# FAKTORALGEBRY

DAVID STANOVSKÝ

## 1. Kongruence a faktoralgebry

V řadě situací se v matematice vyskytuje následující myšlenka: máme dán komplikovaný objekt, některé jeho prvky „ztotožníme“, čímž dostaneme jednodušší objekt, tzv. *faktorobjekt*, se kterým se v dané situaci lépe pracuje. Jako bychom se na objekt podívali zdálky a místo jednotlivých prvků začali vidět obláčky (navzájem nerozlišitelných prvků), tak jako hvězdář není schopen rozlišit jednotlivé hvězdy v galaxiích. Na faktorobjekt (tj. na obláčky) pak přetáhneme vlastnosti původního objektu (tj. jednotlivých hvězd).

Formálně, buď $A$ množina s nějakou strukturou (algebra, graf, metrický prostor, atd.) a $\sim$ vhodná ekvivalence na $A$, která popisuje, které prvky ztotožníme. Faktorobjekt bude mít za nosnou množinu bloky této ekvivalence, tj. $A/{\sim} = \{[a]_\sim : a \in A\}$, a strukturu přetáhneme na bloky tak, že blok $[a]_\sim = \{b \in A : b \sim a\}$ bude simulovat roli prvku $a$. Ne každá ekvivalence je však pro tuto konstrukci vhodná: taková ekvivalence musí nějakým způsobem respektovat původní strukturu. V algebře se takové ekvivalence nazývají *kongruence*.

**Definice.** Buď $\mathbf{A}$ algebra v jazyce $\Sigma$. Ekvivalence $\sim$ na nosné množině $A$ se nazývá *kongruence* algebry $\mathbf{A}$, pokud pro každý $n$-ární symbol $\sigma \in \Sigma$ a všechna $a_1, \dots, a_n, b_1, \dots, b_n \in A$ platí: pokud $a_1 \sim b_1$, …, $a_n \sim b_n$, pak

$$\sigma^{\mathbf{A}}(a_1, \dots, a_n) \sim \sigma^{\mathbf{A}}(b_1, \dots, b_n).$$

Stojí za to explicitně uvést, že pro binární symbol $*$ podmínka říká, že pokud $a_1 \sim b_1$ a $a_2 \sim b_2$, pak

$$a_1 * a_2 \sim b_1 * b_2,$$

a pro unární symbol $'$ říká, že pokud $a \sim b$, pak

$$a' \sim b'.$$

Konstanty zde nehrají žádnou roli, protože $c \sim c$ v každé ekvivalenci.

**Příklad.** Uvažujme algebru $(\mathbb{Z}, +, -, \cdot)$ a definujme na $\mathbb{Z}$ relaci $a \sim_n b$ právě tehdy, když $a \equiv b \pmod n$. Tvrzení **??** říká přesně to, že jde o kongruenci této algebry.

**Definice.** Buď $\mathbf{A}$ algebra a $\sim$ její kongruence. Uvažujme množinu $A/{\sim} = \{[a]_\sim : a \in A\}$ a definujme na ní operace předpisem

$$\sigma^{\mathbf{A}/\sim}([a_1]_\sim, \dots, [a_n]_\sim) = [\sigma^{\mathbf{A}}(a_1, \dots, a_n)]_\sim$$

pro každý $n$-ární symbol $\sigma \in \Sigma$ a všechna $a_1, \dots, a_n \in A$. Algebra

$$\mathbf{A}/{\sim} = (A/{\sim},\ \sigma^{\mathbf{A}/\sim} : \sigma \in \Sigma)$$

se nazývá *faktoralgebra algebry* $\mathbf{A}$ *podle kongruence* $\sim$.

Speciálně, pro binární symbol $*$, unární symbol $'$ a konstantu $c$ dostáváme

$$[a] *^{\mathbf{A}/\sim} [b] = [a *^{\mathbf{A}} b], \qquad [a]'^{\mathbf{A}/\sim} = [a'^{\mathbf{A}}], \qquad c^{\mathbf{A}/\sim} = [c^{\mathbf{A}}].$$

Aby definice dávala smysl, je třeba dokázat, že jsou operace zadány korektně: pokud označíme bloky jiným způsobem, dostaneme stejnou hodnotu operace $\sigma^{\mathbf{A}/\sim}$ ? Potřebujeme dokázat, že pokud $[a_1] = [b_1]$, ..., $[a_n] = [b_n]$, pak $[\sigma^{\mathbf{A}}(a_1, \ldots, a_n)] = [\sigma^{\mathbf{A}}(b_1, \ldots, b_n)]$. Ale to je přesně podmínka z definice kongruence, protože $[x] = [y]$ právě tehdy, když $x \sim y$. (V tomto odstavci i později vynecháváme dolní index ve značení bloků ekvivalencí, kdykoliv je z kontextu jasné, o jakou jde ekvivalenci.)

**Příklad.** Uvažujme kongruence $\sim_n$ na algebře $(\mathbb{Z}, +, \cdot)$ definované v předchozím příkladu. Bloky této kongruence sestávají z čísel, která dávají stejný zbytek po dělení $n$, můžeme je tedy reprezentovat čísly $0, \ldots, n-1$, čili

$$\mathbb{Z}/\sim_n = \{[0], \ldots, [n-1]\}.$$

Operace jsou pak definovány předpisem $[a]+[b] = [a+b] = [a+b \bmod n]$ a $[a]\cdot[b] = [a\cdot b] = [a\cdot b \bmod n]$, čili jde jakoby o sčítání a násobení modulo $n$. Formální popis tohoto jevu uvidíme za chvíli.

Buď $\varphi : \mathbf{A} \to \mathbf{B}$ homomorfismus. Jeho *jádrem* rozumíme relaci

$$\ker(\varphi) = \{(a, b) \in A \times A : \ \varphi(a) = \varphi(b)\}.$$

Následující tvrzení říká, že jádro je kongruencí algebry $\mathbf{A}$, a že každá kongruence je jádrem nějakého homomorfismu.

**Tvrzení 1.1.** *Buď $\mathbf{A}$ algebra a $\sim$ relace na její nosné množině $A$. Pak $\sim$ je kongruencí algebry $\mathbf{A}$ právě tehdy, když je jádrem nějakého homomorfismu z $\mathbf{A}$ do nějaké algebry $\mathbf{B}$.*

*Důkaz.* ($\Rightarrow$) Uvažujme zobrazení

$$\varphi : A \to (A/\sim), \qquad a \mapsto [a]_\sim.$$

Z definice operací fakoralgebry ihned plyne, že jde o homomorfismus $\mathbf{A} \to (\mathbf{A}/\sim)$. Jeho jádrem jsou právě ty dvojice $(a, b)$, pro které $[a]_\sim = [b]_\sim$, tedy $a \sim b$.

