# ZÁKLADY ALGEBRY 2008/09

DAVID STANOVSKÝ

stanovsk@karlin.mff.cuni.cz

Toto jsou provizorní skripta k úvodnímu kurzu obecné algebry, a to jak pro studenty učitelství a finanční matematiky (skripta obsah přednášky přesahují), tak pro studenty informační bezpečnosti. Mohou sloužit jako pomůcka k zápiskům z přednášky, těžko však lze čekat, že student látku pochopí pouze četbou tohoto textu.

Sekce označené * nejsou nezbytně nutné k pochopení základů algebry, ale vhodně dokreslují probíranou problematiku, zpravidla ve dvou směrech: buď ukazují aplikace dokázaných výsledků (např. Lineární diferenční rovnice, Burnsideova věta, Konstrukce pravítkem a kružítkem), nebo prohlubují probíranou teorii (např. Klasifikace konečných abelovských grup a konečných těles).

Vzniku tohoto textu výrazně napomohli studenti Anna Bernáthová, Andrew Kozlík a Ivan Štubňa, kteří pomohli přepisovat zápisky z přednášek do elektronické formy, za což jim jsme všichni vděčni. Poděkování patří i studentům, kteří mě upozornili na řadu drobných chyb.

*Date*: 11. února 2009.


Obrázek 1. Al-Chorezmí: *Hisáb al-džabr wa-l-muqábala*

# Úvod

## 1. Ekvivalence a uspořádané množiny

**Cíl.** *Připomeneme pojmy ekvivalence a uspořádání, které by měly být známy z úvodních matematických kurzů.*

Relací $\rho$ na množině $X$ rozumíme libovolnou podmnožinu kartézského součinu $X \times X$; tedy prvky relace $\rho$ jsou některé dvojice prvků množiny $X$. Místo $(a, b) \in \rho$ píšeme často $a \,\rho\, b$, zejména pokud relaci označíme symbolem typu $\sim$, $\leq$ apod. Na relace je užitečné nahlížet jako na orientované grafy.

**Definice.** Relaci $\sim$ na množině $X$ nazýváme *ekvivalence*, pokud je

(1) *reflexivní*, tj. $x \sim x$ pro všechna $x \in X$,
(2) *tranzitivní*, tj. $x \sim y$ a $y \sim z$ implikuje $x \sim z$,
(3) a *symetrická*, tj. $x \sim y$ implikuje $y \sim x$.

*Blokem* (nebo *třídou*) ekvivalence $\sim$ příslušnou prvku $x \in X$ rozumíme množinu

$$[x]_\sim = \{y \in X : x \sim y\}.$$

Pro daná $x, y$ jsou příslušné bloky buď stejné (pokud $x \sim y$), nebo disjunktní; tvoří tedy *rozklad* množiny $X$. Množinu všech bloků ekvivalence $\sim$ značíme $X/\!\sim$, tj. $X/\!\sim = \{[x]_\sim : x \in X\}$.

Naopak, každému disjunktnímu rozkladu $X = \bigcup_{B \in \mathcal{B}} B$ přísluší ekvivalence definovaná předpisem „$x \sim y \;\Leftrightarrow x, y$ leží ve stejném bloku“.

**Příklad.**

- Na množině přirozených čísel $\mathbb{N}$ zavedeme relaci definovanou předpisem „$a \sim b \;\Leftrightarrow\; a + b$ je sudé číslo“. Je to ekvivalence s dvěma bloky: jeden blok je tvořen sudými čísly, druhý lichými.
- Na množině všech přímek v rovině zavedeme relaci definovanou předpisem „$p_1 \parallel p_2 \;\Leftrightarrow$ přímky $p_1$ a $p_2$ jsou rovnoběžné“. Blok $[p]_\parallel$ obsahuje právě všechny přímky rovnoběžné s $p$.
- Na množině všech trojúhelníků v rovině zavedeme relaci definovanou předpisem „$T_1 \simeq T_2 \;\Leftrightarrow$ trojúhelníky $T_1$ a $T_2$ jsou shodné“. Blok $[T]_\simeq$ obsahuje právě všechny trojúhelníky shodné s $T$.
- Na množině vrcholů daného grafu zavedeme relaci definovanou předpisem „$x \sim y \;\Leftrightarrow$ existuje cesta z $x$ do $y$“. Bloky této ekvivalence jsou komponenty souvislosti daného grafu.

**Definice.** Relaci $\leq$ na množině $X$ nazýváme *částečné uspořádání*, pokud je

(1) *reflexivní*, tj. $x \leq x$ pro všechna $x \in X$,
(2) *tranzitivní*, tj. $x \leq y$ a $y \leq z$ implikuje $x \leq z$,
(3) a *antisymetrická*, tj. $x \leq y$ a $y \leq x$ implikuje $x = y$.

Alternativně říkáme, že $(X, \leq)$ je *uspořádaná množina*. Uspořádání se nazývá *lineární*, pokud navíc pro každé $x, y$ nastane $x \leq y$ nebo $y \leq x$. *Intervalem* rozumíme množinu

$$[a, b] = \{x \in X : a \leq x \leq b\}.$$

Pokud $x \leq y$ a $x \neq y$, píšeme $x < y$.

**Příklad.**

- Na množině přirozených čísel uvažujme obvyklé uspořádání $1 < 2 < 3 < \ldots$; uspořádaná množina $(\mathbb{N}, \leq)$ je lineární.
- Na množině přirozených čísel uvažujme uspořádání dělitelnosti, tj. „$a$ je menší než $b$ pokud $a \mid b$“; uspořádaná množina $(\mathbb{N}, |)$ *není* lineární: např. čísla 2, 3 jsou neporovnatelné.
- Na množině $P(X)$ všech podmnožin dané množiny $X$ uvažujme uspořádání inkluzí, tj. „$A$ je menší než $B$ pokud $A \subset B$“; je-li $|X| > 1$, pak uspořádaná množina $(P(X), \subseteq)$ není lineární: např. dvě různé jednoprvkové množiny jsou neporovnatelné.

Konečné uspořádané množiny se často zadávají pomocí tzv. *Hasseova diagramu*. Jde o graf relace $\leq$, přičemž nekreslíme smyčky (reflexivita), vynecháváme všechny hrany, jejichž existence je zaručena tranzitivitou, a místo šipek kreslíme neorientované hrany tak, aby větší prvky byly výše. Např.

$\mathbf{A} =$  $\mathbf{B} =$ 

**Definice.** Řekneme, že prvek $a \in X$ je v $(X, \leq)$

- *největší*, pokud pro každé $b \in X$ platí $b \leq a$;
- *nejmenší*, pokud pro každé $b \in X$ platí $b \geq a$;
- *maximální*, pokud neexistuje žádné $b \in X$ takové, že $b > a$;
- *minimální*, pokud neexistuje žádné $b \in X$ takové, že $b < a$.

**Příklad.**

- Uspořádaná množina **A** má jeden největší prvek, jeden maximální (ten samý), žádný nejmenší a dva minimální prvky.
- Uspořádaná množina **B** má jeden největší (a zároveň maximální) a jeden nejmenší (a zároveň minimální) prvek. Je to lineární uspořádání.
- Uspořádaná množina $(\mathbb{N}, \leq)$ má nejmenší prvek 1, ale žádný maximální prvek.
- Uspořádaná množina $(\mathbb{N}, |)$ přirozených čísel s relací dělitelnosti má nejmenší prvek 1, ale žádný maximální prvek. Uspořádaná množina $(\mathbb{N} \setminus \{1\}, |)$ má za minimální prvky právě všechna prvočísla.

**Definice.** Nechť $Y \subseteq X$. Řekneme, že prvek $a \in X$ je v $(X, \leq)$

- *horní mez* množiny $Y$, pokud $a \geq y$ pro každý prvek $y \in Y$;
- *supremum* množiny $Y$, pokud to je nejmenší horní mez $Y$; značí se $a = \sup Y$.
- *dolní mez* množiny $Y$, pokud $a \leq y$ pro každý prvek $y \in Y$;
- *infimum* množiny $Y$, pokud to je největší dolní mez $Y$; značí se $a = \inf Y$.

Jinými slovy, supremum množiny $Y$ je nejmenší prvek množiny $X$, který je větší než všechny prvky $Y$. Podobně, infimum množiny $Y$ je největší prvek množiny $X$, který je menší než všechny prvky $Y$.

**Příklad.**

- V uspořádané množině **A** podmnožina sestávající z obou minimálních prvků nemá supremum ani infimum. Infimum proto, že nemá ani žádnou dolní mez. Horní meze sice tato podmnožina má tři, avšak žádná z nich není nejmenší.
- V uspořádané množině **B** má každá neprázdná podmnožina supremum i infimum. Obecně, v každé lineárně uspořádané množině má každá neprázdná *konečná* podmnožina supremum i infimum, přičemž $\sup Y = \max Y$, $\inf Y = \min Y$. Pozor, pro nekonečné to obecně nefunguje: např. v $(\mathbb{N}, \leq)$ neexistuje $\sup \mathbb{N}$.
- V uspořádané množině $(P(X), \subseteq)$ má každá podmnožina infimum i supremum, přičemž $\inf Y$ je rovno průniku všech množin z $Y$ a $\sup Y$ je rovno sjednocení všech množin z $Y$.
- V uspořádané množině $(\mathbb{N}, |)$ má každá konečná podmnožina infimum i supremum. Přitom $\inf Y$ je rovno NSD všech čísel z $Y$ a $\sup Y$ je rovno NSN všech čísel z $Y$. Na druhou stranu, např. $\sup\{p : p \text{ prvočíslo}\}$ neexistuje.

Uvědomte si, že $\sup \emptyset$ je rovno nejmenšímu prvku, pokud takový v $(X, \leq)$ existuje; podobně, $\inf \emptyset$ je rovno největšímu prvku, pokud takový existuje.

**Definice.** *Svazem* nazýváme každou uspořádanou množinu, ve které existují suprema a infima všech *dvouprvkových* podmnožin (pak také zřejmě existují suprema a infima všech *neprázdných konečných* podmnožin). *Úplným svazem* nazýváme každou uspořádanou množinu, ve které existují suprema a infima všech podmnožin. Ve svazu obvykle značíme zkráceně

$$a \vee b = \sup\{a, b\} \quad \text{a} \quad a \wedge b = \inf\{a, b\},$$

symboly $\vee, \wedge$ čteme jako *spojení* a *průsek*.

Tedy v úplném svazu existuje nejmenší i největší prvek ($\sup \emptyset$ a $\inf \emptyset$).

**Příklad.**

- Uspořádaná množina **A** není svaz.
- Lineárně uspořádáná množina je vždy svaz: $a \vee b = \max(a, b)$, $a \wedge b = \min(a, b)$. Tedy $(\mathbb{N}, \leq)$ je svaz, ale není úplný: např. $\sup \mathbb{N}$ neexistuje.
- $(\mathbb{N} \cup \{\infty\}, \leq)$ je úplný svaz.
- $(P(X), \subseteq)$ je úplný svaz: $A \vee B = A \cup B$, $A \wedge B = A \cap B$.
- $(\mathbb{N}, |)$ je (neúplný) svaz: $a \vee b = \text{NSN}(a, b)$, $a \wedge b = \text{NSD}(a, b)$.

