$, $y+A$, $z+A \in O/A$ platí

$$[(x+A)(y+A)](z+A) = (xy+A)(z+A) = (xy)z + A =$$
$$= x(yz) + A = (x+A)(yz+A) = (x+A)[(y+A)(z+A)].$$

Ověření zbývajících vlastností okruhu $(O/A, +, \cdot)$ je obdobné a přenecháváme je čtenáři. Je-li 1 jednotkový prvek okruhu O, je ihned zřejmé, že $1+A$ je jednotkový prvek v O/A.

Definice. *Je-li A ideál v okruhu O, nazývá se struktura $(O/A, +, \cdot)$ z věty 3* faktorový okruh (okruhu O podle ideálu A).

Příklad 6. Zvolme v okruhu celých čísel $\mathbf{Z}$ (hlavní) ideál $A = [4]$. Potom faktorový okruh $\mathbf{Z}/A = \mathbf{Z}/[4]$ má za prvky třídy

$$[4] = 0 + [4] = \{4k;\ k \in \mathbf{Z}\},$$
$$1 + [4] = \{4k+1;\ k \in \mathbf{Z}\},$$
$$2 + [4] = \{4k+2;\ k \in \mathbf{Z}\},$$
$$3 + [4] = \{4k+3;\ k \in \mathbf{Z}\}.$$

Sčítání a násobení v $\mathbf{Z}/A$ ilustrujeme pouze na příkladech

$$(2+[4]) + (3+[4]) = 5 + [4] = 1 + [4],$$
$$(3+[4]) \cdot (2+[4]) = 6 + [4] = 2 + [4].$$

Příklad 7. Vezměme okruh $\mathbf{Q}[x]$ polynomů jedné neurčité nad tělesem racionálních čísel $\mathbf{Q}$ a za ideál A v $\mathbf{Q}[x]$ zvolme (hlavní) ideál generovaný polynomem x^3+1, tj. $A = [x^3+1]$. Pak faktorový okruh

$$\mathbf{Q}[x]/A = \mathbf{Q}[x]/[x^3+1]$$

se skládá ze všech tříd tvaru

(6) $$(a_2x^2 + a_1x + a_0) + A, \quad \text{kde} \quad a_2, a_1, a_0 \in \mathbf{Q}.$$

Operace sčítání a násobení v $\mathbf{Q}[x]/A$ objasníme opět pouze na příkladech.

$$(x^2+2x-3+A) + (2x^2-3x+A) = 3x^2 - x - 3 + A,$$
$$(x^2+2x-3+A) \cdot (2x^2-3x+A) = 2x^4 + x^3 - 12x^2 + 9x + A.$$

Protože výsledná třída není zapsána ve tvaru (6), upravíme její zápis takto:

$$(2x^4+2x) + (x^3+1) - 12x^2 + 7x - 1 + A =$$
$$= 2x(x^3+1) + (x^3+1) - 12x^2 + 7x - 1 + A =$$
$$= (2x+1)(x^3+1) - 12x^2 + 7x - 1 + A.$$

Protože $(2x+1)(x^3+1) \in A$, je dohromady

$$(x^2+2x-3+A) \cdot (2x^2-3x+A) = 12x^2 + 7x - 1 + A.$$

Příklad 8. V tomto příkladě vyjdeme od nekomutativního okruhu matic $(M_2, +, \cdot)$ druhého stupně nad celými čísly (viz větu 3 z kap. IV, § 3). Označme S množinu všech matic z M_2, jejichž všechny prvky jsou sudá čísla. Snadno lze nahlédnout, že množina S splňuje podmínky (1′) a (2), a proto je (oboustranný) ideál v okruhu M_2. Můžeme tudíž sestrojit faktorový okruh M_2/S. Matice

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in M_2$$

budou — jak známo — patřit do téže rozkladové třídy M_2 podle S, právě když

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} - \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1-a_2 & b_1-b_2 \\ c_1-c_2 & d_1-d_2 \end{pmatrix} \in S,$$

tj. když čísla stojící na týchž místech v obou maticích budou téže parity (obě současně sudá nebo obě současně lichá). Proto má faktorový okruh M_2/S celkem 16 prvků. Tyto třídy zapíšeme pomocí matic obsahujících pouze čísla 0 a 1 a označíme je tímto způsobem:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} + S = 0, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + S = 1, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + S = a_1, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + S = a_2,$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} + S = a_3, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + S = a_4, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} + S = a_5, \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + S = b_1,$$

