7. Abelovy grupy, okruhy a tělesa

Grupa $G = G(\cdot, {}^{-1}, \mathbf{1})$ se nazývá *komutativní*, jestliže $ab = ba$ pro každé $a, b \in G$. Pro komutativní grupy se často používá aditivní notace – binární operace se značí $+$, unární $-$ a nulární $\mathbf{0}$. Komutativní grupě v aditivní notaci se zpravidla říká grupa *Abelova* (též abelovská).

Abelova grupa $A = A(+, -, \mathbf{0})$ je tedy algebra s jednou binární, jednou unární a jednou nulární operací, která splňuje pro všechna $a, b, c \in A$ tyto identity:

$$a + (b + c) = (a + b) + c, \qquad a + b = b + a, \qquad a + (-a) = \mathbf{0} \quad \text{a} \quad a + \mathbf{0} = a.$$

Místo $a + (-b)$ píšeme, jak je obvyklé, pouze $a - b$. V aditivní notaci se prvek $-a$ nenazývá prvek inverzní, ale *prvek opačný* (vzhledem k a).

Číselné obory $\mathbb{Z}(+, -, 0)$, $\mathbb{Q}(+, -, 0)$, $\mathbb{R}(+, -, 0)$, $\mathbb{C}(+, -, 0)$ jsou Abelovy grupy. Přitom logaritmus $\lg : \mathbb{R}^+(\cdot, {}^{-1}, 1) \to \mathbb{R}(+, -, 0)$ je izomorfismus multiplikativní grupy všech kladných reálných čísel a aditivní grupy všech reálných čísel.

Existují mnohé jiné příklady komutativních grup, zde jmenujme alespoň Kleinovu grupu.

V aditivním zápisu místo a^n píšeme na. Pro Abelovy grupy podle 6.2 – 6.4 tedy platí:

7.1 Lemma. *Buď $A = A(+, -, 0)$ Abelova grupa, $a \in A$ a $n, m \in \mathbb{Z}$. Potom $n(-a) = -(na)$, $(n + m)a = na + ma$ a $(nm)a = n(ma)$.*

Všimněte si, že každá podgrupa Abelovy grupy je normální.

Algebra $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ se nazývá *okruh*, jestliže $R(+, -, \mathbf{0})$ je Abelova grupa, $R(\cdot, \mathbf{1})$ je monoid a pro všechna $a, b, c \in R$ platí

$$a(b + c) = ab + ac \qquad \text{a} \qquad (b + c)a = ba + ca.$$

Tyto identity jsou známy jako (levý a pravý) *distributivní zákon.*

7.2 Lemma. *Buď $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ okruh. Pak pro libovolná $a, b \in R$ platí $a \cdot \mathbf{0} = \mathbf{0} \cdot a = \mathbf{0}$, $(-a)b = -(ab) = a(-b)$ a $(-a)(-b) = ab$.*

Důkaz. $a\cdot\mathbf{0} = a\cdot(\mathbf{0}+\mathbf{0}) = a\cdot\mathbf{0}+a\cdot\mathbf{0}$, čili $a\cdot\mathbf{0} = \mathbf{0}$. Podobně $\mathbf{0}\cdot a = (\mathbf{0}+\mathbf{0})\cdot a = \mathbf{0}\cdot a+\mathbf{0}\cdot a$, a tedy $\mathbf{0}\cdot a = \mathbf{0}$. Tudíž $\mathbf{0} = \mathbf{0}\cdot b = (a+(-a))\cdot b = ab+(-a)b$. Odsud $(-a)b = -(ab)$, a podobně $-(ab) = a(-b)$, takže $ab = -((-a)b) = (-a)(-b)$. $\square$

7.3 Lemma. *Buď $R = R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ okruh. Je-li $\operatorname{card}(R) \geq 2$, tak $\mathbf{0} \neq \mathbf{1}$.*

Důkaz. Ať $a \neq \mathbf{0}$. Pak $a \cdot \mathbf{1} = a \neq \mathbf{0} = a \cdot \mathbf{0}$, takže $\mathbf{1} \neq \mathbf{0}$. $\square$

Okruh se nazývá *triviální*, jestliže má právě jeden prvek. Podle 7.3 jsou v každém netriviálním okruhu $\mathbf{1}$ a $\mathbf{0}$ různé.