($\Leftarrow$) Uvažujme nějaký homomorfismus $\varphi : \mathbf{A} \to \mathbf{B}$. Jeho jádro je zřejmě ekvivalencí, dokážeme, že jde o kongruenci. Uvažujme $n$-ární symbol $\sigma$. Buď $a_1, \ldots, a_n$, $b_1, \ldots, b_n \in A$ a předpokládejme, že $\varphi(a_1) = \varphi(b_1)$, ..., $\varphi(a_n) = \varphi(b_n)$. Pak

$$\begin{aligned}\varphi(\sigma^{\mathbf{A}}(a_1, \ldots, a_n)) &= \sigma^{\mathbf{B}}(\varphi(a_1), \ldots, \varphi(a_n)) \\ &= \sigma^{\mathbf{B}}(\varphi(b_1), \ldots, \varphi(b_n)) = \varphi(\sigma^{\mathbf{A}}(b_1, \ldots, b_n)),\end{aligned}$$

tedy dvojice $(\sigma^{\mathbf{A}}(a_1, \ldots, a_n), \sigma^{\mathbf{A}}(b_1, \ldots, b_n))$ je v jádru také. □

Následující fakt je stěžejním nástrojem k porozumění, jak vypadají faktoralgebry v konkrétních případech. Prvnímu tvrzení se říká *věta o homomorfismu* a druhému *1. věta o izomorfismu* (standardně se uvádějí tři věty o izomorfismu, ale 2. a 3. nejsou zdaleka tak důležité jako 1., takže je uvádět nebudeme; viz cvičení).

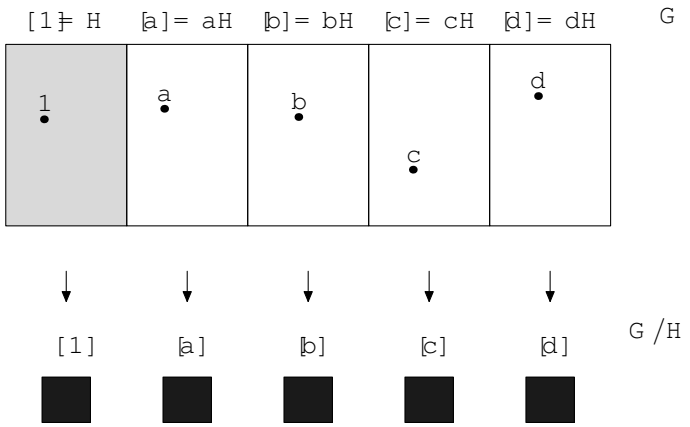
**Věta 1.2.** *Buď $\varphi : \mathbf{A} \to \mathbf{B}$ homomorfismus algeber.*

(1) *Je-li $\sim \subseteq \ker(\varphi)$ kongruence algebry $\mathbf{A}$, pak je zobrazení*

$$\psi : (\mathbf{A}/\sim) \to \mathbf{B}, \qquad [a]_\sim \mapsto \varphi(a)$$

*homomorfismem.*

(2) $\mathbf{A}/\ker(\varphi) \simeq \mathbf{Im}(\varphi)$.




Obrázek 1. Konstrukce faktorgrupy

*Důkaz.* (1) Předně musíme ověřit, že je $\psi$ korektně definované zobrazení, tj. že různá označení bloků nepředepisují různé hodnoty: pokud $[a]_\sim = [b]_\sim$, pak $a \sim b$, takže $(a,b) \in \ker(\varphi)$ podle předpokladu věty, a tedy $\varphi(a) = \varphi(b)$. Zbývá ověřit, že jde o homomorfismus. Uvažujme $n$-ární symbol $\sigma$ a buď $a_1, \dots, a_n \in A$. Pak

$$\begin{aligned}\psi(\sigma^{\mathbf{A}}([a_1], \dots, [a_n])) &= \varphi(\sigma^{\mathbf{A}}(a_1, \dots, a_n)) \\ &= \sigma^{\mathbf{B}}(\varphi(a_1), \dots, \varphi(a_n)) = \sigma^{\mathbf{B}}(\psi([a_1]), \dots, \psi([a_n])).\end{aligned}$$

(2) Dosaďme do věty o homomorfismu za $\sim$ přímo kongruenci $\ker(\varphi)$. Výsledný homomorfismus $\psi$ je prostý, neboť

$$[a] = [b] \;\Leftrightarrow\; (a,b) \in \ker(\varphi) \;\Leftrightarrow\; \varphi(a) = \varphi(b),$$

a uvažujeme-li jej jako zobrazení $\mathbf{A}/\ker(\varphi) \to \mathbf{Im}(\psi) = \mathbf{Im}(\varphi)$, pak je také na. □

Větu opět ilustrujeme na příkladě celých čísel. Mnohem více příkladů pak uvidíme v části o grupách a okruzích.

**Příklad.** Uvažujme zobrazení

$$\varphi : (\mathbb{Z}, +, \cdot) \to (\{0, \dots, n-1\}, +_{\bmod n}, \cdot_{\bmod n}), \quad a \mapsto a \bmod n.$$

Není těžké ověřit, že jde o homomorfismus, který je na. Jeho jádrem je právě ekvivalence $\sim_n$, a tedy, podle 1. věty o izomorfismu,

$$(\mathbb{Z}, +, \cdot)/{\sim_n} \simeq (\{0, \dots, n-1\}, +_{\bmod n}, \cdot_{\bmod n}).$$

## 2. Normální podgrupy a faktorgrupy

Faktorgrupou grupy $\mathbf{G}$ rozumíme faktoralgebru podle nějaké její kongruence $\sim$, tj. algebru

$$\mathbf{G}/{\sim} = (G/{\sim}, \cdot, ^{-1}, [1])$$

s operacemi definovanými $[a] \cdot [b] = [a \cdot b]$ a $[a]^{-1} = [a^{-1}]$. Důležitým pozorováním je, že jde opět o grupu:

$$([a] \cdot [b]) \cdot [c] = [ab] \cdot [c] = [(ab)c] = [a(bc)] = [a] \cdot [bc] = [a] \cdot ([b] \cdot [c])$$

a podobně se ověří také vlastnost jednotky $[a] \cdot [1] = [a \cdot 1] = [a]$ a vlastnost inverzního prvku $[a] \cdot [a]^{-1} = [a] \cdot [a^{-1}] = [aa^{-1}] = [1]$ (analogicky ověříme také stranově převrácená tvrzení).

Druhou zásadní vlastností, kterou si musíme rozmyslet, je, jak vypadají kongruence grup. Pro každou kongruenci $\sim$ grupy $\mathbf{G}$ tvoří blok $[1]_\sim$ podgrupu grupy $\mathbf{G}$, ale ne každá podgrupa je blokem nějaké kongruence. Ukazuje se, že kongruence jsou určeny jistým speciálním typem podgrup, nazývané normální podgrupy, které si nyní popíšeme.

**Tvrzení 2.1.** *Buď* $\mathbf{H}$ *podgrupa grupy* $\mathbf{G}$*. Následující tvrzení jsou ekvivalentní:*

(1) $\mathbf{H} = [1]_\sim$ *pro nějakou kongruenci* $\sim$ *na* $\mathbf{G}$*;*
(2) $\mathbf{H} = \mathbf{Ker}(\varphi)$ *pro nějaký homomorfismus* $\varphi : \mathbf{G} \to \mathbf{K}$*;*
(3) $aha^{-1} \in H$ *pro každé* $h \in H$ *a každé* $a \in G$*;*
(4) $aH = Ha$ *pro každé* $a \in G$*.*

*Důkaz.* (1) $\Rightarrow$ (2). Uvažujme homomorfismus

$$\varphi : \mathbf{G} \to \mathbf{G}/\!\sim, \qquad a \mapsto [a].$$

Jeho jádrem je právě množina všecha $a \in G$ splňujících $[a] = [1]$, tj. přesně blok $[1]$.