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + S = b_2, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} + S = b_3, \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + S = b_4, \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} + S = b_5,$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + S = b_6, \quad \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} + S = b_7, \quad \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} + S = b_8, \quad \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + S = b_9.$$

Sčítání v M_2/S předvedeme na ukázce.

$$a_2 + b_6 = \left[\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} + S\right] + \left[\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} + S\right] = \begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix} + S,$$

což převedeme na tvar

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} + S = a_4.$$

Násobení v M_2/S je popsáno v tabulce 15. Z ní je též například vidět, že prvky 1, a_1, a_2, a_3, a_4, a_5 nejsou a zbývající nenulové prvky b_1 až b_9 jsou dělitelé nuly v okruhu M_2/S.

·	0	1	a_1	a_2	a_3	a_4	a_5	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	a_1	a_2	a_3	a_4	a_5	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8	b_9
a_1	0	a_1	1	a_4	a_5	a_2	a_3	b_3	b_4	b_1	b_2	b_8	b_6	b_7	b_5	b_9
a_2	0	a_2	a_3	a_5	a_4	a_1	1	b_3	b_4	b_6	b_7	b_8	b_1	b_2	b_9	b_5
a_3	0	a_3	a_2	a_1	1	a_5	a_4	b_6	b_7	b_3	b_4	b_9	b_1	b_2	b_8	b_5
a_4	0	a_4	a_5	a_3	a_2	1	a_1	b_1	b_2	b_6	b_7	b_5	b_3	b_4	b_9	b_8
a_5	0	a_5	a_4	1	a_1	a_3	a_2	b_6	b_7	b_1	b_2	b_9	b_3	b_4	b_5	b_8
b_1	0	b_1	b_2	b_2	b_1	b_5	b_5	b_1	b_2	0	0	b_5	b_1	b_2	0	b_5
b_2	0	b_2	b_1	b_5	b_5	b_2	b_1	0	0	b_1	b_2	0	b_1	b_2	b_5	b_5
b_3	0	b_3	b_4	b_4	b_3	b_8	b_8	b_3	b_4	0	0	b_8	b_3	b_4	0	b_8
b_4	0	b_4	b_3	b_8	b_8	b_4	b_3	0	0	b_3	b_4	0	b_3	b_4	b_8	b_8
b_5	0	b_5	b_5	b_1	b_2	b_1	b_2	b_1	b_2	b_1	b_2	b_5	0	0	b_5	0
b_6	0	b_5	b_7	b_7	b_6	b_9	b_9	b_6	b_7	0	0	b_9	b_6	b_7	0	b_9
b_7	0	b_7	b_6	b_9	b_9	b_7	b_6	0	0	b_6	b_7	0	b_6	b_7	b_9	b_9
b_8	0	b_8	b_8	b_3	b_4	b_3	b_4	b_3	b_4	b_3	b_4	b_8	0	0	b_8	0
b_9	0	b_9	b_9	b_6	b_7	b_6	b_7	b_6	b_7	b_6	b_7	b_9	0	0	b_9	0

Tab. 15

Obdobně jako u grup můžeme i pro okruhy zavést pojem faktorového okruhu podle kongruence, což provedeme již stručněji.