Relace dělitelnosti a pojmy invertibilního a inverzního prvku se vztahují, jedná-li se o okruh $R(+, \cdot, -, \mathbf{0}, \mathbf{1})$, k monoidu $R(\cdot, \mathbf{1})$.

Podmnožina I okruhu R se nazývá *ideál* okruhu R, je-li I podgrupa $R(+, -, 0)$ a ra i ar patří do I pro každé $r \in R$ a $a \in I$.

7.4 Lemma. *Množina všech ideálů okruhu R tvoří uzávěrový systém.*

Důkaz. Buď I_j, $j \in J$ ideály v R. Potom $I = \cap(I_j;\, j \in J)$ je podgrupa $R(+, -, \mathbf{0})$ a pro $a \in I$, $r \in R$ patří ra i ar do každého I_j, $j \in J$. Tudíž $ra \in I$ a $ar \in I$. $\square$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Je-li $A \subseteq R$ a $\mathcal{J}$ je uzávěrový systém všech ideálů v R, tak $\mathrm{cl}_{\mathcal{J}}(A)$ nazýváme *ideálem generovaným* množinou A.

Součet $a_1 + a_2 + \cdots + a_n$ prvků okruhu R píšeme též $\sum_{1 \le i \le n} a_i$. Je-li $n = 0$, tak $\sum_{1 \le i \le n} a_i$ klademe rovné $\mathbf{0}$.

7.5 Lemma. *Buď R okruh a $A \subseteq R$. Potom množina $I = \{\sum_{1 \le i \le n} r_i a_i s_i;\ r_i, s_i \in R,\ a_i \in A$ a $n \in \mathbb{N}_0\}$ je rovna ideálu generovanému množinou A.*

Důkaz. I je zjevně uzavřeno na součty, obsahuje $\mathbf{0}$ a podle 7.2 i opačné prvky. Dále $A \subseteq I$ a I musí ležet v každém ideálu, který obsahuje A. Je-li $r \in R$, tak podle distributivních zákonů je $r(\sum r_i a s_i) = \sum r r_i a_i s_i$ a $(\sum r_i a s_i) r = \sum r_i a s_i r$, takže I je vskutku ideál. $\square$

Budeme se zabývat takřka výhradně *komutativními okruhy*, to jest okruhy R, ve kterých $ab = ba$ pro všechna $a, b \in R$. V komutativním okruhu lze ideál I generovaný množinou A vyjádřit jako $\{\sum_{1 \le i \le n} r_i a_i;\ r_i \in R,\ a_i \in A,\ n \in \mathbb{N}_0\}$. Je-li $A = \{a\}$ jednoprvková množina, tak $I = Ra$. Ideál komutativního okruhu R se nazývá *hlavní*, jestliže existuje $a \in R$, že $I = Ra$.

7.6 Lemma. *Buď R komutativní okruh a $a, b \in R$. Pak:*

(i) *a je invertibilní právě když $Ra = R$.*
(ii) *$a|b$ právě když $Ra \supseteq Rb$.*
(iii) *$a||b$ právě když $Ra = Rb$.*

Důkaz. (i) Je-li $Ra = R$, existuje $c \in R$, že $ca = \mathbf{1}$. Je-li c inverzní prvek a, je $r = rca \in Ra$ pro každé $r \in R$.
(ii) Ať $b = ca$ a $r \in R$. Pak $rb = (rc)a$, takže $Rb \subseteq Ra$. Je-li $Ra \supseteq Rb$, je $b \in Ra$, takže $b = ca$ pro nějaké $c \in R$.
(iii) $a||b$ právě když $a|b$ a $b|a$, tedy právě když $Ra \supseteq Rb$ a $Rb \supseteq Ra$, tedy právě když $Ra = Rb$. $\square$