(2) $\Rightarrow$ (3). V Tvrzení **??** jsme dokázali, že jde o podgrupu. Uvažujme $h \in \mathrm{Ker}(\varphi)$, tedy $\varphi(h) = 1$, a libovolné $a \in G$. Pak

$$\varphi(aha^{-1}) = \varphi(a)\varphi(h)\varphi(a)^{-1} = \varphi(a)\varphi(a)^{-1} = 1,$$

čili $aha^{-1} \in \mathrm{Ker}(\varphi)$.

(3) $\Rightarrow$ (4). Dokážeme obě inkluze v rovnosti $aH = Ha$. Nejprve uvažujme $ah \in aH$. Pak $k = aha^{-1} \in H$, a tedy $ah = ka \in Ha$. Nyní uvažujme $ha \in Ha$. Pak $l = a^{-1}ha \in H$, tedy $ha = al \in aH$.

(4) $\Rightarrow$ (3). Buď $h \in H$ a $a \in G$. Pak $ah \in aH = Ha$, a tedy existuje $k \in H$ takové, že $ah = ka$. Dostáváme $aha^{-1} = k \in H$.

(3) $\Rightarrow$ (1). Definujme relaci na $G$ vztahem $a \sim b$ právě tehdy, když $ab^{-1} \in H$. Podle Tvrzení **??** je $a \sim b$ právě tehdy, když $Ha = Hb$, a tedy z Lemmatu **??** plyne, že relace $\sim$ je ekvivalence. Dokážeme, že jde o kongruenci. Uvažujme $a, b, c, d \in G$ takové, že $a \sim b$ a $c \sim d$, tedy $ab^{-1} \in H$ a $cd^{-1} \in H$. Ověříme, že $ac \sim bd$ a $a^{-1} \sim b^{-1}$, tedy že $(ac)(bd)^{-1} \in H$ a $a^{-1}(b^{-1})^{-1} \in H$. První vlastnost plyne ze vztahu

$$(ac)(bd)^{-1} = acd^{-1}b^{-1} = ab^{-1}bcd^{-1}b^{-1} = \underbrace{(ab^{-1})}_{\in H} \cdot \underbrace{b(cd^{-1})b^{-1}}_{\in H} \in H$$

a podobně také

$$a^{-1} \cdot (b^{-1})^{-1} = a^{-1}b = a^{-1}ba^{-1}a = a^{-1}\underbrace{(ab^{-1})^{-1}}_{\in H}a \in H.$$

□

**Definice.** Podgrupa $\mathbf{H} \leq \mathbf{G}$ splňující podmínky předchozího tvrzení se nazývá *normální*. Značíme $\mathbf{H} \trianglelefteq \mathbf{G}$.

**Příklady.**

- V abelovských grupách je každá podgrupa normální, obě vlastnosti (3), (4) jsou triviálně splněny.

- Podgrupa $\mathbf{SL}_n(\mathbf{T})$ matic s determinantem 1 je normální v grupě $\mathbf{GL}_n(\mathbf{T})$ všech regulárních matic, jak plyne z podmínky (3) užitím součinového vzorce pro determinanty: $\det(AHA^{-1}) = (\det A)(\det H)(\det A)^{-1} = \det H$.
- Podgrupa $\mathbf{A}_n$ sudých permutací je normální v grupě $\mathbf{S}_n$, jak plyne ze součinového vzorce pro znaménko: $\operatorname{sgn}(aha^{-1}) = (\operatorname{sgn} a)(\operatorname{sgn} h)(\operatorname{sgn} a)^{-1} = \operatorname{sgn} h$.
- Podmnožina
$$\{id, (12)(34), (13)(24), (14)(23)\}$$
tvoří normální podgrupu grupy $\mathbf{A}_4$ i $\mathbf{S}_4$. Není těžké nahlédnout, že je uzavřena na skládání i invertování a z Tvrzení **??** plyne podmínka (3).

Těžší úlohou je spočítat všechny normální podgrupy dané grupy. Samozřejmě $\{1\} \trianglelefteq \mathbf{G}$ a $\mathbf{G} \trianglelefteq \mathbf{G}$. Další normální podgrupy pak můžeme hledat podobným postupem jako podalgebry, přičemž k dispozici máme navíc konjugaci libovolným prvkem.

**Příklad.** Jediné normální podgrupy $\mathbf{S}_n$, $n \neq 4$, jsou $\{1\}$, $\mathbf{A}_n$, $\mathbf{S}_n$. Grupa $\mathbf{S}_4$ navíc obsahuje čtyřprvkovou normální podgrupu uvedenou v předchozím příkladě. Tento fakt lze dokázat elementárně pomocí Tvrzení **??**, ale není to úplně snadné.

Vraťme se ještě jednou k důkazu implikace (3) $\Rightarrow$ (1) v Tvrzení 2.1. Máme-li normální podgrupu $\mathbf{N} \trianglelefteq \mathbf{G}$, definujeme kongruenci na grupě $\mathbf{G}$ předpisem
$$a \sim_{\mathbf{N}} b \;\Leftrightarrow\; ab^{-1} \in N.$$
Její bloky jsou právě rozkladové třídy podgrupy $\mathbf{N}$, tj.
$$[a]_{\sim_{\mathbf{N}}} = aN = Na.$$
Z důkazu Tvrzení 2.1 plyne, že každá kongruence vzniká tímto způsobem z nějaké normální podgrupy. Faktorgrupu podle kongruence $\sim_{\mathbf{N}}$ budeme značit
$$\mathbf{G}/\mathbf{N} = (\{aN :\ a \in G\}, \cdot, ^{-1}, N),$$
přičemž z definice faktorgrupy plyne, že operace jsou dány předpisy
$$(aN)(bN) = (ab)N \quad \text{a} \quad (aN)^{-1} = a^{-1}N.$$
Jednotkou je rozkladová třída $N = 1N$.

**Věta 2.2.** *Buď $\varphi : \mathbf{G} \to \mathbf{H}$ homomorfismus grup.*

(1) *Je-li $\mathbf{N} \leq \mathbf{Ker}(\varphi)$ normální podgrupa grupy $\mathbf{G}$, pak je zobrazení*
$$\psi : (\mathbf{G}/\sim) \to \mathbf{H}, \qquad [a]_\sim \mapsto \varphi(a)$$
*homomorfismem.*

(2) $\mathbf{G}/\mathbf{Ker}(\varphi) \simeq \mathbf{Im}(\varphi)$.