Definice. *Nechť $(O, +, \cdot)$ je (komutativní) okruh, R relace v množině O; pak R se nazývá* kongruence v okruhu *O, právě když je ekvivalencí v O a platí pro ni*

$$(7) \qquad \begin{aligned} &(\forall x_1, x_2, y_1, y_2 \in O)\,(x_1 R x_2 \wedge y_1 R y_2) \Rightarrow \\ &\Rightarrow [(x_1 + y_1) R (x_2 + y_2) \wedge x_1 y_1 R x_2 y_2]. \end{aligned}$$

Je-li R kongruence v okruhu O, označme O/R (disjunktní) rozklad množiny O indukovaný ekvivalencí R a dále pro libovolné $x \in O$ označme T_x příslušnou třídu $xR\,\square$ rozkladu O podle R. Definujeme-li ještě

$$(8) \qquad (\forall T_x, T_y \in O/R) T_x + T_y = T_{x+y}$$

a

$$(9) \qquad (\forall T_x, T_y \in O/R) T_x \,.\, T_y = T_{xy},$$

lze pomocí (7) — obdobně jako pro grupy v kap. X, § 3 — ukázat, že (8) a (9) definují skutečně operace v O/R a že struktura $(O/R, +, \cdot)$ je okruh, který nazveme faktorový okruh okruhu O podle kongruence R.

Příklad 9. V okruhu $\mathbf{Z}[x]$ zaveďme relaci R tímto způsobem:

$$(\forall f(x), g(x) \in \mathbf{Z}[x]) f(x) R g(x) \Leftrightarrow f(0) = g(0),$$

takže $f(x)Rg(x)$, právě když polynomy $f(x)$ a $g(x)$ mají týž absolutní člen. Snadno nahlédneme, že relace R je kongruence; například pro libovolné polynomy $f_1(x)$, $f_2(x)$, $g_1(x)$ a $g_2(x)$ ze $\mathbf{Z}[x]$ platí

$$[f_1(0) = f_2(0) \wedge g_1(0) = g_2(0)] \Rightarrow f_1(0) \,.\, g_1(0) = f_2(0) \,.\, g_2(0).$$

Prvky faktorového okruhu $\mathbf{Z}[x]/R$ jsou tedy rozkladové třídy tvaru (pro libovolné $f(x) \in \mathbf{Z}[x]$)

$$T_{f(x)} = \{g(x);\ g(x) \in \mathbf{Z}[x] \wedge g(0) = f(0)\};$$

například

$$T_{3x+5} = \{a_n x^n + \ldots + a_1 x + 5;\ a_n, \ldots, a_1 \in \mathbf{Z}\}.$$

Snadno rovněž nahlédneme, že faktorový okruh $\mathbf{Z}[x]/R$ okruhu $\mathbf{Z}[x]$ podle kongruence R je izomorfní s faktorovým okruhem $\mathbf{Z}[x]/[x]$ podle ideálu generovaného polynomem $x \in \mathbf{Z}[x]$.

Tento příklad naznačuje, že pro okruhy platí tvrzení analogické větám 3 a 4 z kap. X, § 3. Toto tvrzení zformulujeme ve tvaru věty; její důkaz však nebudeme uvádět, neboť čtenář jej může jako cvičení snadno získat z důkazů citovaných vět.

Věta 4. *V libovolném okruhu O lze vzájemně jednoznačně přiřadit ideály v O a kongruence na O tak, že faktorové okruhy podle ideálu a podle kongruence, které si v tomto přiřazení odpovídají, jsou si rovny.*

Cvičení

1. Nechť O je okruh s jednotkovým prvkem 1 a nechť A je ideál v O obsahující 1. Ukažte, že $A = O$.

2. a) V okruhu celých čísel $(\mathbf{Z}, +, \cdot)$ sestrojte ideál $A = [6, 21]$.
b) Co platí pro koeficienty polynomů z ideálu $B = [x^2 + 3x, 9]$ v $\mathbf{Z}[x]$?

3. Nechť M je podmnožina okruhu $(O, +, \cdot)$; pak podgrupa A generovaná množinou M v aditivní grupě $(O, +)$ okruhu O nemusí být totožná s ideálem B generovaným touž množinou M v okruhu O. Platí však vždy $A \subseteq B$. Přesvědčte se o tom na příkladě $M = \{2\}$ v okruhu $\mathbf{Z}[x]$.

4. Nechť O/A je faktorový okruh okruhu O podle ideálu A. Ověřte, že platí

$$(\forall x \in O)\,(\forall a \in A)\,(x + a) + A = x + A.$$

5. Zformulujte a dokažte větu 2 pro případ nekonečné množiny M.
[Postupujte analogicky jako při rozšíření pojmu lineární kombinace a lineární nezávislosti pro nekonečnou množinu vektorů — viz kap. III, § 1.]