7.7 Lemma. *Jediné ideály okruhu $\mathbb{Z}(+, \cdot, -, 0, 1)$ jsou hlavní ideály $m\mathbb{Z}$, $m \in \mathbb{N}_0$.*

Důkaz. Buď I ideál $\mathbb{Z}$ a ať $a \in I$ je nenulové. Protože $-a$ patří také do I, lze předpokládat $a > 0$. Buď m nejmenší možné takové a. Pak $m\mathbb{Z} \subseteq I$, a je-li naopak $n \in I$, lze nalézt $p \in \mathbb{Z}$, $q \in \mathbb{N}_0$, že $n = mp + q$, $0 \le q < m$. Protože $q = n - mp \in I$, musí být $q = 0$, a tedy $n \in m\mathbb{Z}$. $\square$

Je-li ρ kongruence okruhu R, tak je ρ i kongruencí Abelovy grupy $R(+, -, \mathbf{0})$. Proto ρ musí být tvaru $\bmod H$, kde H je podgrupa $R(+, -, \mathbf{0})$.

7.8 Tvrzení. *Ekvivalence ρ je kongruencí okruhu R právě když ρ je rovno* $\bmod I$ *pro nějaký ideál I.*

Důkaz. Ať je $\rho = \bmod H$ kongruence a ať $a \in H$ a $r \in R$. Pak je $a\rho\mathbf{0}$ a z $r \cdot \mathbf{0} = \mathbf{0} = \mathbf{0} \cdot r$ plyne $ra\rho\mathbf{0}$, $ar\rho\mathbf{0}$, a tedy $ra \in H$ a $ar \in H$, takže H je ideál.

Buď naopak I ideál R. Je třeba ukázat, že $\bmod I$ je slučitelné s operací $\cdot$. Ať $a \equiv b \bmod I$ a $c \equiv d \bmod I$ pro nějaká $a, b, c, d \in I$. Potom $b - a \in I$, $d - b \in I$, a proto $cd - ab = c(d - b) + (c - a)b \in I$, takže $ab \equiv cd \bmod I$. $\square$

Zobrazení $I \mapsto \bmod I$ je bijekcí mezi svazem všech ideálů okruhu R a svazem všech jeho kongruencí. Protože $I \subseteq J$ je pro ideály I a J ekvivalentní $\bmod I \subseteq$

mod J, jedná se podle 4.4 o izomorfismus svazu ideálů a svazu kongruencí. (Srovnej s podobnou situací u grup, kde na místě ideálů vystupují normální podgrupy.)

Je-li I ideál okruhu R, tak kvocientní okruh $R/\bmod I$ se, podobně jako v případu grup, označuje R/I. Jeho prvky jsou množiny $r + I$, kde r probíhá R. Označení A/I ve významu $\{a + I;\, a \in A\}$ používáme i pro všechna $A \subseteq R$, kde $a + I \subseteq A$ platí pro všechna $a \in A$. Uvažme, jak vypadají kongruence okruhu R/I. Položíme-li $\rho = \mathrm{mod} I$, tak podle 3.5 lze každou takovou kongruenci vyjádřit jako σ/ρ, kde $\sigma \supseteq \rho$ je kongruence R. Ovšem podle 7.8 je σ rovno $\mathrm{mod} J$, kde J je ideál okruhu R. Podmínka $\sigma \supseteq \rho$ pak znamená $J \supseteq I$. Je tedy σ/ρ rovno $\mathrm{mod} J/\bmod I$, kde $J \supseteq I$ je určeno jednoznačně. Podle 7.8 je σ/ρ také rovno $\mathrm{mod} K$, kde K je ideál okruhu R/I. Přitom K obsahuje $\mathbf{0}_{R/I}$, a $K = [\mathbf{0}_{R/I}]_{\sigma/\rho}$ je, jak vyplývá z 1.8(i), rovno $\mathrm{nat}_\rho([\mathbf{0}]_\sigma) = \mathrm{nat}_\rho(J) = \{j + I;\, j \in I\} = J/I$. Ideály okruhu R/I se tedy rovnají množinám J/I, kde $J \supseteq I$ je ideál R.