Definici úplného svazu lze zjednodušit: stačí předpokládat existenci buď suprem, nebo infim.

**Tvrzení 1.1.** *Uspořádaná množina, ve které existují infima všech podmnožin, je úplný svaz.*

*Důkaz.* Označme danou uspořádanou množinu $(X, \leq)$. Stačí si uvědomit, že

$$\sup Y = \inf\{a \in X : a \geq y \text{ pro každé } y \in Y\},$$

tedy že suprema lze definovat pomocí infim. □

(Analogicky lze předpokládat pouze existenci suprem.)

Na závěr úvodní kapitoly zformulujeme jedno pozorování o konečných množinách, které nijak nesouvisí s uspořádánými množinami, avšak bude se nám v budoucnu párkrát hodit.

**Lemma 1.2.** *Buď $f : X \to Y$ zobrazení mezi stejně velkými konečnými množinami. Je-li $f$ prosté, pak je bijektivní.*

*Důkaz.* Nechť $n = |X| = |Y|$. Každému z $n$ prvků množiny $X$ přiřadí $f$ nějakou hodnotu, přičemž tyto hodnoty jsou navzájem různé; obor hodnot zobrazení $f$ tedy musí mít $n$ prvků. Takže to musí být celé $Y$. □

## Dělitelnost v oborech integrity

### 2. Elementární teorie čísel

**Cíl.** *Nejprve stručně nastíníme, jak se formálně definují přirozená čísla, a hned poté se pustíme do základních poznatků o dělitelnosti: existence a jednoznačnost rozkladu na prvočísla (Základní věta aritmetiky); Eukleidův algoritmus a Bézoutova rovnost; Čínská věta o zbytcích; Eulerova funkce a Eulerova věta. Naučíme se pracovat s šikovným značením pomocí kongruencí* $\equiv \pmod{n}$.

2.1. **Přirozená čísla.**

Přirozenými čísly intuitivně rozumíme množinu $\mathbb{N} = \{1, 2, 3, 4, \ldots\}$. Formálně vzato však tento zápis nedává valný smysl: nekonečnou množinu přece nemůžeme definovat výčtem prvků! V tomto odstavci nastíníme, jak lze přirozená čísla zavést formálně. Protože však u čtenáře nepředpokládáme žádnou znalost matematické logiky, nebudeme se pouštět do detailů a některé pojmy z logiky budeme používat bez dalšího vysvětlení na intuitivní úrovni. Z jistých důvodů se v logice zavádějí přirozená čísla i s nulou, čehož se v tomto odstavci přidržíme.

Jeden ze způsobů, jak přirozená čísla zavést, je zformulovat sadu *axiomů*, z nichž se budou všechna tvrzení o přirozených číslech dokazovat. Standardním přístupem je tzv. *Peanova axiomatika*. Přirozená čísla s nulou zavedeme jako teorii, v níž máme konstantu 0, unární funkční symbol $s$ a následující axiomy:

(1) pro každé $a$ existuje právě jedno $b$ takové, že $s(a) = b$;
(2) pro každé $a$ je $s(a) \neq 0$;
(3) pro každé $a \neq b$ platí $s(a) \neq s(b)$;
(4) je-li $V$ vlastnost taková že
   (a) 0 má vlastnost $V$;
   (b) pro každé $a$ platí následující: jestliže má $a$ vlastnost $V$, pak $s(a)$ má také vlastnost $V$;

   pak má každé $a$ vlastnost $V$.

Interpretace symbolu $s$ je taková, že „číslu“ přiřadí „číslo o jedna větší“. První tři axiomy říkají, že $s$ je prostá funkce, v jejímž oboru hodnot není 0. Poslednímu axiomu se říká *matematická indukce*.

Na základě těchto axiomů můžeme induktivně definovat standardní operace: sčítání předpisy $a + 0 = a$ a $a + s(b) = s(a + b)$ (tj. umíme-li spočítat $a + b$, definujeme na jeho základě $a + s(b)$), násobení předpisy $a \cdot 0 = 0$ a $a \cdot s(b) = a \cdot b + a$, atd. Uspořádání definujeme předpisem $a \leq b \Leftrightarrow \exists c\ a + c = b$ a podobně lze postupovat pro další známé pojmy a vlastnosti.

Z Peanových axiomů lze logicky odvodit všechna tvrzení o přirozených číslech, na která si vzpomenete — i když zpravidla nejde vůbec o jednoduchou práci (zkuste např. dokázat, že sčítání je komutativní!). Přesto má tato metoda své limity: slavná

Gödelova věta o neúplnosti říká, že existují tvrzení, jež z těchto axiomů nelze dokázat ani vyvrátit. A ještě hůře: dokonce neexistuje žádná „hezká“ sada axiomů, která by tuto nepříjemnou vlastnost neměla. Naštěstí se ukazuje, že taková tvrzení jsou dosti obskurní, Gödelovou větou se tedy nemusíme příliš trápit.

Druhým přístupem, který uvedeme, je vybudování *modelu* přirozených čísel (s nulou) v rámci nějaké dobře známé teorie, např. teorie množin. Standardním modelem v teorii množin jsou tzv. *von Neumannova čísla*, definovaná jako nejmenší množina $\omega$ splňující

(1) $\emptyset \in \omega$;
(2) jestliže $A \in \omega$, pak $A \cup \{A\} \in \omega$.

Tedy $\omega$ obsahuje postupně množiny

$$\emptyset, \quad \{\emptyset\}, \quad \{\emptyset, \{\emptyset\}\}, \quad \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \quad \dots$$

Tímto způsobem můžeme definovat číslovky $0 = \emptyset$, $1 = \{\emptyset\}$, $2 = \{\emptyset, \{\emptyset\}\}$ atd. Všimněte si, že v tomto značení je $1 = \{0\}$, $2 = \{0, 1\}$, $3 = \{0, 1, 2\}$, atd. Pokud iterpretujeme symbol $s$ jako $s(A) = A \cup \{A\}$, pro von Neumannova čísla budou platit Peanovy axiomy.

Na závěr stručně uvedeme, jak se formálně zavádějí ostatní číselné obory. Celá čísla lze definovat jako sjednocení čísel kladných, záporných a nuly, přičemž záporným číslem rozumíme formální zápis $-a$, kde $a$ je přirozené číslo; operace se definují zřejmým způsobem. Celá čísla s operacemi sčítání, odčítání a násobení tvoří strukturu, které se říká *obor integrity*. Racionální čísla se pak definují jako *podílové těleso* tohoto oboru (viz Tvrzení 8.1). Způsobů, jak formálně zavést čísla reálná je celá řada, jeden příklad za všechny: jde o tzv. *zúplnění* uspořádaného tělesa racionálních čísel — doplníme suprema a infima všech omezených podmožin a pomocí limit na ně přeneseme operace (detaily konstrukce patří spíše do topologie). Na komplexní čísla pak lze nahlížet jako na *algebraický uzávěr* čísel reálných (viz Věta 26.4).

### 2.2. **Základní věta aritmetiky.**

V tomto odstavci zopakujeme znalosti, které byste měli mít ze střední školy, přičemž doplníme některé důkazy. Tato fakta byla známa již starořeckým matematikům a v moderní podobě byly formulovány Carlem Friedrichem Gaussem v jeho slavné knize *Disquisitiones Arithmeticae* z roku 1801, která položila základ moderní teorie čísel.

Čísly budeme nadále rozumět přirozená čísla. Jak známo, pro každou dvojici čísel $a, b$ existuje právě jedna dvojice čísel $q, r$, kde $r \in \{0, \dots, b-1\}$, splňující vztah

$$a = q \cdot b + r.$$

Číslo $q$ se nazývá *celočíselný podíl* čísel $a, b$, značí se $a \operatorname{div} b$, a číslo $r$ se nazývá *zbytek* po dělení, značí se $a \bmod b$.

Řekneme, že číslo $b$ *dělí* číslo $a$, píšeme $b \mid a$, pokud existuje číslo $q$ splňující $a = b \cdot q$ (tj. pokud je zbytek $r = 0$). Pro každé $a$ platí $1 \mid a$ a $a \mid a$; tito dělitelé se nazývají *nevlastní*. Číslo $p \neq 1$, které má pouze nevlastní dělitele, se nazývá *prvočíslo*; ostatní čísla se nazývají *složená*. Zcela základním poznatkem teorie čísel je fakt, že každé číslo lze jednoznačně vyjádřit jako součin prvočísel.

**Věta 2.1** (Základní věta aritmetiky)**.** *Pro každé přirozené číslo $a \neq 1$ existují různá prvočísla $p_1, p_2, \dots, p_n$ a přirozená čísla $k_1, k_2, \dots, k_n$ splňující*

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_n^{k_n}$$

*(tomuto vyjádření se říká* prvočíselný rozklad*). Tento zápis je jednoznačný až na pořadí činitelů.*

Přiznejme si však na tomto místě: kdo z nás umí takovou „samozřejmost“, jakou je existence a jednoznačnost prvočíselného rozkladu, dokázat?

Tedy existenci rozkladu lze dokázat poměrně snadno indukcí: je-li $a$ prvočíslo, rozklad zřejmě existuje; budeme tedy předpokládat, že $a$ je složené a že rozklad existuje pro všechna menší čísla. Napíšeme $a = b \cdot c$ pro nějaká $1 < b, c < a$. Podle indukčního předpokladu existuje prvočíselný rozklad jak pro $b$, tak pro $c$. Jejich složením získáme rozklad čísla $a$.

S jednoznačností je to však složitější.