*Důkaz.* Věta je okamžitým důsledkem Věty 1.2, když si uvědomíme, že $(a, b) \in \ker(\varphi)$ právě tehdy, když $ab^{-1} \in \operatorname{Ker}(\varphi)$. □

Stejně jako pro obecné algebry, k prvnímu tvrzení referujeme jako k *větě o homomorfismu*, zatímco k druhému jako k *1. větě o izomorfismu*. Ta je dobrým nástrojem, pokud chceme vyšetřit, jak vypadá daná faktorgrupa. Chceme-li dokázat, že $\mathbf{G}/\mathbf{N} \simeq \mathbf{H}$, stačí najít homomorfismus z $\mathbf{G}$ na $\mathbf{H}$, jehož jádro je $\mathbf{N}$. Jak takový homomorfismus najít? Na to není obecná odpověď. Metodu ilustrujeme na několika příkladech.

**Příklad.** Jak vypadá faktorgrupa $\mathbb{Z}/n\mathbb{Z}$ ? Nejprve neformální analýza situace: dva prvky jsou ekvivalentní, tj. $a \sim_{n\mathbb{Z}} b$, právě tehdy, když $a - b \in n\mathbb{Z}$, tj. právě tehdy, když $n \mid a - b$, tj. právě tehdy, když $a \equiv b \pmod{n}$. Za reprezentanty bloků tedy budeme volit zbytky po dělení $n$, vhodnou operací pak bude sčítání mod $n$. Formálně, uvažujme zobrazení

$$\varphi : \mathbb{Z} \to \mathbb{Z}_n, \qquad a \mapsto a \bmod n.$$

Jde o homomorfismus na $\mathbb{Z}_n$, jehož jádro je $\{x \in \mathbb{Z} : \ x \bmod n = 0\} = n\mathbb{Z}$. Podle 1. věty o izomorfismu je

$$\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n.$$

**Příklad.** Jak vypadá faktorgrupa $\mathbf{S}_n/\mathbf{A}_n$ ? Nejprve neformální analýza situace: dva prvky jsou ekvivalentní, tj. $\pi \sim_{\mathbf{A}_n} \sigma$, právě tehdy, když $\pi\sigma^{-1} \in A_n$, a je snadné nahlédnout, že to nastane právě tehdy, když obě permutace $\pi, \sigma$ mají stejné znaménko. Za reprezentanty bloků tedy budeme volit znaménko, vhodnou operací pak bude díky součinovému vzorci násobení. Formálně, uvažujme zobrazení

$$\varphi : \mathbf{S}_n \to \mathbb{Z}^*, \qquad \pi \mapsto \operatorname{sgn} \pi.$$

Známý součinový vzorec $\operatorname{sgn} \pi\sigma = \operatorname{sgn} \pi \cdot \operatorname{sgn} \sigma$ říká, že jde o homomorfismus. Je to zobrazení na $\mathbb{Z}^*$ a jeho jádro sestává ze sudých permutací. Podle 1. věty o izomorfismu je

$$\mathbf{S}_n/\mathbf{A}_n \simeq \mathbb{Z}^*.$$

**Příklad.** Jak vypadá faktorgrupa $\mathbf{GL}_n(\mathbf{T})/\mathbf{SL}_n(\mathbf{T})$? Dvě matice jsou ekvivalentní právě tehdy, když $AB^{-1} \in \mathrm{SL}_n(T)$, tj. právě tehdy, když $\det AB^{-1} = (\det A)(\det B)^{-1} = 1$, tj. právě tehdy, když $\det A = \det B$. Za reprezentanty bloků tedy budeme volit nenulové prvky tělesa $\mathbf{T}$, vhodnou operací pak bude díky součinovému vzorci násobení. Formálně, uvažujme zobrazení

$$\varphi : \mathbf{GL}_n(\mathbf{T}) \to \mathbf{T}^*, \qquad A \mapsto \det A.$$

Známý součinový vzorec $\det AB = \det A \cdot \det B$ říká, že jde o homomorfismus. Je to zobrazení na $\mathbf{T}^*$ a jeho jádro sestává z matic s determinantem 1. Podle 1. věty o izomorfismu je

$$\mathbf{GL}_n(\mathbf{T})/\mathbf{SL}_n(\mathbf{T}) \simeq \mathbf{T}^*.$$

Jsou však případy, kdy podobná analýza nedává žádný dobrý náhled. Leckdy je možné použít dalších triků, například úvah o počtu prvků a znalosti malých grup.

**Příklad.** Jak vypadá faktorgrupa $\mathbf{S}_4/\mathbf{H}$, kde $\mathbf{H}$ je výše uvedená čtyřprvková normální podgrupa? Protože $|\mathbf{S}_4| = 24$ a $|\mathbf{H}| = 4$, podle Lagrangeovy věty je $|\mathbf{S}_4/\mathbf{H}| = [\mathbf{S}_4 : \mathbf{H}] = 6$, tedy tato faktorgrupa je izomorfní buď grupě $\mathbf{S}_3$, nebo cyklické grupě $\mathbb{Z}_6$. Dokážeme, že grupa $\mathbf{S}_4/\mathbf{H}$ není abelovská, což potvrdí první variantu:

$$[(1\ 2\ 3)] \circ [(1\ 2\ 3\ 4)] = [(1\ 2\ 3) \circ (1\ 2\ 3\ 4)] = [(1\ 3\ 4\ 2)],$$
$$[(1\ 2\ 3\ 4)] \circ [(1\ 2\ 3)] = [(1\ 2\ 3\ 4) \circ (1\ 2\ 3)] = [(1\ 3\ 2\ 4)],$$

ovšem $[(1\ 3\ 4\ 2)] \neq [(1\ 3\ 2\ 4)]$, neboť $(1\ 3\ 4\ 2) \circ (1\ 3\ 2\ 4)^{-1} = (1\ 2\ 4) \notin H$.

Pomocí 1. věty o izomorfismu lze provést přehlednější důkaz klasifikace cyklických grup.

*Alternativní důkaz Věty* **??**. Buď $\mathbf{G} = \langle a \rangle$ cyklická grupa a uvažujme zobrazení

$$\varphi : \mathbb{Z} \to \mathbf{G}, \qquad k \mapsto a^k.$$

Podle Tvrzení **??** je toto zobrazení na $\mathbf{G}$. Je-li $\varphi$ také prosté, pak je izomorfismem $\mathbf{G} \simeq \mathbb{Z}$. V opačném případě je $\mathbf{Ker}(\varphi) = n\mathbb{Z}$, kde $n = \mathrm{ord}(a)$, a podle 1. věty o izomorfismu je $\mathbf{G} \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$. □

## 3. Ideály a faktorokruhy

### 3.1. Konstrukce faktorokruhu.

Faktorokruhem komutativního okruhu $\mathbf{R}$ rozumíme faktoralgebru podle nějaké jeho kongruence $\sim$, tj. algebru

$$\mathbf{R}/\!\sim = (R/\!\sim, +, -, \cdot, [0])$$

s operacemi definovanými $[a]+[b] = [a+b]$, $-[a] = [-a]$ a $[a]\cdot[b] = [a\cdot b]$. Důležitým pozorováním je, že jde opět o komutativní okruh (čtenář si dokáže snadno sám, podobným způsobem jako pro grupy). Má-li $\mathbf{R}$ jednotku 1, pak bude $[1]$ jednotkou v faktorokruhu. Pozor, vlastnost býti oborem integrity zachována být nemusí, viz diskuse v Sekci 3.2.