Je-li $f : R \to S$ homomorfismus okruhů, tak $\ker f$ je kongruence R a $\mathrm{Ker}\, f = [0]_{\ker f} = f^{-1}(\mathbf{0}_S)$. Proto platí:

7.9 Lemma. *Buď $f : R \to S$ homomorfismus okruhů. Pak* Ker f *je ideál R.*

Protože v dalších kapitolách budeme na několika místech používat 1. větu o izomorfismu (viz kapitola 3) pro okruhy, uvedeme ji zde jako samostatné tvrzení.

7.10 Tvrzení. (1. věta o izomorfismu pro okruhy) *Ať $f : R \to S$ je surjektivní homomorfismus okruhů a ať I je jeho jádro. Potom zobrazení $a + I \mapsto f(a)$ je izomorfismus okruhů R/I a S.*

Ideál R okruhu R nazveme *vlastní*, jestliže je kongruence mod I vlastní, čili jestliže $I \neq R$ a $I \neq \{\mathbf{0}\}$. Podobně I nazveme *maximální* ideál, jestliže je kongruence mod I maximální. Ideál I je tedy maximální právě když je $I \neq R$, a pro každý ideál J okruhu R z $I \subseteq J \subseteq R$ plyne $I = J$ nebo $I = R$.

Okruh R je proto jednoduchý (ve smyslu definice jednoduché algebry v kapitole 3), jestliže má alespoň dva prvky a nemá vlastní ideály.

Okruh T se nazývá *těleso*, jestliže je každý jeho nenulový prvek invertibilní a jestliže T obsahuje alespoň dva prvky. Množina $T \backslash \{\mathbf{0}\}$ se značívá T^*. Protože T^* je monoid, který obsahuje pouze invertibilní prvky, lze T^* považovat za grupu (hovoříme o *multiplikativní grupě* tělesa T). Inverzní prvky v T^* značíme a^{-1}.

7.11 Lemma. *Těleso neobsahuje vlastní ideály.*

Důkaz. Ať I je ideál tělesa T a ať $a \in I$, $a \neq \mathbf{0}$. Pak $aa^{-1} = \mathbf{1} \in I$, takže $I = T$. $\square$

7.12 Důsledek. *Buď T těleso a R netriviální okruh. Pak každý homomorfismus $f : T \to R$ je injektivní.*

Důkaz. $f(\mathbf{1}_T) = \mathbf{1}_R \neq \mathbf{0}_R$. Proto je $\mathrm{Ker}\, f \neq T$, takže podle 7.11 je $\mathrm{Ker}\, f = \{\mathbf{0}_T\}$. Tudíž $\ker f = \mathrm{id}_T$ a tedy f je injektivní. $\square$

V případě komutativních okruhů platí k 7.11 i opačné tvrzení:

7.13 Tvrzení. *Buď R netriviální komutativní okruh. Pak R je těleso právě když R neobsahuje vlastní ideály.*

Důkaz. Ať R obsahuje pouze nevlastní ideály a $a \in R$ je nenulové. Podle 7.6(i) je a invertibilní. $\square$

Podle 7.13 je komutativní okruh těleso právě když je to okruh jednoduchý. Aplikací 3.6 tudíž dostáváme

7.14 Tvrzení. *Buď I ideál komutativního okruhu R. Pak R/I je těleso právě když I je maximální ideál R.*

Podokruh tělesa T, který je sám tělesem, se nazývá *podtěleso.*

7.15 Tvrzení. *Množina všech podtěles tělesa T tvoří uzávěrový systém.*

Důkaz. Ať $\mathcal{R}$ označuje uzávěrový systém podokruhů T, $\mathcal{G}$ uzávěrový systém podgrup T^* a ať $\mathcal{G}' = \{G \cup \{\mathbf{0}\};\, G \in \mathcal{G}\}$. K je podtěleso T právě když $K \in \mathcal{G}' \cap \mathcal{R}$, takže lze použít 1.2. $\square$