*Největší společný dělitel* čísel $a$ a $b$ je největší číslo $c$ splňující zároveň $c \mid a$ a $c \mid b$. Toto číslo značíme $\mathrm{NSD}(a, b)$; všimněte si, že jde o infimum množiny $\{a, b\}$ ve svazu $(\mathbb{N}, |)$. Podobně, *nejmenší společný násobek* čísel $a$ a $b$ je nejmenší číslo $c$ splňující zároveň $a \mid c$ a $b \mid c$. Toto číslo značíme $\mathrm{NSN}(a, b)$ a jde o supremum v tomto svazu. Zřejmě

$$\mathrm{NSN}(a, b) = \frac{a \cdot b}{\mathrm{NSD}(a, b)}.$$

Na výpočet NSD používáme známý *Eukleidův algoritmus*, kterému se budeme blíže věnovat v sekci o Eukleidovských oborech (viz Sekce 6). Ten funguje následujícím způsobem: začneme s danými dvěma čísly a budujeme posloupnost tak, že vždy vezmeme zbytek po dělení předposledního čísla posledním. Odpovědí je poslední nenulová hodnota. Např. pro $\mathrm{NSD}(168, 396)$ dostáváme posloupnost 396, 168, 60, 48, 12, 0, a tedy $\mathrm{NSD}(168, 396) = 12$. Správnost algoritmu plyne z následujícího pozorování:

**Lemma 2.2.** *Pro libovolná přirozená čísla $a, b$ platí*

$$\mathrm{NSD}(a, b) = \mathrm{NSD}(a \bmod b, b).$$

*Důkaz.* Zopakujme, že

$$a = b \cdot (a \operatorname{div} b) + (a \bmod b).$$

Tedy dané číslo $c$ dělí obě čísla $a, b$ právě tehdy, když $c$ dělí obě čísla $a \bmod b, b$. Protože tyto dvě dvojice mají stejné společné dělitele, mají stejného i toho největšího. □

Pomocí Eukleidova algoritmu lze dokázat také následující větu:

**Věta 2.3** (Bézoutova rovnost)**.** *Pro každou dvojici přirozených čísel $a, b$ existují celá čísla $u, v$ splňující*

$$\mathrm{NSD}(a, b) = u \cdot a + v \cdot b.$$

Formální důkaz této věty provedeme v obecnějším prostředí pro Eukleidovské obory, viz Věta 6.1. Princip je však snadný: zbytek po dělení lze vyjádřit jako lineární kombinace obou dělených čísel, neboť $a \bmod b = 1 \cdot a - (a \operatorname{div} b) \cdot b$, a tedy ve vznikající posloupnosti budou samé lineární kombinace původních čísel. Vše je dobře vidět z následujícího příkladu:

**Příklad.** Pro $\mathrm{NSD}(168, 396)$ dostáváme posloupnost $396 = 1 \cdot 396 + 0 \cdot 168$, $168 = 0 \cdot 396 + 1 \cdot 168$, $60 = 396 - 2 \cdot 168$, $48 = 168 - 2 \cdot 60 = -2 \cdot 396 + 5 \cdot 168$, $12 = 60 - 48 = 3 \cdot 396 - 7 \cdot 168$. Tedy $\mathrm{NSD}(168, 396) = 3 \cdot 396 - 7 \cdot 168$.

Druhou možností jak počítat NSD je pomocí (jednoznačných) prvočíselných rozkladů: protože $168 = 2^3 \cdot 3 \cdot 7$ a $396 = 2^2 \cdot 3^2 \cdot 11$, máme $\mathrm{NSD}(168, 396) = 2^2 \cdot 3 = 12$. Problém je, že kdybychom neměli jednoznačnost rozkladů, kdyby se např. číslo 396 rozkládalo na součin úplně jiných prvočísel než $2, 3, 11$, dostali bychom z jiného rozkladu jiný NSD, což je absurdní. Tím se dostáváme zpět k původní úloze, totiž k důkazu Základní věty aritmetiky. Jeho důsledkem je, že uvedená metoda výpočtu NSD funguje. (Skutečným protipříkladem na tuto metodu je např. následující situace v oboru $\mathbb{Z}[\sqrt{5}]$: $4 = 2 \cdot 2 = (\sqrt{5} - 1)(\sqrt{5} + 1)$. Z prvního rozkladu bychom vydedukovali $\mathrm{NSD}(2, 4) = 2$, z druhého $\mathrm{NSD}(2, 4) = 1$. Detaily viz Sekce 7.)

Pomocí Bézoutovy rovnosti dokážeme jedno pomocné tvrzeníčko. (Opět, kdybychom měli v ruce jednoznačnost prvočíselných rozkladů, bylo by tvrzení očividné.)

**Lemma 2.4.** *Buď $p$ prvočíslo a $a, b \in \mathbb{N}$. Platí-li $p \mid a \cdot b$, pak $p \mid a$ nebo $p \mid b$.*

*Důkaz.* Předpokládejme, že $p \nmid a$. Pak $\mathrm{NSD}(a, p) = 1$, protože je $p$ prvočíslo, a tedy podle Věty 2.3 existují čísla $u, v$ splňující $au + pv = 1$. Vynásobením obou stran rovnosti číslem $b$ dostaneme $abu + pvb = b$. Jelikož $p$ dělí oba sčítance na levé straně, dělí i $b$. □

Indukcí snadno odvodíme následující důsledek:

**Lemma 2.5.** *Buď $p$ prvočíslo a $a_1, \ldots, a_n \in \mathbb{N}$. Platí-li $p \mid a_1 \cdot \ldots \cdot a_n$, pak $p \mid a_i$ pro alespoň jedno $i$.*

Nyní můžeme přistoupit k důkazu jednoznačnosti prvočíselných rozkladů. Buď $a$ nejmenší číslo s nejednoznačným provčíselným rozkladem a uvažujme dva různé rozklady

$$a = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} = q_1^{l_1} \cdot \ldots \cdot q_n^{l_n}.$$

Protože $p_1 \mid a = q_1^{l_1} \cdot \ldots \cdot q_n^{l_n}$, musí existovat $i$ takové, že $p_1 \mid q_i$. Ovšem $q_i$ je prvočíslo, tedy $p_1 = q_i$. Pak ale uvažujme číslo $b = \frac{a}{p_1}$: to má také dva různé rozklady

$$b = p_1^{k_1 - 1} \cdot p_2^{k_2} \cdot \ldots \cdot p_m^{k_m} = q_1^{l_1} \cdot \ldots \cdot q_i^{l_i - 1} \cdot \ldots \cdot q_n^{k_n},$$

ale přitom $b < a$, což je spor s minimalitou $a$. Věta 2.1 je dokázána.

**Důsledek 2.6.** *Existuje nekonečně mnoho prvočísel.*

*Důkaz.* Pro spor předpokládejme, že jich je jen konečně mnoho a že $p_1, \ldots, p_n$ je jejich seznam. Uvažujme číslo $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$: to není dělitelné ani jedním z prvočísel, přitom musí mít nějaký prvočíselný rozklad. Spor. □

## 2.3. **Kongruence.**

Zápis pomocí kongruencí, zavedený Gaussem ve zmiňované knize *Disquisitiones Arithmeticae* (1801), značně usnadňuje počítání modulo dané číslo.

**Definice.** Pokud $a$ a $b$ dávají stejný zbytek po dělení $m$, tj. pokud $m \mid a - b$, budeme psát

$$a \equiv b \pmod{m}$$

(čteme *$a$ je kongruentní s $b$ modulo $m$*).

Uvědomte si, že relace „býti kongruentní modulo $m$“ je ekvivalence: je reflexivní, tj. $a \equiv a \pmod{m}$, protože $m \mid a - a$; je symetrická, protože $m \mid a - b \Leftrightarrow m \mid b - a$;

a je tranzitivní, protože

$$\left.\begin{array}{lll} a \equiv b \pmod m & \Rightarrow & m \mid a-b \\ b \equiv c \pmod m & \Rightarrow & m \mid b-c \end{array}\right\} \quad m \mid (a-b)+(b-c) = a-c.$$

Tedy znaménko kongruence je možné používat podobně jako rovnítko. Ukážeme si to na krátkém výpočtu (řešení je očividné, ale pro ilustraci jej podrobně rozepíšeme).

**Úloha.** Spočtěte $77^{333} + 12^{333} \bmod 6$.

*Řešení.* Protože $12 \equiv 0$, $7 \equiv 1$ a $11 \equiv -1 \pmod 6$, můžeme psát

$$77^{333} + 12^{333} \equiv 77^{333} + 0^{333} = 77^{333} = 7^{333} \cdot 11^{333} \equiv 1^{333} \cdot (-1)^{333} = -1 \pmod 6.$$

Výsledek je tedy 5. □

Při výpočtu jsme použili několik jednoduchých vlastností kongruencí, které nyní zformulujeme a dokážeme.

**Tvrzení 2.7.** *Nechť $a \equiv b \pmod m$ a $c \equiv d \pmod m$. Pak platí*

$$a + c \equiv b + d \pmod m, \quad a - c \equiv b - d \pmod m, \quad a \cdot c \equiv b \cdot d \pmod m$$

*a pro každé přirozené $k$ platí*

$$a^k \equiv b^k \pmod m.$$

*Důkaz.* Podle předpokladu $m \mid a-b$ a $m \mid c-d$. Tedy $m \mid (a-b)+(c-d) = (a+c)-(b+d)$ a podobně pro operaci $-$. Dále $m \mid (a-b)\cdot c$ a $m \mid (c-d)\cdot b$, a tedy $m \mid (a-b)\cdot c + (c-d)\cdot b = ac - bd$. Poslední tvrzení se snadno dokáže z předchozího vzorce indukcí: $a^2 = a \cdot a \equiv b \cdot b = b^2 \pmod m$, $a^3 = a^2 \cdot a \equiv b^2 \cdot b = b^3 \pmod m$ atd. □

V kongruenci smíme krátit číslem, které je nesoudělné s modulem $m$. Naopak, jsou-li všechna tři čísla v kongruenci soudělná, celý výraz můžeme zjednodušit tím, že společný faktor vykrátíme na obou stranách *i v modulu*. Formálně tyto vlastnosti vyjadřuje následující tvrzení.

**Tvrzení 2.8.** *Pro každá $a, b, c, m$ platí*

(1) $a \equiv b \pmod m \;\Leftrightarrow\; ca \equiv cb \pmod{cm}$;
(2) *jsou-li $c, m$ nesoudělná, pak* $a \equiv b \pmod m \;\Leftrightarrow\; ca \equiv cb \pmod m$.

*Důkaz.* (1) Tvrzení říká, že $m \mid a-b \;\Leftrightarrow\; cm \mid ca - cb = c(a-b)$, což je zřejmé.

(2) Protože $m \mid ca - cb = c(a-b)$ a čísla $c, m$ jsou nesoudělná, musí platit $m \mid a-b$. Opačná implikace plyne z Tvrzení 2.7. □

**Úloha.** Najděte všechna $x$ splňující a) $6x \equiv 9 \pmod{21}$, b) $10x \equiv 5 \pmod{21}$.

*Řešení.* a) Užitím Tvrzení 2.8 (1) dostaneme ekvivalentní podmínku $2x \equiv 3 \pmod 7$, která má očividně řešení $x = 5 + 7k$, $k \in \mathbb{Z}$.

b) Užitím Tvrzení 2.8 (2) dostaneme ekvivalentní podmínku $2x \equiv 1 \pmod{21}$, která má očividně řešení $x = 11 + 21k$, $k \in \mathbb{Z}$. □

2.4. **Eulerova věta.**

Pro motivaci připomeňme úlohu uvedenou za definicí kongruence: řešení bylo snadné především proto, že $12 \equiv 0$ a $77 \equiv -1$, přičemž tato čísla se snadno mocní. Zamyslete se nad následující úlohou.

**Úloha.** Zjistěte poslední cifru čísla $77^{333}$.

*Řešení.* Jinými slovy, spočtěte $77^{333} \bmod 10$. Můžeme psát $77^{333} \equiv 7^{333} \pmod{10}$. Nemáme-li však k dispozici lepší teorii, nezbývá, než zkoušet mocnit sedmičku. Záhy si všimneme, že se poslední cifry opakují s periodou 4, a protože $333 \bmod 4 = 1$, dostáváme $7^{333} \equiv 7^1 = 7 \pmod{10}$. □

To, že zbytky modulo dané číslo vykazují periodu jako v předchozí úloze, není náhoda, nýbrž pravidlo, které se nazývá *Eulerova věta*. Délku periody udává tzv. Eulerova funkce.