Podobně jako v grupách, kongruence komutativních okruhů pocházejí ze speciálního typu podokruhů, tzv. *ideálů*. Důležitou roli opět hraje blok $[0]$. Pokud $a \in [0]$ a $r \in R$, pak $a \cdot r \sim 0 \cdot r = 0$, tedy $ar \in [0]$. Tato vlastnost se ukazuje být charakterizující.

**Definice.** Podokruh $\mathbf{I} \leq \mathbf{R}$ se nazývá *ideálem*, pokud pro každé $a \in I$ a $r \in R$ platí $ar \in I$.

Příkladem ideálů jsou např. množiny $n\mathbb{Z} = \{nr : \ r \in \mathbb{Z}\} = \{u \in \mathbb{Z} : \ n \mid u\}$ v oboru $\mathbb{Z}$. Tento příklad lze zobecnit na velmi důležitý pojem hlavního ideálu.

**Tvrzení 3.1.** *Buď $\mathbf{R}$ komutativní okruh a $a \in R$. Pak*

$$aR = \{ar : \ r \in R\} = \{u \in R : \ a \mid u\}$$

*tvoří ideál. Je to nejmenší ideál (nejmenší vzhledem k inkluzi) obsahující prvek $a$.*

Tento ideál se nazývá *hlavní ideál* generovaný prvkem $a$.

*Důkaz.* Je zřejmé, že jde skutečně o ideál: $a \mid 0$, tedy $0 \in aR$, součet i rozdíl dvou prvků dělitelných $a$ je dělitelný $a$, a pokud $a \mid u$, pak $a \mid ru$ pro libovolné $r \in R$. Buď $I$ libovolný ideál obsahující prvek $a$. Pak $I$ jistě obsahuje i všechny jeho násobky, tedy $aR \subseteq I$, čili $aR$ je nejmenší ideál obsahující prvek $a$. □

Uvažujme homomorfismus okruhů $\varphi : \mathbf{R} \to \mathbf{S}$. Podobně jako v grupách, jeho *jádrem* budeme rozumět množinu

$$\mathrm{Ker}(\varphi) = \{a \in R : \ \varphi(a) = 0\}.$$

Z následujícího tvrzení (mimo jiné) plyne, že tato množina tvoří ideál.

**Tvrzení 3.2.** *Buď $\mathbf{I}$ podokruh okruhu $\mathbf{R}$. Následující tvrzení jsou ekvivalentní:*

(1) $\mathbf{I} = [1]_\sim$ *pro nějakou kongruenci $\sim$ na $\mathbf{R}$;*
(2) $\mathbf{I} = \mathbf{Ker}(\varphi)$ *pro nějaký homomorfismus $\varphi : \mathbf{R} \to \mathbf{S}$;*
(3) $\mathbf{I}$ *je ideál.*

*Důkaz.* Důkaz se provede podobně jako u Tvrzení 2.1. V důkazu (3) $\Rightarrow$ (1) použijeme kongruenci danou předpisem

$$a \sim_{\mathbf{I}} b \;\Leftrightarrow\; a - b \in I.$$

Oproti grupám je navíc třeba dokázat, že z $a \sim b$ a $c \sim d$ plyne také $ac \sim bd$ (pozor, násobení v grupách odpovídá sčítání v okruzích). Čili předpokládáme $a - b \in I$ a $c - d \in I$, z čehož plyne $(a - b) \cdot c \in I$ a $b \cdot (c - d) \in I$, čili $(a - b) \cdot c + b \cdot (c - d) = a \cdot c - b \cdot d \in I$ a dostáváme $a \cdot c \sim b \cdot d$. □

Z důkazu vidíme, že k ideálu $\mathbf{I}$ je přiřazena kongruence na $\mathbf{R}$ daná předpisem

$$a \sim_{\mathbf{I}} b \;\Leftrightarrow\; a - b \in I,$$

přičemž každá kongruence vzniká tímto způsobem z nějakého ideálu. Její bloky jsou právě rozkladové třídy

$$[a]_{\sim_{\mathbf{I}}} = a + I.$$

Faktorokruh podle kongruence $\sim_{\mathbf{I}}$ budeme značit

$$\mathbf{R}/\mathbf{I} = (\{a + I :\; a \in R\}, +, -, \cdot, I).$$

Z definice faktorokruhu plyne, že operace jsou dány předpisy

$$(a+I)+(b+I) = (a+b)+I, \quad -(a+I) = (-a)+I \quad \text{a} \quad (a+I)(b+I) = (ab)+I.$$

Nulovým prvek je rozkladová třída $I = 0 + I$ a eventuální jednotkou třída $1 + I$.

Zvláště důležitý je případ, kdy $\mathbf{R}$ je komutativní okruh a $\mathbf{I}$ jeho hlavní ideál, tj. $I = mR$ pro nějaké $m \in R$. Faktorokruh pak zapisujeme zkráceně $\mathbf{R}/(m)$. Jak takový faktorokruh vypadá? Dva prvky jsou ekvivalentní, tj. $a \sim_{mR} b$, právě tehdy, když $a - b \in mR$, tj. právě tehdy, když $m \mid a - b$, což symbolicky značíme $a \equiv b \pmod m$. Je-li v okruhu $\mathbf{R}$ definováno dělení se zbytkem, prvky $\mathbf{R}/(m)$ můžeme reprezentovat jako všechny možné zbytky po dělení prvkem $m$ a operace v $\mathbf{R}/(m)$ budou jako operace v původním okruhu modulo $m$:

$$[a] \pm [b] = [a \pm b] = [a \pm b \bmod m], \qquad [a] \cdot [b] = [a \cdot b] = [a \cdot b \bmod m].$$

**Příklad.** Obor $\mathbb{Z}$ je eukleidovský, s jednoznačně definovaným podílem a zbytkem. Prvky faktorokruhu $\mathbb{Z}/(n)$ tedy můžeme reprezentovat jako všechny možné zbytky po dělení číslem $n$, tj. jako čísla $0, \ldots, n-1$, přičemž operace provádíme modulo $n$. Je vidět, že zobrazení $\mathbb{Z}_n \to \mathbb{Z}/(n)$, $a \mapsto [a]$, je izomorfismem.

**Příklad.** Obor $\mathbf{T}[x]$, $\mathbf{T}$ těleso, je eukleidovský, s jednoznačně definovaným podílem a zbytkem. Prvky faktorokruhu $\mathbf{T}[x]/(f)$, kde $f \in T[x]$, tedy můžeme reprezentovat jako všechny možné zbytky po dělení polynomem $f$, tj. jako všechny polynomy stupně menšího než $\deg f$, přičemž operace provádíme modulo $f$. Určit strukturu faktorokruhu $\mathbf{T}[x]/(f)$ je bez 1. věty o izomorfismu těžší (a záleží na $f$).