6. Ukažte, že věta 2 je speciálním případem věty 2′.

7. Dokažte pro okruhy věty odpovídající větám 3 a 4 z kapitoly X, § 3.

§ 2. Homomorfní zobrazení okruhů

S pojmem homomorfního zobrazení neboli homomorfismu struktur se dvěma binárními operacemi se čtenář již setkal v kap. II, § 4 a pracovali jsme s ním též například v kap. XI, § 2. Proto zde pouze příslušnou definici — pro případ okruhů — připomeneme.

Definice. *Nechť* $(O_1, +, \cdot)$ a $(O_2, +, \cdot)$ *jsou okruhy. Řekneme, že okruh* $(O_2, +, \cdot)$ *je* homomorfním obrazem okruhu $(O_1, +, \cdot)$, *právě když existuje zobrazení* φ *množiny* O_1 *na množinu* O_2, *které splňuje takzvané* podmínky homomorfismu

(1) $$(\forall x, y \in O_1)\varphi(x + y) = \varphi(x) + \varphi(y),$$

(2) $$(\forall x, y \in O_1)\varphi(x \,.\, y) = \varphi(x) \,.\, \varphi(y).$$

Zobrazení φ *splňující* (1) *a* (2) *se nazývá* homomorfní zobrazení, *krátce* homomorfismus okruhu $(O_1, +, \cdot)$ na okruh $(O_2, +, \cdot)$.
Je-li φ *navíc prosté zobrazení množiny* O_1 *na množinu* O_2, *mluvíme o* izomorfním zobrazení (izomorfismu) okruhu $(O_1, +, \cdot)$ na okruh $(O_2, +, \cdot)$.

Z této definice ihned vyplývá, že každý homomorfismus okruhu $(O_1, +, \cdot)$ na okruh $(O_2, +, \cdot)$ je současně homomorfním zobrazením aditivní grupy $(O_1, +)$ okruhu O_1 na aditivní grupu okruhu O_2 a pologrupy $(O_1, \cdot)$ na pologrupu $(O_2, \cdot)$. Proto z věty 2′ z kapitoly II, § 4 ihned plyne následující tvrzení.

Lemma 1. *Pro každé homomorfní zobrazení* φ *okruhu* O_1 *na okruh* O_2 *platí*
a) *je-li* 0 *nulový prvek okruhu* O_1, *je jeho obraz* $\varphi(0)$ *nulový prvek okruhu* O_2;

b) *jsou-li* a, $-a$ *opačné prvky v* O_1, *jsou jejich obrazy* $\varphi(a)$ *a* $\varphi(-a)$ *opačné prvky v* O_2 *neboli*

$$(\forall a \in O_1)\varphi(-a) = -\varphi(a);$$

c) *je-li* 1 *jednotkový prvek v* O_1, *je* $\varphi(1)$ *jednotkový prvek v okruhu* O_2.

Příklad 1. a) Nechť φ je zobrazení množiny celých čísel $\mathbf{Z}$ na množinu $\mathbf{Z}_3$ z příkladu 1 kap. XI, § 2 definované takto: pro libovolné číslo $a \in \mathbf{Z}$ je $\varphi(a)$ nejmenší nezáporný zbytek při dělení čísla a číslem 3. Tedy například

$$\varphi(3) = \varphi(21) = \varphi(-6) = 0,\ \varphi(5) = \varphi(11) = \varphi(-1) = 2.$$