**Definice.** *Eulerova funkce* $\varphi(n)$ značí pro $n > 1$ počet čísel v intervalu $1, \dots, n-1$ nesoudělných s číslem $n$.

Např. $\varphi(10) = 4$, neboť s desítkou nesoudělná jsou právě čísla $1, 3, 7, 9$. Pro libovolné prvočíslo $p$ platí $\varphi(p) = p-1$, protože nesoudělná jsou s ním právě všechna menší čísla.

Výpočet Eulerovy funkce pouze z definice by byl pro větší než malá čísla poněkud pracný. Naštěstí existuje vzorec, pomocí něhož je snadné spočítat hodnotu $\varphi(n)$, pokud známe prvočíselný rozklad čísla $n$.

**Tvrzení 2.9.** *Je-li* $n = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}$ *prvočíselný rozklad čísla* $n > 1$*, pak*

$$\varphi(n) = p_1^{k_1-1}(p_1 - 1) \cdot \ldots \cdot p_m^{k_m-1}(p_m - 1).$$

**Příklad.** $\varphi(4056) = \varphi(2^3 \cdot 3^1 \cdot 13^2) = 2^2 \cdot 1 \cdot 3^0 \cdot 2 \cdot 13^1 \cdot 12 = 1248$.

Důkaz správnosti vzorce není úplně jednoduchý, necháme si jej na později. Teď se podíváme na samotnou Eulerovu větu.

**Věta 2.10** (Eulerova věta)**.** *Jsou-li čísla* $a, m$ *nesoudělná, pak*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

K důkazu se nám bude hodit jedno pomocné lemma. Označme

$$m^* = \{k \in \{1, \dots, m-1\} : \mathrm{NSD}(k, m) = 1\}.$$

Eulerovu funkci pak můžeme zapsat jako $\varphi(m) = |m^*|$.

**Lemma 2.11.** *Buď* $a, m$ *nesoudělná čísla a definujme*

$$\begin{aligned} f_a : m^* &\to m^* \\ x &\mapsto ax \bmod m. \end{aligned}$$

*Pak je zobrazení* $f_a$ *bijekce.*

*Důkaz.* Předně vzniká otázka: je vůbec $ax \bmod m$ vždy prvek $m^*$? Ovšemže ano: jsou-li obě čísla $a$, $x$ nesoudělná s $m$, pak je s $m$ nesoudělné i číslo $ax$ a tudíž podle Lemmatu 2.2 také $ax \bmod m$.

Dokážeme, že zobrazení $f_a$ je bijekce. Protože jde o zobrazení na konečné množině, stačí díky Lemmatu 1.2 ověřit prostost. Uvažujme tedy $x, y \in m^*$ taková, že $f_a(x) = f_a(y)$, tj. $ax \equiv ay \pmod{m}$. Podle Tvrzení 2.8 je $x \equiv y \pmod{m}$, tedy $x$ i $y$ dávají stejný zbytek po dělení $m$. Ovšem obě čísla jsou menší než $m$, takže musí být stejná. □

*Důkaz Eulerovy věty.* Uvažujme následující výpočet, kde $f_a$ je zobrazení definované v předchozím lemmatu:

$$\prod_{b\in m^*} b \;=\; \prod_{b\in m^*} f_a(b) \;=\; \prod_{b\in m^*} ab \bmod m \;\equiv\; \prod_{b\in m^*} ab \;=\; a^{\varphi(m)}\cdot \prod_{b\in m^*} b \pmod m.$$

První rovnost platí díky tomu, že v obou případech násobíme přes všechny prvky množiny $m^*$, pouze v různém pořadí. Označíme-li

$$c = \prod_{b\in m^*} b,$$

právě jsme dokázali, že

$$c \;=\; a^{\varphi(m)}\cdot c \pmod m.$$

Číslo $c$ je nesoudělné s $m$ (protože je součinem čísel nesoudělných s $m$), takže jím můžeme podle Tvrzení 2.8 krátit a dostáváme $1 \equiv a^{\varphi(m)} \pmod m$. □

Leonhard Euler publikoval tuto větu v roce 1736. Speciální případ pro $m$ prvočíslo bývá připisován Pierre de Fermatovi (objevuje se v jednom z jeho dopisů z roku 1640), a někdy se nazývá Malá Fermatova věta.

**Důsledek 2.12** (Malá Fermatova věta)**.** *Je-li $p$ prvočíslo a $p \nmid a$, pak*

$$a^{p-1} \equiv 1 \pmod p.$$

**Úloha.** Zjistěte poslední cifru čísla $77^{333}$.

*Řešení.* Použijeme Eulerovu větu: protože $\varphi(10) = 4$ a $\mathrm{NSD}(77, 10) = 1$, platí

$$77^{333} \;\equiv\; 7^{333} = 7^{4\cdot 83+1} \;\equiv\; (7^4)^{83}\cdot 7^1 \;\equiv\; 1^{83}\cdot 7 \;=\; 7 \pmod{10}.$$

(Z didaktických důvodů jsme vše detailně rozepsali, v praxi samozřejmě provedete většinu úvah zpaměti a budete psát rovnou $7^{333} \equiv 7^1 = 7$.) □

**Úloha.** Spočtěte $8^{7^6} \bmod 21$.

*Řešení.* Opět použijeme Eulerovu větu: protože $\varphi(21) = 12$ a $\mathrm{NSD}(8, 21) = 1$, stačí zjistit zbytek po dělení $7^6$ číslem 12. Tedy řešíme úlohu $7^6 \bmod 12$ a ještě jednou použijeme Eulerovu větu: protože $\varphi(12) = 4$ a $\mathrm{NSD}(7, 12) = 1$, stačí zjistit zbytek po dělení exponentu 6 číslem 4, což je 2. Tedy $7^6 \equiv 7^2 = 49 \equiv 1 \pmod{12}$ a $8^{7^6} \equiv 8^1 = 8 \pmod{21}$. □

**Úloha.** Řešte $x^6 + x + xy \equiv 1 \pmod 7$

*Řešení.* Pokud $7 \mid x$, pak 7 dělí levou stranu, a tedy $x^6 + x + xy$ nedává zbytek 1 po dělení 7. Takže budeme předpokládat, že 7 nedělí $x$ a použijeme malou Fermatovu větu, která říká, že $x^6 \equiv 1 \pmod 7$. Zadaná rovnice je tak ekvivalentní rovnici $1 + x + xy \equiv 1 \pmod 7$, tj. $7 \mid x(y + 1)$. Protože předpokládáme, že $7 \nmid x$, musí 7 dělit $y + 1$, tj. $y \equiv -1 \pmod 7$. Řešením je tedy množina

$$\big\{(x, y) : 7 \nmid x,\; y \equiv -1 \pmod 7\big\}.$$

□

**Poznámka.** Podle Lemmatu 2.11 pro každé $a$ nesoudělné s $m$ existuje právě jedno $b \in \{1, \ldots, m-1\}$ takové, že $ab \equiv 1 \pmod m$. Toto $b$ lze podle Eulerovy věty spočítat jako $b = a^{\varphi(m)-1}$. Jiný, efektivnější, postup dává Eukleidův algoritmus: pokud zjistíme Bézoutovy koeficienty $1 = \mathrm{NSD}(a, m) = ua + vm$, odpovědí je očividně číslo

$u \mod m$. Toto pozorování nachází aplikaci např. při výpočtu inverzních prvků v tělese $\mathbb{Z}_p$, viz kapitola o tělesech.

2.5. **Čínská věta o zbytcích.**

Čínská věta o zbytcích hovoří o řešeních soustav lineárních kongruencí. Byla známa již starověkým Číňanům (je uvedena v knize matematika Sun-c' ze 4. století) a o něco málo později i ve staré Indii.

**Věta 2.13** (Čínská věta o zbytcích)**.** *Nechť $m_1, \dots, m_n$ jsou po dvou nesoudělná přirozená čísla, označme $M = m_1 \cdot \ldots \cdot m_n$. Pak pro libovolná celá čísla $u_1, \dots, u_n$ existuje právě jedno $x \in \{0, \dots, M-1\}$, které řeší soustavu kongruencí*

$$x \equiv u_1 \pmod{m_1}, \quad \dots, \quad x \equiv u_n \pmod{m_n}.$$

*Důkaz.* Nejprve dokážeme jednoznačnost řešení. Předpokládejme, že soustava má dvě řešení $x, y \in \{0, \dots, M-1\}$, tj. pro každé $i$ platí

$$x \equiv y \equiv u_i \pmod{m_i}.$$

Pak pro každé $i$

$$m_i \mid x - y$$

a protože jsou čísla $m_i$ navzájem nesoudělná, dostáváme

$$M = m_1 \cdot \ldots \cdot m_n \mid x - y.$$

Ovšem $|x - y| < M$ (protože $x, y$ volíme z intervalu $0, \dots, M-1$), takže $x - y = 0$, tj. $x = y$.

Nyní dokážeme, že nějaké řešení vůbec existuje. Uvažujme zobrazení

$$f : \{0, \dots, M-1\} \to \{0, \dots, m_1 - 1\} \times \cdots \times \{0, \dots, m_k - 1\}$$
$$x \mapsto (x \bmod m_1, \dots, x \bmod m_k).$$

V předchozím odstavci jsme vlastně ukázali, že zobrazení $f$ je prosté. Přitom definiční obor i obor hodnot této funkce mají stejnou velikost $M$ (velikost kartézského součinu je součin velikostí činitelů), takže zobrazení $f$ musí být podle Lemmatu 1.2 i na. Tedy ke každé $k$-tici $(u_1, \dots, u_k)$ existuje právě jedno $x$, které se na něj zobrazuje; a to je hledané řešení soustavy. □

Důkaz věty bohužel vůbec nedává návod, jak řešení takové soustavy spočítat. Existují sice efektivní algoritmy, které řešení najdou, jsou ale poměrně složité a zde se jimi zabývat nebudeme. Zájemce odkazujeme na skripta z Počítačové algebry.

**Úloha.** Najděte všechna řešení soustavy kongruencí

$$x \equiv 1 \pmod 2, \quad x \equiv -1 \pmod 3, \quad x \equiv 2 \pmod 5.$$

*Řešení.* Čínská věta o zbytcích říká, že existuje právě jedno řešení $0 \leq x < 30$. Třetí kongruenci splňují čísla 2,7,12,17,22 a 27. Z první kongruence plyne, že hledané číslo je liché, zbývají tedy 7, 17 a 27, z nichž jedině 17 řeší druhou kongruenci. Všechna řešení soustavy jsou tedy tvaru $x = 17 + 30k$, $k \in \mathbb{Z}$. □

Traduje se, že motivací Čínské věty o zbytcích věty byl způsob, jakým čínští generálové počítali své vojáky. Generál věděl, že před bitvou měl 1000 vojáků, a chtěl je spočítat po bitvě. Nechal je tedy řadit do trojstupů, čtyřstupů, atd., a zjišťoval, kolik mu jich zbyde mimo řady. Jinými slovy, zjistil, kolik je počet vojáků modulo 3, modulo 4, atd. Z Čínské věty o zbytcích plyne, že pokud zvolil dostatek

nesoudělných čísel (součin $> 1000$), může jednoznačně určit celkový počet svých vojáků.