**Věta 3.3.** *Buď $\varphi : \mathbf{R} \to \mathbf{S}$ homomorfismus komutativních okruhů.*

(1) *Je-li $\mathbf{I} \leq \mathbf{Ker}(\varphi)$ ideál v $\mathbf{R}$, pak je zobrazení*

$$\psi : (\mathbf{R}/\!\sim) \to \mathbf{S}, \qquad [a]_\sim \mapsto \varphi(a)$$

*homomorfismem.*

(2) $\mathbf{R}/\mathbf{Ker}(\varphi) \simeq \mathbf{Im}(\varphi)$.

*Důkaz.* Věta je okamžitým důsledkem Věty 1.2, když si uvědomíme, že $(a, b) \in \ker(\varphi)$ právě tehdy, když $a - b \in \mathrm{Ker}(\varphi)$. □

Stejně jako pro obecné algebry, k prvnímu tvrzení referujeme jako k *větě o homomorfismu*, zatímco k druhému jako k *1. větě o izomorfismu*.

**Příklad.** Jak vypadá faktorokruh $\mathbb{Z}/(n)$ ? Uvažujme zobrazení

$$\varphi : \mathbb{Z} \to \mathbb{Z}_n, \qquad a \mapsto a \bmod n.$$

Je to homomorfismus na $\mathbb{Z}_n$ a jeho jádro je $\{x \in \mathbb{Z} :\ x \bmod n = 0\} = n\mathbb{Z}$. Podle 1. věty o izomorfismu je

$$\mathbb{Z}/(n) \simeq \mathbb{Z}_n.$$

Pro určování struktury faktorokruhů polynomiálních okruhů často poslouží tzv. *dosazovací homorfismus*, tedy zobrazení

$$\varphi_u : \mathbf{R}[x] \to \mathbf{S}, \qquad f \mapsto f(u),$$

kde $\mathbf{R} \leq \mathbf{S}$ jsou komutativní okruhy a $u \in S$. Připomeňme, že je-li $f = \sum_{i=1}^{n} a_i x^i$ polynom z $\mathbf{R}[x]$ a $u \in S$, pak výrazem $f(u)$ rozumíme hodnotu polynomu $f$ na $u$, tj. prvek $f(u) = \sum_{i=1}^{n} a_i u^i \in S$. Je snadné ověřit, že zobrazení přiřazující polynomům jejich hodnotu v daném bodě je homomorfismus.

**Příklad.** Jak vypadá faktorokruh $\mathbb{Z}[x]/(x-1)$ ? Uvažujme homomorfismus

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}, \qquad f \mapsto f(1).$$

Je to zobrazení na $\mathbb{Z}$ a jeho jádro je

$$\{f \in \mathbb{Z}[x] :\ f(1) = 0\} = \{f \in \mathbb{Z}[x] :\ x - 1 \mid f\} = (x-1)\mathbb{Z}[x].$$

Podle 1. věty o izomorfismu je

$$\mathbb{Z}[x]/(x-1) \simeq \mathbb{Z}.$$

**Příklad.** Jak vypadá faktorokruh $\mathbb{Z}[x]/(x^2+1)$ ? Uvažujme homomorfismus

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}, \qquad f \mapsto f(i).$$

Je to zobrazení na $\mathbb{Z}[i]$ a jeho jádro je

$$\begin{aligned}
\{f \in \mathbb{Z}[x] :\ f(i) = 0\} &= \{f \in \mathbb{Z}[x] :\ f(i) = f(-i) = 0\} \\
&= \{f \in \mathbb{Z}[x] :\ x - i \mid f,\ x + i \mid f\} \\
&= \{f \in \mathbb{Z}[x] :\ (x-i)(x+i) = x^2 + 1 \mid f\} \\
&= (x^2+1)\mathbb{Z}[x],
\end{aligned}$$

Podle 1. věty o izomorfismu je

$$\mathbb{Z}[x]/(x^2+1) \simeq \mathbb{Z}[i].$$

**Příklad.** Jak vypadá faktorokruh $\mathbb{Z}[x]/(x^2-1)$ ? Uvažujme homomorfismus

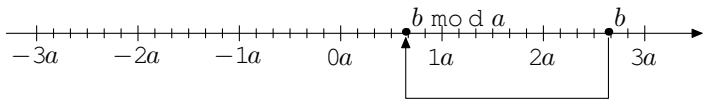
$$\varphi : \mathbb{Z}[x] \to \mathbb{Z} \times \mathbb{Z}, \qquad f \mapsto (f(1), f(-1)).$$

Jeho jádro je

$$\begin{aligned}
\{f \in \mathbb{Z}[x] :\ f(1) = f(-1) = 0\} &= \{f \in \mathbb{Z}[x] :\ x - 1 \mid f,\ x + 1 \mid f\} \\
&= \{f \in \mathbb{Z}[x] :\ (x-1)(x+1) = x^2 - 1 \mid f\} \\
&= (x^2-1)\mathbb{Z}[x],
\end{aligned}$$

a jeho obraz je $\mathrm{Im}(\varphi) = \{(a, b) :\ a \equiv b \pmod 2\}$. Podle 1. věty o izomorfismu je

$$\mathbb{Z}[x]/(x^2-1) \simeq \mathbf{Im}(\varphi) \leq \mathbb{Z} \times \mathbb{Z}.$$




Obrázek 2. Ilustrace důkazu Věty 3.4 v případě $\mathbf{R} = \mathbb{Z}$.

Na závěr jeden příklad s ideálem, který není hlavní.

**Příklad.** Jak vypadá faktorokruh $\mathbb{Z}[x]/\mathbf{I}$, kde $I = \{f \in \mathbb{Z}[x] : \ 4 \mid f(0)\}$ ? Dva polynomy jsou ekvivalentní právě tehdy, když $f - g \in I$, tj. právě tehdy, když $4 \mid f(0) - g(0)$, tj. právě tehdy, když $f(0) \equiv g(0) \pmod 4$. Existují tedy přesně čtyři rozkladové třídy. Není těžké nahlédnout, že zobrazení

$$\varphi : \mathbb{Z}[x] \to \mathbb{Z}_4, \qquad f \mapsto f(0) \bmod 4$$

je homomorfismem, a tedy

$$\mathbb{Z}[x]/\mathbf{I} \simeq \mathbb{Z}_4.$$

3.2. **Ideály a dělitelnost.**

Ideály hrají v teorii dělitelnosti zásadní roli, mimo jiné z následujícího důvodu: v komutativním okruhu $\mathbf{R}$ platí

- $a \mid b$ právě tehdy, když $bR \subseteq aR$;
- $a \parallel b$ právě tehdy, když $aR = bR$.

Čili hlavní ideály s uspořádáním inkluze přesně odrážejí dělitelnost až na asociovanost. Historicky vznikl pojem ideálu tak, že v některých oborech jakoby chybějí prvky, které by činily teorii dělitelnosti lepší. Tyto prvky lze označit za „ideální“, míněno myšlenkové. Ukázalo se, že roli těchto prvků lze zastoupit počítáním s ideály, přičemž „skutečné prvky“ odpovídají hlavním ideálům. Hlouběji se této teorii věnuje komutativní algebra. Zde se soustředíme na opačný případ, totiž obory, kde „nic nechybí“. Mezi tyto obory patří např. celá čísla nebo polynomy jedné proměnné nad tělesem, které pro nás budou nejdůležitější v kapitole o tělesech.