Je-li T těleso, $\mathcal{T}$ uzávěrový systém jeho podtěles a $A \subseteq T$, tak $\mathrm{cl}_{\mathcal{T}}(A)$ se nazývá *podtěleso generované* množinou A. Nejmenší podtěleso (je generované prázdnou množinou) se nazývá *prvotěleso.* Podobně v okruhu R je *prvookruh* nejmenší podokruh. Prvookruh okruhu R vždy obsahuje $\mathbf{0}_R$ a $\mathbf{1}_R$. Prvotěleso tělesa T vždy obsahuje prvookruh.

Buď $R = R(+,\cdot,-,\mathbf{0},\mathbf{1})$ okruh, $a \in R$ a $n \in \mathbb{Z}$. Protože $R(+,-,\mathbf{0})$ je Abelova grupa, lze použít zápisu $n \cdot a$. Vyjasníme nyní vztah tohoto multiplikativního zápisu a multiplikativního zápisu daného okruhovou operací $\cdot$. Abychom oba zápisy od sebe výrazněji oddělili, budeme do konce této kapitoly výjimečně místo $n \cdot a$ psát $n \times a$. Je tedy například $3 \times a = a + a + a$ a $(-2) \times a = (-a) + (-a)$. Podle 7.1 platí:

7.16 Lemma. *Buď R okruh a $a \in R$. Zobrazení $n \mapsto n \times a$ je pro každé $a \in R$ homomorfismus $\mathbb{Z}(+,-,0)$ do $R(+,-,\mathbf{0})$.*

7.17 Lemma. *Buď R okruh, $a \in R$ a $n \in \mathbb{Z}$. Pak $n \times a = (n \times \mathbf{1}_R) \cdot a$.*

Důkaz. Podle 7.16 platí $-(n \times a) = (-n) \times a$, takže $((-n) \times \mathbf{1})a = (-(n \times \mathbf{1}))a = -((n \times \mathbf{1})a)$, a proto stačí podat důkaz pro $n \geq 0$. Pro $n \leq 1$ vztah zjevně platí, postupujme tedy indukcí a ať $n > 1$. Pak $n \times a = ((n-1) \times a) + a = ((n-1) \times \mathbf{1}) \cdot a + (1 \times \mathbf{1}) \cdot a = (((n-1) \times \mathbf{1}) + (1 \times \mathbf{1})) \cdot a = (n \times \mathbf{1}) \cdot a$. $\square$

7.18 Tvrzení. *Ať R je okruh a $\varphi : \mathbb{Z} \to R$, $\varphi(n) = n \times \mathbf{1}$ pro každé $n \in \mathbb{Z}$. Potom φ je homomorfismus okruhů a $\mathrm{Im}\,\varphi$ je prvookruh okruhu R.*

Důkaz. Buď $n, m \in \mathbb{Z}$. Podle 7.16 je $\varphi(n+m) = \varphi(n) + \varphi(m)$ a podle 7.1 a 7.17 je $\varphi(nm) = (nm) \times \mathbf{1} = n \times (m \times \mathbf{1}) = (n \times \mathbf{1}) \cdot (m \times \mathbf{1}) = \varphi(n)\varphi(m)$. $\mathrm{Im}\,\varphi$ musí obsahovat provookruh P. Protože $\mathbf{1} \in P$ a $-\mathbf{1} \in P$, je $n \times \mathbf{1} \in P$ pro každé $n \in \mathbb{Z}$, takže také $\mathrm{Im}\,\varphi \subseteq P$. $\square$