Na závěr pomocí Čínské věty o zbytcích dokážeme vzorec na výpočet Eulerovy funkce, tj. vztah

$$\varphi(p_1^{k_1} \cdot \ldots \cdot p_m^{k_m}) = p_1^{k_1-1}(p_1-1) \cdot \ldots \cdot p_m^{k_m-1}(p_m-1).$$

*Důkaz Tvrzení 2.9.* Dokážeme následující dvě vlastnosti:

(1) pro každé prvočíslo $p$ platí $\varphi(p^k) = p^{k-1}(p-1)$;
(2) pro každá dvě nesoudělná čísla $a, b$ platí $\varphi(ab) = \varphi(a) \cdot \varphi(b)$.

Uvedený vzorec snadno plyne z těchto dvou tvrzení: číslo $n$ rozložíme na součin $m$ po dvou nesoudělných mocnin $p_i^{k_i}$ a dostaneme

$$\varphi(n) \overset{(2)}{=} \varphi(p_1^{k_1}) \cdot \ldots \cdot \varphi(p_m^{k_m}) \overset{(1)}{=} p_1^{k_1-1}(p_1-1) \cdot \ldots \cdot p_m^{k_m-1}(p_m-1).$$

(1) V tomto speciálním případě je snadné spočítat *soudělná* čísla: jsou to právě čísla $p, 2p, 3p, \ldots, p^{k-1} \cdot p$. Vidíme, že jich je $p^{k-1}$. Všechna zbylá čísla jsou nesoudělná, takže $\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

(2) Uvažujme zobrazení

$$f : \{0, \ldots, ab-1\} \to \{0, \ldots, a-1\} \times \{0, \ldots, b-1\}$$
$$x \mapsto (x \bmod a, x \bmod b).$$

Podle Čínské věty o zbytcích je $f$ bijekce. Dále uvažujme pouze restrikci $f$ na množinu $(ab)^*$. To je prosté zobrazení, jehož definiční obor je množina $(ab)^*$ velikosti $\varphi(ab)$. Stačí tedy dokázat, že jeho oborem hodnot je množina $a^* \times b^*$ — pak, díky prostosti, bude $\varphi(ab) = |(ab)^*| = |a^* \times b^*| = |a^*| \cdot |b^*| = \varphi(a) \cdot \varphi(b)$, což chceme dokázat. Potřebujeme tedy ověřit, že

(a) $f$ zobrazuje množinu $(ab)^*$ do množiny $a^* \times b^*$, tj. že $\mathrm{NSD}(x, ab) = 1$ implikuje $\mathrm{NSD}(x \bmod a, a) = \mathrm{NSD}(x \bmod b, b) = 1$;
(b) $f$ zobrazuje množinu $(ab)^*$ <u>na</u> tuto množinu, tj. že pokud $\mathrm{NSD}(u, a) = \mathrm{NSD}(v, b) = 1$, pak to jediné $x$, které se zobrazuje na dvojici $(u, v)$, splňuje $\mathrm{NSD}(x, ab) = 1$.

Pro důkaz (a) si stačí uvědomit, že $\mathrm{NSD}(x \bmod a, a) = \mathrm{NSD}(x, a)$, a kdyby tato čísla byla soudělná, tím spíše by byla soudělná čísla $x, ab$. Podobně pro $b$.

Pro důkaz (b) uvažujme (to jediné) $x$ zobrazující se na $(u, v)$, tj. $u = x \bmod a$ a $v = x \bmod b$. Dosazením za $u, v$ plyne $\mathrm{NSD}(x, a) = \mathrm{NSD}(x \bmod a, a) = 1$ a $\mathrm{NSD}(x, b) = \mathrm{NSD}(x \bmod b, b) = 1$. Kdyby byla čísla $x, ab$ soudělná, pak by existovalo prvočíslo $p$, které dělí zároveň $x$ i $ab$, tedy podle Lemmatu 2.4 by $p$ dělilo $a$ nebo $b$, a tudíž by $x, a$ nebo $x, b$ byly soudělné, spor. □

## 3. Obory integrity

**Cíl.** *Zavedeme pojem oboru integrity, který abstraktně vymezuje prostředí, ve kterém lze studovat dělitelnost. Jako hlavní příklady představíme obor celých čísel a jeho rozšíření, a dále obory polynomů a formálních mocninných řad.*

3.1. **Definice oboru integrity.**

Celá čísla sdílí z hlediska dělitelnosti řadu vlastností s dalšími obory. Jak známo, dělitelnost lze studovat pro polynomy, ale také třeba pro různá rozšíření celých čísel (např. Gaussovská celá čísla, komplexní čísla s celočíselnými koeficienty) a další struktury. V různých oborech pak platí různě silná tvrzení: např. analogie Základní věty aritmetiky platí pro celočíselné i racionální polynomy i pro Gaussovská celá čísla. Polynomy nad tělesem i Gaussovská čísla lze dělit se zbytkem a platí pro ně Bézoutova rovnost, to ale není pravda např. pro celočíselné polynomy nebo pro polynomy více proměnných. A pro některá rozšíření $\mathbb{Z}$ neplatí ani Základní věta aritmetiky. V následujících čtyřech sekcích se budeme snažit udělat v uvedených vlastnostech a příkladech pořádek.

Abychom mohli studovat všechny zmíněné obory naráz, zavádí se obecná struktura nazývaná *obor integrity*, jejíž axiomy vystihují základní aritmetické vlastnosti. Jde o stejný princip, který vedl v lineární algebře k abstraktnímu pojmu tělesa a vektorového prostoru.

**Definice.** *Komutativním okruhem s jednotkou* $\mathbf{R}$ rozumíme množinu $R$, na které jsou definovány operace $+, -, \cdot$ a konstanty $0 \neq 1$ splňující pro každé $a, b, c \in R$ následující podmínky:

$$a + (b + c) = (a + b) + c, \qquad a + b = b + a, \qquad a + 0 = a,$$
$$a + (-a) = 0,$$
$$a \cdot (b \cdot c) = (a \cdot b) \cdot c, \qquad a \cdot b = b \cdot a, \qquad a \cdot 1 = a,$$
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

- Platí-li navíc podmínka
$$\text{pokud } a, b \neq 0, \text{ pak } a \cdot b \neq 0,$$
nazýváme $\mathbf{R}$ *obor integrity.*
- Platí-li navíc podmínka
$$\text{pro každé } a \neq 0 \text{ existuje } b \text{ splňující } a \cdot b = 1,$$
nazýváme $\mathbf{R}$ *těleso.* Značíme $b = a^{-1}$.

V zápise zpravidla vynecháváme závorky, násobení má vyšší prioritu než sčítání. Místo $a + (-b)$ píšeme $a - b$.

V matematice obecně je zvykem uvádět množinu axiomů tak krátkou, jak je to jen možné; spousta užitečných vlastností se tak do ní nevejde. Následující tvrzení ukazuje několik aritmetických pravidel, které z definice snadno plynou a v dalším textu je budeme zcela automaticky používat.

**Tvrzení 3.1.** *Buď* $\mathbf{R}$ *obor integrity,* $a, b, c \in R$. *Pak*

(1) *pokud* $a + c = b + c$, *pak* $a = b$;
(2) $a \cdot 0 = 0$;
(3) $-(-a) = a, \quad -(a + b) = -a - b$;
(4) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b), \quad (-a) \cdot (-b) = ab$.
(5) *pokud* $a \cdot c = b \cdot c$ $a$ $c \neq 0$, *pak* $a = b$;

*Důkaz.* (1) Je-li $a+c = b+c$, pak také $(a+c)+(-c) = (b+c)+(-c)$. Použitím axiomů dostaneme $(a+c)+(-c) = a+(c+(-c)) = a+0 = a$ a podobně $(b+c)+(-c) = b$, tedy $a = b$.

(2) Pomocí distributivity spočteme $0 + a \cdot 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ a krácením dostáváme $a \cdot 0 = 0$.

(3) Protože $0 = a + (-a) = -(-a) + (-a)$, krácením dostáváme $a = -(-a)$. Protože $0 = (a+b)+(-(a+b))$ a zároveň $0 = a+(-a)+b+(-b) = (a+b)+(-a-b)$, krácením dostáváme $-(a + b) = -a - b$.

(4) Protože $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0 = a \cdot b + (-(a \cdot b))$, krácením dostáváme $-(a \cdot b) = (-a) \cdot b$. Druhou rovnost dokážeme analogicky a užitím předchozího $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$.

(5) Protože $a \cdot c = b \cdot c$, platí $0 = a \cdot c - b \cdot c = (a - b) \cdot c$. Tedy aspoň jeden z prvků $c$, $a - b$ musí být 0. Protože předpokládáme $c \neq 0$, musí být $a - b = 0$, tedy $a = b$. □

### 3.2. **Příklady oborů integrity.**

**Příklad.** Celá čísla tvoří obor integrity.

**Příklad.** Každé těleso je oborem integrity.

*Důkaz.* Kdyby existovaly $a, b \neq 0$ takové, že $a \cdot b = 0$, pak $b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$, spor. □

Tělesa znáte z lineární algebry, připomeňme nejdůležitější příklady: racionální čísla $\mathbb{Q}$, reálná čísla $\mathbb{R}$, komplexní čísla $\mathbb{C}$ a konečná tělesa $\mathbb{Z}_p$, $p$ prvočíslo.

**Poznámka.** Je-li obor integrity konečný, pak je to těleso. (Speciálně $\mathbb{Z}_n$ je oborem integrity právě tehdy, když je $n$ prvočíslo. Více o konečných tělesech se dozvíte v poslední kapitole.) Máme-li totiž nenulové $a \in R$, uvažujme zobrazení

$$f_a : R \to R, \quad x \mapsto a \cdot x.$$

Podle Tvrzení 3.1(5) je toto zobrazení prosté, a protože jde o zobrazení na konečné množině, podle Lemmatu 1.2 je to bijekce. Inverzním prvkem k prvku $a$ je tedy $f_a^{-1}(1)$.

Další příklady oborů integrity můžeme odvodit z již známých oborů pomocí různých konstrukcí. Jednou z nich je tzv. *podobor*.

**Definice.** Buď $\mathbf{R}$ obor integrity a $S$ jeho podmnožina taková, že $0, 1 \in S$ a kdykoliv $a, b \in S$, pak také $-a \in S$, $a + b \in S$ a $a \cdot b \in S$. Vezmeme-li na této množině restrikce operací oboru $\mathbf{R}$, dostaneme také obor integrity (jsou-li všechny axiomy splněny na větší množině $R$, pak jistě i na její podmnožině $S$); takové obory se nazývají *podobory* oboru $\mathbf{R}$.