**Definice.** Komutativní okruhy, kde je každý ideál hlavní, se nazývají *okruhy hlavních ideálů*. V případě oborů integrity hovoříme o *oborech hlavních ideálů*.

Nejdůležitější příklady popisuje následující věta.

**Věta 3.4.** *V eukleidovských oborech je každý ideál hlavní.*

*Důkaz.* Buď $I$ ideál v eukleidovském oboru $\mathbf{R}$. Je-li $I = \{0\}$, pak $I = 0R$. V opačném případě označme $a$ takový prvek ideálu $I$, který má nejmenší nenulovou eukleidovskou normu (libovolný z nich, je-li jich více). Dokážeme, že $I = aR$. Zřejmě $aR \subseteq I$, pro spor tedy předpokládejme, že existuje nějaký prvek $b \in I \setminus aR$. Zvolme $q, r$ splňující $b = aq + r$ a $\nu(r) < \nu(a)$. Samozřejmě $r \neq 0$, protože $b$ není dělitelné $a$, a tedy $0 < \nu(r) < \nu(a)$. Ovšem

$$r = \underbrace{b}_{\in I} - \underbrace{aq}_{\in I} \in I,$$

což je spor s výběrem $a$ jako prvku $I$ s nejmenší kladnou normou. □

Opačná implikace neplatí, ale vymyslet nějaký protipříklad není snadné: asi nejjednodušším příkladem je obor $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Důkaz tohoto faktu je poměrně obtížný.

Pro tělesa platí ještě silnější vlastnost. Tento fakt se nám bude hodit později, až budeme konstruovat tělesa jako faktorokruhy (viz Sekce 3.3).

**Tvrzení 3.5.** *Buď* $\mathbf{R}$ *komutativní okruh s jednotkou. Pak* $\mathbf{R}$ *je těleso právě tehdy, když má pouze nevlastní ideály.*

*Důkaz.* ($\Rightarrow$) Buď $I$ ideál v $\mathbf{R}$ a předpokládejme, že $I \neq \{0\}$. Zvolme libovolné $0 \neq a \in I$. Pak pro každé $b \in R$ platí $b = a \cdot (a^{-1} \cdot b) \in I$, a tedy $I = R$.

($\Leftarrow$) Ke každému $0 \neq a \in R$ hledáme prvek $b \in R$ takový, že $a \cdot b = 1$. Uvažujme hlavní ideál $aR$. Ten obsahuje prvek $a$, čili je různý od $\{0\}$, a tudíž podle předpokladu $aR = R$. Speciálně $1 \in aR$, tj. existuje $b \in R$ splňující $1 = a \cdot b$. □

V Sekci **??** jsme ukázali, že obory $\mathbb{Z}[x]$ ani obory polynomů více proměnných nejsou eukleidovské. Ukážeme, že to dokonce nejsou ani obory hlavních ideálů. Oba důkazy jsou založené na následující myšlence. Hlavní ideál $aR$, který obsahuje dva nesoudělné prvky $u, v$, je roven celému $R$: je-li $u, v \in aR$, tj. $a \mid u$ i $a \mid v$, pak musí být $a \parallel 1$, z čehož plyne $aR = R$. Toto pozorování lze snadno použít k hledání ideálů, které nejsou hlavní.

**Příklad.** Obor $\mathbb{Z}[x]$ není obor hlavních ideálů. Uvažujme množinu

$$I = \{f \in \mathbb{Z}[x] : \ f(0) \text{ je sudé}\} \subset \mathbb{Z}[x].$$

Je vidět, že jde o ideál. Přitom $I$ obsahuje polynomy 2 a $x$, které jsou nesoudělné, nemůže tedy být hlavní.

**Příklad.** Obor $\mathbf{R}[x_1, \ldots, x_k]$ (kde $\mathbf{R}$ je libovolný obor integrity a $k > 1$) není obor hlavních ideálů. Uvažujme množinu

$$I = \{f \in R[x_1, \ldots, x_k] : \ f(0, \ldots, 0) = 0\} \subset R[x_1, \ldots, x_k].$$

Je vidět, že jde o ideál. Přitom $I$ obsahuje polynomy $x_1$ a $x_2$, které jsou nesoudělné, nemůže tedy být hlavní.

Obory hlavních ideálů jsou důležitou třídou oborů integrity z toho důvodu, že struktura ideálů věrně odráží pojem dělitelnosti až na asociovanost. Jako ukázku práce s hlavními ideály si ukážeme větu, která obory hlavních ideálů zařazuje do hierarchie oborů z hlediska teorie dělitelnosti.

**Věta 3.6.** *Obory hlavních ideálů jsou gaussovské.*

*Důkaz.* Buď $\mathbf{R}$ obor hlavních ideálů. Podle Věty **??** stačí dokázat, že v $\mathbf{R}$ (1) existují NSD a (2) neexistují nekonečné posloupnosti vlastních dělitelů. Připomeňme, že pro libovolná $u, v$ platí $u \mid v \Leftrightarrow vR \subseteq uR$.

(1) Zvolme $a, b \in R$ a označme $I$ nejmenší ideál obsahující množinu $aR \cup bR$. Existuje tedy $c \in R$ takové, že $I = cR$. Protože $aR \subseteq cR$, máme $c \mid a$, a analogicky $c \mid b$. Přitom pokud je $d$ společným dělitelem $a, b$, pak $aR \subseteq dR$ a $bR \subseteq dR$, tedy $I = cR \subseteq dR$ a dostáváme $d \mid c$. Tedy $c = \mathrm{NSD}(a, b)$.

(2) Pro spor předpokládejme, že v $\mathbf{R}$ existuje nekonečná posloupnost vlastních dělitelů $a_1, a_2, \ldots$ (tj. $a_{i+1} \mid a_i$ a $a_i \nmid a_{i+1}$). Pak $a_1R \subset a_2R \subset a_3R \subset \ldots$ a označme $I = \bigcup_{i=1}^{\infty} a_iR$. Tato množina také tvoří ideál (dokáže se podobně jako Tvrzení **??**), takže $I = bR$ pro nějaké $b \in I$. Ovšem protože $b \in I = \bigcup_{i=1}^{\infty} a_iR$, existuje $i$ takové, že $b \in a_iR$. Pak ale $bR = a_iR = a_{i+1}R = \ldots$, spor. □

Podobně lze pro obory hlavních ideálů dokázat další vlastnosti, např. Bézoutovu rovnost: není těžké nahlédnout, že nejmenší ideál obsahující množinu $aR \cup bR$ je ideál $aR + bR = \{au + bv : \ u, v \in R\}$, a protože tento ideál obsahuje $\mathrm{NSD}(a, b)$, dostáváme $\mathrm{NSD}(a, b) = au + bv$ pro nějaká $u, v \in R$.