Jádro $\mathrm{Ker}\,\varphi$ zobrazení $\varphi : \mathbb{Z} \to R$ je podle 7.7 hlavní ideál $m\mathbb{Z}$ pro nějaké $m \in \mathbb{N}_0$, přičemž podle 7.6(iii) je m určeno jednoznačně. Číslo m nazýváme *charakteristikou* okruhu R. Z definice zobrazení φ okamžitě plyne:

7.19 Tvrzení. *Buď R okruh charakteristiky p a ať $n \in \mathbb{Z}$. Potom $n \times \mathbf{1}_R = \mathbf{0}_R$ právě když p dělí n.*

Je-li R okruh charakteristiky p a $p > 0$, tak p je nejmenší kladné číslo takové, že $p \times \mathbf{1}_R = \mathbf{0}$. (Z této vlastnosti se často vychází při definici charakteristiky okruhu.)

Důkaz následujícího tvrzení lze vynechat, neboť je zcela stejný jako důkaz běžné binomické věty.

7.20 Lemma. *Buď R komutativní okruh $a, b \in R$ a $n \in \mathbb{N}$. Pak*
$$(a+b)^n = \sum_{0 \le i \le n} \binom{n}{i} \times a^i b^{n-i}.$$

7.21 Důsledek. *Buď R komutativní okruh charakteristiky $p > 0$ a ať p je prvočíslo. Potom zobrazení $a \mapsto a^p$ je endomorfismus okruhu R.*

Důkaz. Buď $a, b \in R$. Jistě $(ab)^p = a^p b^p$. Dále platí $(a+b)^p = a^p + b^p + \sum_{1 \le i < p} \binom{p}{i} \times a^i b^{p-i}$, přičemž p dělí $\binom{p}{i}$ pro každé $1 \le i < p$, takže podle 7.19 je $\sum_{1 \le i < p} \binom{p}{i} \times a^i b^{p-i} = \mathbf{0}$. $\square$

Endomorfismu $a \mapsto a^p$ říkáme *Frobeniův endomorfismus.* Označíme-li ho φ, tak $\varphi^k(a) = a^{p^k}$ pro každé $a \in R$ a $k \ge 0$. Pro popis konečných těles má velký význam následující tvrzení.

7.22 Tvrzení. *Ať T je komutativní těleso prvočíselné charakteristiky p. Pak $\{a \in T;\ a^{p^k} = a\}$ je pro každé $k \ge 0$ podtělesem T.*

Důkaz. Ať φ značí Frobeniův endomorfismus. Položme $f = \varphi^k$ a $g = \mathrm{id}_T$. Z 3.2 plyne, že $\{a \in T;\ a^{p^k} = a\}$ je podokruh tělesa T. Je-li $a^{p^k} = a$, tak platí $(a^{-1})^{p^k} = (a^{p^k})^{-1} = a^{-1}$, takže tento podokruh je uzavřený na inverzní prvky, a je tedy podtělesem tělesa T. $\square$

Na závěr této kapitoly uvedeme několik často používaných pojmů. Podmnožina I okruhu $R(+, \cdot, -, \mathbf{0}, \mathbf{1})$ se nazývá *levý ideál*, je-li I podgrupa $R(+, -, \mathbf{0})$ a $ra \in I$ pro každé $a \in I$, $r \in R$. Podobně se definuje *pravý ideál.*

Abelova grupa $M(+, -,)$ se nazývá *modul* nad okruhem R, jestliže pro každé $r \in R$, $a \in M$ je definován skalární násobek $r \cdot a$ tak, že
$$r(a+b) = ra + rb, \qquad (r+s)a = ra + sa, \qquad r(sa) = (rs)a \quad \text{a} \quad \mathbf{1} \cdot a = a$$
pro všechna $a, b \in M$ a $r, s \in R$. Modulům nad tělesem se říká vektorové prostory.

Polookruh je algebra $R(+, \cdot, \mathbf{0}, \mathbf{1})$ taková, že $R(+, \mathbf{0})$ je komutativní monoid, $R(\cdot, \mathbf{1})$ monoid a platí distributivní zákony $a(b+c) = ab + ac$ a $(b+c)a = ba + ca$.