**Příklad.**

- Obor $\mathbb{Z}$ je podoborem oboru $\mathbb{Q}$, který je podoborem oboru $\mathbb{R}$, který je podoborem oboru $\mathbb{C}$.
- Množina $\{a + bi : a, b \in \mathbb{Z}\}$ tvoří podobor oboru $\mathbb{C}$. Nazývá se *Gaussovská celá čísla*.
- Množina $\{a + b\omega : a, b \in \mathbb{Z}\}$, kde $\omega = e^{2\pi i/3}$ je komplexní třetí odmocnina z jedné, tvoří podobor oboru $\mathbb{C}$. Nazývá se *Eisensteinova celá čísla*.

**Definice.** Buď $\mathbf{R}$ podobor oboru $\mathbf{S}$ a $a_1, \ldots, a_n \in S$. Definujeme $\mathbf{R}[a_1, \ldots, a_n]$ jako nejmenší podobor oboru $\mathbf{S}$ obsahující množinu $R$ i prvky $a_1, \ldots, a_n$. Tomuto oboru se říká *rozšíření* $\mathbf{R}$ *o prvky* $a_1, \ldots, a_n$.

Více o podoborech a rozšířeních se dozvíte v kapitole o okruzích a tělesech.

**Příklad.**

- $\mathbb{Z}[i]$ jsou Gaussovská celá čísla, $\mathbb{R}[i] = \mathbb{C}$.
- Obecněji,
$$\mathbb{Z}[\sqrt{s}] = \{a + b\sqrt{s} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$$
je oborem integrity pro libovolné celé číslo $s$ (rozumí se $\sqrt{-1} = i$).
- Můžeme uvažovat i komplikovanější obory, jako např.
$$\mathbb{Z}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Z}\}$$
nebo
$$\mathbb{Z}[\sqrt[3]{s}] = \{a + b\sqrt[3]{s} + c\sqrt[3]{s^2} : a, b, c \in \mathbb{Z}\}.$$
- Obecně
$$\mathbf{R}[u] = \{a_0 + a_1 u + \ldots + a_n u^n : n \in \mathbb{N}, a_0, \ldots, a_n \in R\}.$$
Pokud např. $\mathbf{R} = \mathbb{Z}$ a $u = \pi$, pak jsou tyto prvky pro různé koeficienty různé.

Rozšíření oboru celých čísel se objevují v řadě aplikací, především v teorii čísel. Ve skriptech jim je věnována samostatná Sekce 7, kde si mimo jiné ukážeme jejich využití při řešení jistého typu diofantických rovnic.

Druhou důležitou konstrukcí jsou polynomy a formální mocninné řady nad daným oborem.

**Definice.** *Polynomem proměnné $x$* nad oborem integrity $\mathbf{R}$ rozumíme formální výraz
$$a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,$$
nebo zkráceně
$$\sum_{i=0}^{n} a_i x^i,$$
kde $a_0, \ldots, a_n \in R$ a $a_n \neq 0$. Prvky $a_0, \ldots, a_n$ nazýváme *koeficienty* a symbol $x$ *proměnná*. (Implicitně se rozumí se $a_m = 0$ pro všechna $m > n$.) Číslo $n$ nazýváme *stupeň polynomu*, značíme $\deg f$. Prvek $a_n$ se nazývá *vedoucí koeficient* a $a_0$ *absolutní člen*. Polynom se nazývá *monický*, pokud je vedoucí člen 1. Je třeba speciálně dodefinovat nulový polynom; pro něj položíme $\deg 0 = -1$.

Na množině všech polynomů definujeme operace předpisy
$$\sum_{i=0}^{m} a_i x^i \; + \; \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{\max(m,n)} (a_i + b_i) x^i, \qquad - \sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{m} (-a_i) x^i,$$
$$(\sum_{i=0}^{m} a_i x^i) \cdot (\sum_{i=0}^{n} b_i x^i) = \sum_{i=0}^{m+n} \big( \sum_{j+k=i} a_j b_k \big) x^i.$$

Jak si za chvíli dokážeme, dostaneme obor integrity; značíme jej $\mathbf{R}[x]$.

**Definice.** *Formální mocninnou řadou proměnné $x$* nad oborem integrity $\mathbf{R}$ rozumíme formální výraz

$$\sum_{i=0}^{\infty} a_i x^i,$$

kde $a_0, a_1, \ldots \in R$; používáme podobnou terminologii. Tedy polynom je mocninná řada, v níž je jen konečně mnoho nenulových koeficientů. Speciálně $0 = \sum_{i=0}^{\infty} 0x^i$. (Jde o *formální výrazy*, nikoliv o funkce nebo součty! Otázky typu konvergence nás tedy vůbec nezajímají.)

Na množině všech formálních mocninných řad definujeme analogicky operace

$$\sum_{i=0}^{\infty} a_i x^i \; + \; \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i, \qquad - \sum_{i=0}^{\infty} a_i x^i = \sum (-a_i) x^i,$$

$$(\sum_{i=0}^{\infty} a_i x^i) \cdot (\sum_{i=0}^{\infty} b_i x^i) = \sum_{i=0}^{\infty} \big( \sum_{j+k=i} a_j b_k \big) x^i.$$

Jak si nyní dokážeme, dostaneme obor integrity; značíme jej $\mathbf{R}[[x]]$. Polynomy zřejmě tvoří jeho podobor, protože součet i součin dvou polynomů je opět polynom.

**Tvrzení 3.2.** *Je-li $\mathbf{R}$ obor integrity, pak je $\mathbf{R}[[x]]$ také obor integrity.*

*Důkaz.* Ověření všech rovností (tj. kromě poslední vlastnosti) z definice oboru je čistě mechanická práce. Rovnosti pro sčítání jsou očividné, komutativita násobení také, a $(\sum a_i x^i) \cdot (1 + 0 + 0 + \ldots)$ dává řadu $\sum (\sum_{j+k=i} a_j b_k) x^i$, kde všechny $b_i$ kromě $b_0$ jsou nulové, tedy výsledkem je opět $\sum a_i x^i$. Asociativita je obtížnější: máme $(\sum a_i x^i) \cdot ((\sum b_i x^i) \cdot (\sum c_i x^i)) = (\sum a_i x^i) \cdot ((\sum (\sum_{k+l=i} b_k c_l) x^i) = \sum (\sum_{j+k+l=i} a_j b_k c_l) x^i)$, a stejně vyjde i analogický výpočet $((\sum a_i x^i) \cdot (\sum b_i x^i)) \cdot (\sum c_i x^i)$. Distributivita se prověří podobně.

Zajímavější je důkaz poslední vlastnosti. Buď $f = \sum a_i x^i$ a $g = \sum b_i x^i$ dva nenulové prvky $\mathbf{R}[[x]]$ a označme $m, n$ nejmenší indexy takové, že $a_m, b_n \neq 0$. Uvažujeme-li v součinu $f \cdot g$ koeficient u $x^{m+n}$, dostáváme vyjádření

$$\sum_{j+k=m+n} a_j b_k = \underbrace{a_0 b_{m+n} + \ldots + a_{m-1} b_{n+1}}_{0} + \underbrace{a_m b_n}_{\neq 0} + \underbrace{a_{m+1} b_{n-1} + \ldots + a_{m+n} b_0}_{0}.$$

Protože $a_0 = \ldots = a_{m-1} = 0 = b_0 = \ldots = b_{n-1}$ a zároveň $a_m, b_n \neq 0$, vidíme, že $a_m b_n \neq 0$ a tak je tento koeficient nenulový. □

**Důsledek 3.3.** *Je-li $\mathbf{R}$ obor integrity, pak je $\mathbf{R}[x]$ také obor integrity.*

*Důkaz.* Plyne z toho, že $\mathbf{R}[x]$ je podoborem oboru $\mathbf{R}[[x]]$. □

Je třeba striktně rozlišovat mezi polynomem $f \in R[x]$ jako formálním výrazem (tento se bude zapisovat výhradně $f$, bez uvedení proměnné) a jeho *hodnotou po dosazení* nějakého prvku $u \in R$, kterou pro polynom

$$f = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$$

definujeme předpisem

$$f(u) = a_0 + a_1 u + \ldots + a_n u^n \in R$$

(všechna mocnění, násobení i sčítání provádíme v oboru $\mathbf{R}$). Např. je-li $f = x^2+1 \in \mathbb{Z}_3[x]$, pak v oboru $\mathbb{Z}_3$ máme $f(0) = 1$, $f(1) = f(2) = 2$. Přitom pro polynom $g = x^4 + 1 \in \mathbb{Z}_3[x]$ dostáváme stejné hodnoty $g(0) = 1$, $g(1) = g(2) = 2$; jsou to tedy *různé polynomy*, které definují *stejné funkce* na množině $\{0, 1, 2\}$.

Poznamenejme, že pojem „hodnota mocninné řady“ (ani pojem konvergence a divergence) nedává pro řadu oborů žádný smysl, protože není jasné, co by se mělo rozumět nekonečným součtem. Vzpomeňte si na definici sumy z analýzy a uvědomte si, jaké další vlastnosti tělesa $\mathbb{R}$, event. $\mathbb{C}$, k ní byly potřeba. Srovnejte např. s konečnými tělesy $\mathbb{Z}_p$.

**Definice.** *Polynomem v proměnných* $x_1, \dots, x_n$ nad oborem integrity $\mathbf{R}$ rozumíme formální výraz

$$\sum_{k_1,\dots,k_n=0}^{N} a_{k_1,\dots,k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n},$$

kde koeficienty $a_{k_1,\dots,k_n}$ jsou prvky $R$. Podobně, *formální mocninnou řadou v proměnných* $x_1, \dots, x_n$ nad $\mathbf{R}$ rozumíme formální výraz

$$\sum_{k_1,\dots,k_n=0}^{\infty} a_{k_1,\dots,k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n}.$$

Operace na těchto výrazech definujeme analogicky jako v případě jedné proměnné. Polynomy i mocninné řady více proměnných také tvoří obory integrity, které značíme $\mathbf{R}[x_1, \dots, x_n]$, resp. $\mathbf{R}[[x_1, \dots, x_n]]$. Toto tvrzení lze dokázat velmi snadno pomocí následujícího pozorování: mocninné řady dvou proměnných vzniknou z mocninných řad jedné proměnné přidáním druhé proměnné. Čili dvojí aplikací Tvrzení 3.2 dostaneme, že $\mathbf{R}[[x, y]] = (\mathbf{R}[[x]])[[y]]$ je obor integrity, atd. indukcí.

Poznamenejme, že se nemusíme omezovat pouze na případ konečně mnoha proměnných. Je-li $X$ libovolná neprázdná množina, definujeme $\mathbf{R}[X]$ jako obor všech polynomů v konečně mnoha proměnných, které se vybírají z množiny $X$.