Zobrazení φ je homomorfismus okruhu $(\mathbf{Z}, +, \cdot)$ na okruh $(\mathbf{Z}_3, +, \cdot)$, jehož operace jsou uvedeny v tabulkách 8a, b. Například

$$\varphi(14 + 5) = \varphi(19) = \varphi(3 \,.\, 6 + 1) = 1,$$
$$\varphi(14) = \varphi(3 \,.\, 4 + 2) = 2,\ \varphi(5) = 2,\ \varphi(14) + \varphi(5) = 1,$$
$$\varphi(14 \,.\, 5) = \varphi(70) = \varphi(3 \,.\, 23 + 1) = 1,\ \varphi(14) \,.\, \varphi(5) = 1,$$
$$\varphi(-14) = \varphi(3 \,.\, (-5) + 1) = 1,\ \varphi(14) + \varphi(-14) = 0.$$

b) Zobrazení ψ množiny $\mathbf{Z}$ na množinu všech sudých celých čísel, které má tvar

$$(\forall a \in \mathbf{Z})\psi(a) = 2a,$$

není homomorfní zobrazení okruhu $(\mathbf{Z}, +, \cdot)$ na okruh $(\mathbf{S}, +, \cdot)$, neboť $(\mathbf{Z}, +, \cdot)$ je okruh s jednotkovým prvkem a $(\mathbf{S}, +, \cdot)$ nemá tuto vlastnost, což odporuje tvrzení c) lemmatu 1 (ostatně ani podmínka (2) není pro zobrazení ψ splněna).

Příklad 2. Nechť φ je zobrazení, které každému komplexnímu číslu $a + b\mathrm{i} \in \mathbf{K}$ přiřadí číslo

$$\varphi(a + b\mathrm{i}) = a - b\mathrm{i},$$

tj. číslo sdružené k číslu $a + b\mathrm{i}$. Pak φ je izomorfní zobrazení tělesa komplexních čísel $\mathbf{K}$ na sebe. Zřejmě je φ prosté zobrazení množiny $\mathbf{K}$ na množinu $\mathbf{K}$. Dále pro libovolná čísla $a + b\mathrm{i} \in \mathbf{K}$, $c + d\mathrm{i} \in \mathbf{K}$ platí

$$\varphi((a + b\mathrm{i}) + (c + d\mathrm{i})) = \varphi(a + c + (b + d)\mathrm{i}) = a + c - (b + d)\mathrm{i} =$$
$$= a - b\mathrm{i} + c - d\mathrm{i} = \varphi(a + b\mathrm{i}) + \varphi(c + d\mathrm{i})$$

a obdobně

$$\varphi((a + b\mathrm{i}) \,.\, (c + d\mathrm{i})) = \varphi(ac - bd + (ad + bc)\mathrm{i}) =$$
$$= ac - bd - (ad + bc)\mathrm{i} = (a - b\mathrm{i})\,(c - d\mathrm{i}) =$$
$$= \varphi(a + b\mathrm{i}) \,.\, \varphi(c + d\mathrm{i}),$$

takže φ splňuje podmínky homomorfismu (1) a (2).

Příklad 3. Mějme obory integrity $\mathbf{Z}[x, y]$ a $\mathbf{Z}[x]$ dvou a jedné neurčité nad celými čísly. Nechť φ je zobrazení, které každému polynomu

$$f(x, y) = a_{mn}x^m y^n + \ldots + a_{10}x + a_{01}y + a_{00} \in \mathbf{Z}[x, y] \tag{3}$$

přiřadí polynom

$$\varphi(f(x, y)) = f(x, x) = a_{mn}x^{m+n} + \ldots + a_{10}x + a_{01}x + a_{00} \in \mathbf{Z}[x],$$

pak φ je zřejmě homomorfní zobrazení oboru integrity $\mathbf{Z}[x, y]$ na obor integrity $\mathbf{Z}[x]$.

Obdobně, jsou-li b, c libovolná celá čísla, je zobrazení ψ, které libovolnému polynomu (3) ze $\mathbf{Z}[x, y]$ přiřadí číslo

$$\psi(f(x, y)) = f(b, c) = a_{mn}b^m c^n + \ldots + a_{10}b + a_{01}c + a_{00} \in \mathbf{Z},$$

homomorfismus oboru integrity $\mathbf{Z}[x, y]$ na obor integrity celých čísel $\mathbf{Z}$.

V obou případech jde o takzvané dosazovací homomorfismy.

Z lemmat 1 a 2 z kap. X, § 4 a z definice homomorfního zobrazení okruhů vyplývá následující tvrzení, které je obdobou věty 1 z kap. X, § 4 pro okruhy.