### 3.3. **Maximální ideály a konstrukce těles.**

Ideál **I** okruhu **R** nazveme *maximální*, pokud je **I** maximální v uspořádané množině vlastních ideálů, tj. pokud neexistuje ideál **J** splňující $I \subset J \subset R$. Konstrukce těles založená na následující větě nachází široké použití v kapitole o tělesech (např. konstrukce konečných těles, konstrukce kořenového nadtělesa, konstrukce algebraického uzávěru).

**Věta 3.7.** *Je-li* **R** *komutativní okruh s jednotkou a* **I** *jeho maximální ideál, pak je faktorokruh* $\mathbf{R}/\mathbf{I}$ *těleso.*

*Důkaz.* Podle Tvrzení 3.5 stačí dokázat, že okruh $\mathbf{R}/\mathbf{I}$ neobsahuje žádné vlastní ideály. Pro spor tedy uvažujme vlastní ideál **K** v $\mathbf{R}/\mathbf{I}$ a definujme

$$J = \{a \in R : \ [a] \in K\}.$$

Ukážeme, že $J$ tvoří ideál okruhu **R**. Skutečně, $0 \in J$, neboť $[0] \in K$. A jsou-li $a, b \in J$, tj. $[a], [b] \in K$, pak $a \pm b \in J$, neboť $[a \pm b] = [a] \pm [b] \in K$, a navíc pro libovolné $r \in R$ je $a \cdot r \in J$, neboť $[a \cdot r] = [a] \cdot [r] \in K$. Přitom $I \subseteq J$, neboť pro každé $i \in I$ máme $[i] = [0] \in K$, a $I \neq J \neq R$, protože $K$ tvoří vlastní ideál. Tím dostáváme spor s předpokládanou maximalitou ideálu **I**. □

**Poznámka.** Platí i opačná implikace: pokud je faktorokruh $\mathbf{R}/\mathbf{I}$ těleso, pak je nutně ideál **I** maximální. Tento fakt se dokáže podobně, viz cvičení. Platí také mnohem obecnější věta, která říká, že ideály faktorokruhu $\mathbf{R}/\mathbf{I}$ jednoznačně korespondují s ideály **J** okruhu **R**, pro které platí $\mathbf{I} \leq \mathbf{J} \leq \mathbf{R}$. Tato jednoznačná korespondence je dána přiřazením, které se objevilo v důkazu, ideálu **K** v $\mathbf{R}/\mathbf{I}$ odpovídá ideál $J = \{a \in R : \ [a] \in K\}$ v **R**.

Často budeme používat Větu 3.7 v situaci, kdy je **R** obor hlavních ideálů. Které hlavní ideály jsou pak maximální? Připomeňme, že $a \mid b$ právě tehdy, když $bR \subseteq aR$. Pokud jsou v **R** všechny ideály hlavní, pak je $aR$ maximální (nejde zvětšit) právě tehdy, když je $a$ minimální (nejde zmenšit) vzhledem k dělitelnosti, neboli ireducibilní. (V obecných oborech to nemusí být pravda, protože mezi $aR$ a $R$ může existovat ideál, který není hlavní.)

**Příklad.** Faktorokruh $\mathbb{Z}/(n) \simeq \mathbb{Z}_n$ je těleso právě tehdy, když $n$ je prvočíslo, což je právě tehdy, když je $n\mathbb{Z}$ maximální ideál.

**Příklad.** Uvažujme faktorokruhy oboru $\mathbb{Z}[x]$, které jsme diskutovali na konci Sekce 3.1. Obor $\mathbb{Z}[x]$ není oborem hlavních ideálů, a tedy ideály $mR$, kde $m$ je ireducibilní polynom, nemusejí být maximální, čili příslušné faktorokruhy nemusí být tělesem. Skutečně, pohledem do výsledků zjistíme, že ani jeden z faktorokruhů $\mathbb{Z}[x]/(x-1) \simeq \mathbb{Z}$ a $\mathbb{Z}[x]/(x^2+1) \simeq \mathbb{Z}[i]$ není tělesem. Ideál $(x-1)\mathbb{Z}[x]$ není maximální, například ideál $I = \{f \in \mathbb{Z}[x] : \ 2 \mid f(1)\}$ je větší. Zkuste sami najít podobný příklad pro $(x^2+1)\mathbb{Z}[x]$.

**Příklad.** Uvažujme faktorokruhy oboru $\mathbb{Q}[x]$ podle stejných polynomů, jako jsme diskutovali na konci Sekce 3.1. Vyjdeme z vlastnosti, že $\mathbb{Q}[x]$ je oborem hlavních ideálů.

- Polynom $x-1$ je ireducibilní, tedy ideál $(x-1)\mathbb{Q}[x]$ je maximální, a skutečně, podle 1. věty o izomorfismu je $\mathbb{Q}[x]/(x-1) \simeq \mathbb{Q}$ těleso.
- Polynom $x^2-1$ není ireducibilní, tedy ideál $(x^2-1)\mathbb{Q}[x]$ není maximální (např. ideál $(x-1)\mathbb{Q}[x]$ je větší), a skutečně, podle 1. věty o izomorfismu

$\mathbb{Q}[x]/(x^2-1) \simeq \mathbb{Q} \times \mathbb{Q}$ není těleso (odvoďte si, že obraz homomorfismu v tomto případě vyjde celé $\mathbb{Q} \times \mathbb{Q}$).

- Polynom $x^2+1$ je ireducibilní, tedy ideál $(x^2+1)\mathbb{Q}[x]$ je maximální, a skutečně, podle 1. věty o izomorfismu je $\mathbb{Q}[x]/(x^2+1) \simeq \mathbb{Q}[i]$ těleso.

**Příklad.** Uvažujme ireducibilní polynom $f \in \mathbb{Z}_p[x]$, $p$ prvočíslo, stupně $k$. Protože je $\mathbb{Z}_p[x]$ oborem hlavních ideálů, faktorokruh $\mathbb{Z}_p[x]/(f)$ je tělesem. Jeho prvky lze reprezentovat jako polynomy stupně $< k$. Tyto mají přesně $k$ koeficientů ze $\mathbb{Z}_p$, a tedy $\mathbb{Z}_p[x]/(f)$ je *konečným tělesem*, které má $p^k$ prvků.

V Sekci **??** o konečných tělesech dokážeme následující netriviální fakta: pro každé $p, k$ takový ireducibilní polynom existuje, na jeho volbě (až na izomorfismus zkonstruovaných těles) nezáleží a žádná jiná konečná tělesa než tato neexistují.

**Poznámka.** Analogii Věty 3.7 lze dokázat i pro vlastnost býti oborem integrity: *faktorokruh* $\mathbf{R}/\mathbf{I}$ *je obor integrity právě tehdy, když je* $\mathbf{I}$ *prvoideál*, tj. ideál, který má následující vlastnost: kdykoliv $a \cdot b \in I$, pak $a \in I$ nebo $b \in I$. Hlavní ideál $aR$ je prvoideálem právě tehdy, když je prvek $a$ prvočinitelem. V oborech hlavních ideálů tyto dva pojmy splývají, ale obecně ne. Prvoideály jsou velmi důležitým strukturním pojmem, hrajícím roli „ideálních prvočísel“.