## 4. Základní pojmy teorie dělitelnosti

**Cíl.** *Ujasníme si, které prvky jsou z hlediska dělitelnosti nerozlišitelné (relace asociovanosti, souvislost s invertibilními prvky), což nám umožní na relaci dělitelnosti pohlížet jako na uspořádání. Zavedeme největší společný dělitel a definujeme analogii k pojmu prvočísla, tzv. ireducibilní prvky.*

V celé sekci budeme uvažovat nějaký pevně daný obor integrity $\mathbf{R}$.

### 4.1. Invertibilní prvky.

**Definice.** Řekneme, že $a$ *dělí* $b$ v oboru $\mathbf{R}$ (píšeme $a \mid b$), pokud existuje $c \in R$ takové, že $b = ac$. Řekneme, že prvky $a$ a $b$ jsou *asociované* (píšeme $a \parallel b$), pokud $a \mid b$ a $b \mid a$. Prvek $a$ se nazývá *invertibilní*, pokud $a \parallel 1$, tj. existuje $b$ takové, že $ab = 1$; toto $b$ obvykle značíme $a^{-1}$. Dělitel prvku $a$ se nazývá *vlastní*, jestliže není asociovaný ani s 1, ani s $a$.

**Tvrzení 4.1.** *Dva prvky $a, b$ jsou asociované právě tehdy, když existuje invertibilní prvek $q$ takový, že $a = bq$.*

*Důkaz.* ($\Leftarrow$) Protože $a = bq$, platí $b \mid a$. Protože taky $b = aq^{-1}$, platí $a \mid b$.

($\Rightarrow$) Protože $b \mid a$, můžeme psát $a = bu$, a protože $a \mid b$, můžeme psát $b = av$, pro nějaká $u, v$. Tedy $a = bu = avu$ a krácením dostáváme $uv = 1$, čili $u, v \parallel 1$. □

**Příklad.**

- V tělese je každý nenulový prvek invertibilní. Tedy $a \parallel b$ pro každé $a, b \neq 0$.
- V oboru $\mathbb{Z}$ jsou invertibilní pouze prvky $\pm 1$. Tedy $a \parallel b$ právě tehdy, když $a = \pm b$.
- V oboru $\mathbb{Z}[i]$ jsou invertibilní pouze prvky $\pm 1, \pm i$. Tedy $a \parallel b$ právě tehdy, když $a = \pm b$ nebo $\pm ib$.
- V oboru $\mathbf{R}[x]$ jsou invertibilní právě polynomy stupně 0, jejichž člen je invertibilní v oboru $\mathbf{R}$.

**Příklad.** Pozor na následující záludnost!

- $3x+6 \parallel x+2$ v oboru $\mathbb{Q}[x]$, protože $3x+6 = 3 \cdot (x+2)$ a $x+2 = \frac{1}{3} \cdot (3x+6)$;
- $3x + 6 \nparallel x + 2$ v oboru $\mathbb{Z}[x]$, protože $\frac{1}{3} \notin \mathbb{Z}[x]$.

4.2. **Dělitelnost jako uspořádání.**

Uvažujme na množině $R$ relaci dělitelnosti. Je reflexivní: $a \mid a$, protože $a = a \cdot 1$. Je tranzitivní, protože pokud $a \mid b$ a $b \mid c$, tj. $b = ax$ a $c = by$, pak $c = a(xy)$, tj. $a \mid c$. Z toho ihned plyne následující pozorování:

**Pozorování 4.2.** *Relace $\parallel$ je ekvivalence na množině $R$.*

K tomu, aby byla relace $\mid$ uspořádání, chybí antisymetrie. Ta téměř nikdy splněna není, neboť v každém oboru platí $1 \mid -1$ a zároveň $-1 \mid 1$. (Výjimkou jsou obory charakteristiky 2, kde $1 = -1$ — např. obor $\mathbb{Z}_2[x]$.) Tuto vadu lze napravit tak, že z každého bloku ekvivalence $\parallel$ na množině $R$ vybereme po jednom zástupci. Označíme-li množinu takto vybraných prvků $\bar{R}$, pak $(\bar{R}, |)$ je uspořádanou množinou.

Volbu množiny $\bar{R}$ můžeme provést mnoha způsoby. V některých oborech však existuje přirozený výběr, proto se zavádějí následující konvence:

**Příklad.**

- V tělese $\mathbf{T}$ má ekvivalence $\parallel$ pouze dva bloky: $\{0\}$ a $T \setminus \{0\}$.
- V oboru $\mathbb{Z}$ z dvou asociovaných čísel vybereme to nezáporné, tj. $\bar{\mathbb{Z}} = \mathbb{N} \cup \{0\}$.
- V oboru $\mathbb{Z}[i]$ ze čtyřech asociovaných čísel vybereme to $a + bi$, kde $a > 0$, $b \geq 0$ (resp. nulu ve svém bloku).
- V oboru $\mathbb{Z}[x]$ z dvou asociovaných polynomů vybereme ten s nezáporným vedoucím koeficientem (resp. nulový polynom ve svém bloku).
- V oboru $\mathbf{T}[x]$, $\mathbf{T}$ těleso, volíme z navzájem asociovaných polynomů ten monický (resp. nulový polynom ve svém bloku).

4.3. **Největší společný dělitel.**

**Definice.** Řekneme, že $c = \mathrm{NSD}(a, b)$ (*největší společný dělitel*), pokud

(1) $c \mid a$ a $c \mid b$ (tj. $c$ je společný dělitel);
(2) kdykoliv $d \mid a$ a $d \mid b$, pak $d \mid c$ (tj. $c$ je největší).

Řekneme, že $c = \mathrm{NSN}(a, b)$ (*nejmenší společný násobek*), pokud

$$c \cdot \mathrm{NSD}(a, b) = a \cdot b.$$

NSD a NSN není určen jednoznačně (pokud vůbec existuje, pro danou dvojici prvků). Například,

- v oboru $\mathbb{Z}$ platí $\mathrm{NSD}(4,10) = 2$, ale také $\mathrm{NSD}(4,10) = -2$,
- v oboru $\mathbb{Q}[x]$ platí $\mathrm{NSD}(x^2+2x+1, x^2-1) = x-1$, ale také $\mathrm{NSD}(x^2+2x+1, x^2-1) = -5x+5$.

Na druhou stranu, pokud $\mathrm{NSD}(a,b) = c$ a $\mathrm{NSD}(a,b) = d$, pak $c$ i $d$ jsou společní dělitelé $a, b$, a tedy $c \mid d$ a zároveň $d \mid c$. Čili NSD a NSN jsou určené *jednoznačně až na asociovanost*.

Operátory NSD a NSN se obvykle používají ve významu funkce dvou parametrů. Jednoznačnosti lze dosáhnout trikem popsaným v předchozím odstavci: máme-li dánu množinu $\bar{R}$, pak definujeme hodnotu $\mathrm{NSD}(a,b)$ jako to jediné $c \in \bar{R}$ splňující $\mathrm{NSD}(a,b) = c$. Pro představu je šikovné mít na paměti, že

$$\mathrm{NSD}(a,b) = \inf\{a,b\} \qquad \text{a} \qquad \mathrm{NSN}(a,b) = \sup\{a,b\},$$

kde sup a inf se rozumí v uspořádané množině $(\bar{R}, |)$.

Na závěr poznamenejme, že v některých oborech NSD a NSN nemusí pro danou dvojici prvků vůbec existovat. Uvažujme obor $\mathbb{Z}[\sqrt{5}]$ a prvky 4 a $2+2\sqrt{5}$. Dá se dokázat, že čísla 2 a $1+\sqrt{5}$ jsou *maximálními* společnými děliteli obou prvků, tedy žádný *největší* společný dělitel neexistuje. Tento fakt je snadným důsledkem teorie v Sekci 7.

### 4.4. **Ireducibilní prvky.**

**Definice.** Neinvertibilní prvek $a$ se nazývá *ireducibilní*, pokud nemá vlastní dělitele. Jinými slovy, pokud pro každý rozklad $a = bc$ platí $b \parallel 1$ nebo $c \parallel 1$.

**Příklad.**

- V tělesech žádné ireducibilní prvky nejsou.
- V oboru $\mathbb{Z}$ jsou ireducibilní právě prvočísla a čísla tvaru $-p$, $p$ prvočíslo.
- V oboru $\mathbb{Z}[i]$ jsou ireducibilní následující prvky:
  - $a + 0i$ právě tehdy, když je $a$ prvočíslo a $a \equiv 3 \pmod 4$;
  - $a + bi$, $b \neq 0$, právě tehdy, když $a^2 + b^2$ je prvočíslo.
- V oboru $\mathbb{C}[x]$ jsou ireducibilní právě polynomy stupně 1.
- V oboru $\mathbb{R}[x]$ jsou ireducibilní právě polynomy stupně 1 a ty polynomy stupně 2, které nemají reálný kořen.

**Příklad.** V tabulce jsou uvedeny rozklady polynomů na součin ireducibilních v různých oborech:

| | $x^2+1$ | $2x^2+2$ | $x^2-2$ | $x^4+2x^2+1$ |
|---|---|---|---|---|
| $\mathbb{Z}[x]$ | ireducibilní | $2\cdot(x^2+1)$ | ireducibilní | $(x^2+1)^2$ |
| $\mathbb{Q}[x]$ | ireducibilní | ireducibilní | ireducibilní | $(x^2+1)^2$ |
| $\mathbb{R}[x]$ | ireducibilní | ireducibilní | $(x-\sqrt{2})(x+\sqrt{2})$ | $(x^2+1)^2$ |
| $\mathbb{C}[x]$ | $(x-i)(x+i)$ | $(2x-2i)(x+i)$ | $(x-\sqrt{2})(x+\sqrt{2})$ | $(x-i)^2(x+i)^2$ |
| $(\mathbb{Z}[i])[x]$ | $(x-i)(x+i)$ | * | ireducibilní | $(x-i)^2(x+i)^2$ |

* Chybějícím polynomem je $(1-i)(1+i)(x-i)(x+i)$ — pozor na rozklad dvojky, která není v $\mathbb{Z}[i]$ ireducibilní!

## 5. Gaussovské obory

**Cíl.** *Budeme zkoumat obory, ve kterých platí analogie Základní věty aritmetiky. Ukážeme, jak tato vlastnost souvisí s existencí největších společných dělitelů.*

**Definice.** Obor integrity se nazývá *Gaussovský*, pokud má každý neinvertibilní nenulový prvek jednoznačný rozklad na ireducibilní činitele.

*Rozkladem prvku $a$ na ireducibilní činitele* rozumíme zápis $a = b_1 \cdot b_2 \cdot \ldots \cdot b_n$, kde $b_1, \ldots, b_n$ jsou ireducibilní prvky. *Jednoznačností rozkladu* prvku $a$ pak rozumíme jednoznačnost *až na pořadí a asociovanost*, neboli následující vlastnost: jsou-li $a = b_1 \cdot b_2 \cdot \ldots \cdot b_m = c_1 \cdot c_2 \cdot \ldots \cdot c_n$ dva ireducibilní rozklady prvku $a$, pak $m = n$ a existuje permutace indexů $\pi$ taková, že $b_i \parallel c_{\pi(i)}$ pro každé $i$.