Věta 1. *Nechť struktura $(O_2, +, \cdot)$ je homomorfní obraz okruhu O_1; pak O_2 je rovněž okruh. Je-li O_1 okruh komutativní, respektive okruh s jednotkovým prvkem, má okruh O_2 touž vlastnost.*

Věta 1 tedy vlastně tvrdí, že vlastnost struktury být okruhem se při homomorfním zobrazení zachovává. Následující věta ukazuje, že obdobné tvrzení pro obory integrity neplatí.

Věta 2. *Homomorfní obraz libovolného oboru integrity je okruh s jednotkovým prvkem, který nemusí být obor integrity.*

Důkaz. Protože libovolný obor integrity je okruh s jednotkovým prvkem, je podle věty 1 jeho homomorfní obraz rovněž okruh s jednotkovým prvkem.

Zbývá tedy ukázat, že může nastat případ, kdy homomorfní obraz oboru integrity má dělitele nuly.

Obor integrity celých čísel $\mathbf{Z}$ zobrazíme na faktorový okruh $\mathbf{Z}/[4]$ z příkladu 6 z předchozího paragrafu tímto způsobem: každému celému číslu a přiřadíme jako obraz $\varphi(a)$ tu rozkladovou třídu ze $\mathbf{Z}/[4]$, v níž číslo a leží, tj.

$$(\forall a \in \mathbf{Z})\varphi(a) = a + [4].$$

Zobrazení φ zřejmě zobrazuje množinu $\mathbf{Z}$ na $\mathbf{Z}/[4]$. Ukážeme, že φ je homomorfismus: Nechť $a, b \in \mathbf{Z}$, pak jednak

$$\varphi(a + b) = (a + b) + [4] = (a + [4]) + (b + [4]) = \varphi(a) + \varphi(b),$$

jednak

$$\varphi(a \,.\, b) = ab + [4] = (a + [4]) \,.\, (b + [4]) = \varphi(a) \,.\, \varphi(b).$$

Tedy okruh $\mathbf{Z}/[4]$ je homomorfním obrazem oboru integrity $\mathbf{Z}$. Snadno však nahlédneme, že třída $2 + [4]$ je dělitelem nuly v $\mathbf{Z}/[4]$.

$$(2 + [4]) \,.\, (2 + [4]) = 4 + [4] = 0 + [4],$$

takže $\mathbf{Z}/[4]$ není obraz integrity. Tím je věta 2 dokázána.

Poznamenejme, že vlastnost být oborem integrity se homomorfismem nepřenáší. To je způsobeno tím, že podmínka neexistence dělitelů nuly v oboru integrity I, tj. podmínka

$$(\forall a, b \in I)\ (ab = 0 \wedge a \neq 0) \Rightarrow b = 0,$$

nemá tvar požadovaný v lemmatu 2 z kap. X, § 4. Nemáme tudíž zaručeno, že homomorfní obraz musí tuto podmínku rovněž splňovat. Příklad v důkazu věty 1 pak ukazuje, že případ, kdy homomorfní obraz oboru integrity zmíněnou podmínku nesplňuje, skutečně někdy nastane.

Skutečnost, že okruh lze homomorfně zobrazit na jeho faktorový okruh, jež byla na speciálním případě ukázána v důkazu věty 1, má obecnou platnost. Obdobně jako pro grupy platí i pro okruhy následující tvrzení.

Věta 3. *Nechť O je okruh, A ideál v O. Pak faktorový okruh O/A je homomorfním obrazem okruhu O.*

Důkaz. Zvolíme obdobně jako ve větě 2 z kap. X a jako v důkazu předchozí věty zobrazení φ, které každému prvku z O přiřadí tu třídu z O/A, v níž tento prvek leží. Ověření skutečnosti, že φ je homomorfní zobrazení okruhu O na okruh O/A, přenecháváme čtenáři.

Při studiu homomorfních zobrazení grup hrál důležitou roli pojem jádra homomorfismu, jímž byla vždy normální podgrupa zobrazované grupy. Při vyšetřování homomorfismů okruhů je situace obdobná.

Definice. *Nechť φ je homomorfní zobrazení okruhu $(O, +, \cdot)$ na okruh $(O', +, \cdot)$, jehož nulový prvek označíme $0'$. Jádro homomorfismu φ je množina — označíme ji J_φ — skládající se ze všech prvků z okruhu O, které se v zobrazení φ zobrazí na nulový prvek $0' \in O'$, tj.*

$$J_\varphi = \{x \in O;\ \varphi(x) = 0'\}. \tag{4}$$

Obdobou lemmatu 3 z kap. X, § 4 je tento výsledek:

Lemma 2. *Nechť φ je homomorfní zobrazení okruhu O na okruh O'; pak jádro J_φ je ideál v okruhu O.*

Důkaz. Označme opět nulový prvek okruhu O' symbolem $0'$. Skutečnost, že J_φ je ideál, ověříme podle lemmatu 1 z předchozího paragrafu. Množina J_φ je neprázdná, neboť obsahuje nulový prvek okruhu O. Jsou-li a, b libovolné prvky z J_φ, je podle (4)

$$\varphi(a)=\varphi(b)=0',$$

takže také

$$\varphi(a-b)=\varphi(a)-\varphi(b)=0'-0'=0',$$

což znamená podle (4) $a-b\in J_\varphi$. Je-li $a\in J_\varphi$, $x\in O$, je $\varphi(a)=0'$, a tedy

$$\varphi(ax)=\varphi(a).\varphi(x)=0'.\varphi(x)=0',$$

takže $ax\in J_\varphi$. Tedy J_φ je ideál.

V závěru tohoto paragrafu uvedeme větu nazývanou věta o homomorfismu pro okruhy, analogickou příslušné větě o grupách.

Věta 4. *Nechť okruh O' je homomorfním obrazem okruhu O; pak existuje ideál A v O takový, že faktorový okruh O/A je izomorfní s okruhem O'.*

Důkaz. Obdobně jako v důkazu věty 3 z kap. X, § 4 označme homomorfismus okruhu O na O' a položme $A=J_\varphi$, což lze díky lemmatu 2. Utvoříme faktorový okruh O/A a definujeme zobrazení ψ množiny O/A do O' takto:

$$(\forall a+A\in O/A)\psi(a+A)=\varphi(a).$$

Zcela stejně jako v důkazu citované věty 3 ověříme, že ψ je izomorfní zobrazení grupy $(O/A, +)$ na grupu $(O', +)$. K tomu, abychom dokázali, že ψ je izomorfismus okruhu $(O/A, +, \cdot)$ na okruh $(O', +, \cdot)$, zbývá ukázat, že platí podmínka (2) homomorfismu. Nechť tedy $a+A$, $b+A$ jsou libovolné prvky z O/A. Pak postupně

$$\psi((a+A)(b+A))=\psi(ab+A)=\varphi(ab)=$$
$$=\varphi(a).\varphi(b)=\psi(a+A).\psi(b+A).$$

Tím je věta 4 dokázána.

Ve 3. a 4. paragrafu kapitoly XIV se čtenář seznámí s řadou užití této věty i ostatních poznatků o okruzích, jež získal v této kapitole.

Cvičení

1. Vyšetřete všechny možnosti pro jádra homomorfismů libovolného tělesa. Jaké důsledky z toho plynou pro homomorfní obrazy těles?

2. Dokažte: homomorfní zobrazení φ okruhu O na okruh O_1 je izomorfismus, právě když J_φ je jednoprvková množina.
[Jde o obdobu lemmatu 4 z kap. X, § 4.]

3. Nechť okruh O_1 je homomorfním obrazem okruhu O v homomorfismu φ a okruh O_2 homomorfním obrazem téhož okruhu v homomorfismu ψ a nechť $J_\varphi=J_\psi$. Pak okruhy O_1 a O_2 jsou izomorfní.
[Ověřte, že zobrazení σ definované předpisem

$$(\forall a_1\in O_1)\sigma(a_1)=a_2\in O_2\Leftrightarrow(\exists b\in O)(\varphi(b)=a_1\wedge\psi(b)=a_2)$$

je izomorfní zobrazení O_1 na O_2.]