(Definice jednoznačnosti je motivována následujícím pozorováním: v oboru $\mathbb{Z}$ můžeme psát $6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3)$. Formálně vzato, jde o tři různé rozklady. Přesto je rozumné je považovat za „stejné“: liší se pouze pořadím a volbou z navzájem asociovaných prvků.)

**Příklad.** Řada oborů integrity je Gaussovských:

- Tělesa jsou Gaussovské obory; podmínka z definice je prázdná.
- Obor $\mathbb{Z}$ je Gaussovský, jak říká Základní věta aritmetiky 2.1.
- Obor $\mathbb{Z}[i]$ je Gaussovský, jak bude dokázáno později.
  Obecněji, některé obory $\mathbb{Z}[\sqrt{s}]$ jsou Gaussovské, např. pro $s = -1, \pm 2, 3$, některé ne, např. pro $s = -3, 5$.
- (Gaussova věta) *Je-li* $\mathbf{R}$ *Gaussovský obor, pak je* $\mathbf{R}[x_1, \ldots, x_n]$ *také Gaussovský obor.*

**Příklad.** Obor $\mathbb{Z}[\sqrt{5}]$ *není* Gaussovský — prvek 4 má dva různé rozklady na ireducibilní činitele:

$$4 = 2 \cdot 2 = (\sqrt{5} - 1)(\sqrt{5} + 1).$$

Je zřejmé, že prvky 2 a $\sqrt{5} \pm 1$ jsou navzájem neasociované, protože všechny prvky dělitelné 2 mají sudé koeficienty. Fakt, že jsou tyto tři prvky skutečně ireducibilní, není očividný, ale je opět snadným důsledkem teorie v Sekci 7.

To, že naším protipříkladem na existenci NSD i jednoznačnost rozkladů byl v obou případech obor $\mathbb{Z}[\sqrt{5}]$, není náhoda. Obě vlastnosti spolu totiž těsně souvisejí. Z existence a jednoznačnosti rozkladů plyne existence NSD, a za jistých předpokladů platí i opak. Této souvislosti je věnován zbytek sekce.

Pro práci s Gaussovskými obory je stěžejní následující pozorování o tom, jak vypadají dělitelé daného prvku.

**Tvrzení 5.1.** *Buď* $\mathbf{R}$ *Gaussovský obor,* $a \in R$ *a mějme rozklad*

$$a = a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}$$

*na ireducibilní činitele, přičemž* $a_i \nparallel a_j$ *pro* $i \neq j$. *Pak* $b \mid a$ *právě tehdy, když*

$$b \parallel a_1^{l_1} \cdot \ldots \cdot a_n^{l_n}$$

*pro nějaká* $0 \leq l_i \leq k_i$.

*Důkaz.* Jedna implikace je snadná: zřejmě $a_1^{l_1} \cdot \ldots \cdot a_n^{l_n} \mid a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}$, neboť $a \parallel b \cdot (a_1^{k_1-l_1} \cdot \ldots \cdot a_n^{k_n-l_n})$. Jak dokázat opačnou implikaci? Nechť $b \mid a = a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}$. Tedy $a = b \cdot c$ pro nějaké $c \in R$ a označme

$$b = b_1 \cdot \ldots \cdot b_r \quad \text{a} \quad c = c_1 \cdot \ldots \cdot c_s$$

ireducibilní rozklady prvků $b, c$. Pak

$$a = a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} = b_1 \cdot \ldots \cdot b_r \cdot c_1 \cdot \ldots \cdot c_s$$

jsou dva rozklady prvku $a$, a tedy z jednoznačnosti plyne, že ke každému $i = 1, \ldots, r$ existuje $j$ takové, že $b_i \parallel a_j$, přičemž pro každé $j = 1, \ldots, n$ existuje nejvýše $k_j$ indexů $i$ takových, že $b_i \parallel a_j$. Z toho vyplývá, že $b \parallel a_1^{l_1} \cdot \ldots \cdot a_n^{l_n}$ pro nějaká $0 \leq l_i \leq k_i$. □

Snadným důsledkem je, že v Gaussovských oborech platí analogie Lemmatu 2.4, které tvořilo klíčový krok důkazu Základní věty aritmetiky.

**Tvrzení 5.2.** *Buď* **R** *Gaussovský obor a $p \in R$ ireducibilní prvek. Platí-li $p \mid a \cdot b$, pak $p \mid a$ nebo $p \mid b$.*

Ideu důkazu předvedeme na příkladě: pokud $p \mid 14 \cdot 12 = 2 \cdot 7 \cdot 2^2 \cdot 3$, pak $p$ je buď 2 (pak $p \mid 14$ i $p \mid 12$), nebo 3 (pak $p \mid 12$), nebo 7 (pak $p \mid 14$).

*Důkaz.* Označme $a = a_1 \cdot \ldots \cdot a_m$ a $b = b_1 \cdot \ldots \cdot b_n$ ireducibilní rozklady prvků $a, b$. Protože

$$p \mid a_1 \cdot \ldots \cdot a_m \cdot b_1 \cdot \ldots \cdot b_n,$$

musí $p$ mít podle Tvrzení 5.1 rozklad, který obsahuje některé z prvků $a_1, \ldots a_m$, $b_1, \ldots, b_n$. Protože je $p$ ireducibilní, musí být $p \parallel a_i$ nebo $p \parallel b_i$ pro nějaké $i$. V prvním případě $p \mid a$, v druhém $p \mid b$. □

**Poznámka.** Prvek $p$ splňující implikaci

$$p \mid a \cdot b \;\Rightarrow p \mid a \text{ nebo } p \mid b$$

se nazývá *prvočinitel*. Právě jsme dokázali, že v Gaussovských oborech jsou ireducibilní prvky prvočinitelé, obecně to však neplatí: např. v oboru $\mathbb{Z}[\sqrt{5}]$ je 2 ireducibilní, avšak $2 \mid (\sqrt{5}-1)(\sqrt{5}+1)$ a zároveň $2 \nmid (\sqrt{5} \pm 1)$. Dále si všimněte, že prvočinitelé jsou vždy ireducibilní: kdybychom měli rozklad $p = ab$, pak zřejmě $a \mid p$ a $b \mid p$, a protože $p \mid p = ab$, z předpokladu, že $p$ je prvočinitel, plyne $p \mid a$ nebo $p \mid b$; tedy $a \parallel p$ nebo $b \parallel p$, čili jde o triviální rozklad. (Tedy v Gaussovských oborech oba pojmy splývají.)

Jiným snadným důsledkem Tvrzení 5.1 je existence největších společných dělitelů.

**Tvrzení 5.3.** *V Gaussovských oborech existuje NSD všech dvojic prvků.*

Ideu důkazu předvedeme na příkladě: $\mathrm{NSD}(540, 336) = \mathrm{NSD}(2^2 \cdot 3^3 \cdot 5, 2^4 \cdot 3 \cdot 7) = \mathrm{NSD}(2^2 \cdot 3^3 \cdot 5^1 \cdot 7^0, 2^4 \cdot 3^1 \cdot 5^0 \cdot 7^1) = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 12$.

*Důkaz.* Buď

$$a \parallel c_1^{k_1} \cdot \ldots \cdot c_n^{k_n} \quad \text{a} \quad b \parallel c_1^{l_1} \cdot \ldots \cdot c_n^{l_n}$$

ireducibilní rozklady prvků $a, b$, přičemž předpokládáme $c_i \nparallel c_j$ pro $i \neq j$. (Uvědomte si, že rozklady můžeme zvolit v této speciální formě, tj. se stejnými ireducibilními prvky: do rozkladu případně doplníme činitele v nulté mocnině.) Položme

$$c = c_1^{\min(k_1,l_1)} \cdot \ldots \cdot c_n^{\min(k_n,l_n)}$$

a ukažme, že $\mathrm{NSD}(a, b) = c$. Z Tvrzení 5.1 plyne, že $d$ je společný dělitel $a, b$ právě tehdy, když $d \parallel c_1^{r_1} \cdot \ldots \cdot c_n^{r_n}$ pro nějaká $r_1, \ldots, r_n \geq 0$ splňující zároveň $r_i \leq k_i$ a $r_i \leq l_i$ pro všechna $i$. Je zřejmé, že největší (vzhledem k dělitelnosti) je takové $d$, kde $r_i = \min(k_i, l_i)$. □

Tím se dostáváme k slibované souvislosti ireducibilních rozkladů a existence NSD. Už víme, že v Gaussovských oborech NSD existují. K tomu, abychom dokázali Gaussovskost pomocí existence NSD chybí jedna důležitá věc: nějaká analogie indukce. Tu není možné aplikovat přímočaře, neboť obory integrity obecně nejsou dobře uspořádané. Pomůžeme si podmínkou, že žádný prvek „nelze dělit do nekonečna“.

**Věta 5.4.** *Buď* $\mathbf{R}$ *obor integrity. Pak* $\mathbf{R}$ *je Gaussovský právě tehdy, když*

(1) *existuje NSD všech dvojic prvků;*
(2) *neexistuje posloupnost* $a_1, a_2, a_3, \ldots \in R$ *taková, že* $a_{i+1} \mid a_i$ *a* $a_i \nmid a_{i+1}$.

K důkazu se nám bude ještě jednou hodit analogie Lemmatu 2.4: tentokrát dokázaná za předpokladu existence NSD. Protože obecně nemáme k dispozici Bézoutovu rovnost, budeme muset postupovat obezřetněji než v důkaze zmíněného lemmatu v Sekci 2.

**Lemma 5.5.** *Buď* $\mathbf{R}$ *obor integrity a* $a, b, c \in R$ *takové, že existuje* $\mathrm{NSD}(a, b)$ *i* $\mathrm{NSD}(ac, bc)$. *Pak*

$$\mathrm{NSD}(ac, bc) = c \cdot \mathrm{NSD}(a, b).$$

*Důkaz.* Vzhledem k tomu, že NSD je definován *až na asociovanost*, stačí dokázat, že levá strana rovnosti dělí pravou a naopak. Označme $u = \mathrm{NSD}(ac, bc)$.

Nejprve dokážeme, že $u \mid c \cdot \mathrm{NSD}(a, b)$. Protože $u \mid ac$, existuje $x$ s vlastností $ac = ux$. Protože $u \mid bc$, existuje $y$ s vlastností $bc = uy$. Protože $c$ je společný dělitel $ac$, $bc$, platí $c \mid u$, a tedy existuje $z$ s vlastností $u = cz$. Dostáváme $ac = czx$ a $bc = czy$ a krácením získáme vztahy $a = zx$ a $b = zy$. Tedy $z$ je společný dělitel $a, b$, tedy $z$ dělí $\mathrm{NSD}(a, b)$, a tudíž $u = cz \mid c \cdot \mathrm{NSD}(a, b)$.

Naopak, protože $\mathrm{NSD}(a, b)$ dělí $a$ i $b$, tak $c \cdot \mathrm{NSD}(a, b)$ dělí $ac$ i $bc$, a tudíž musí dělit i jejich největšího společného dělitele. □

**Lemma 5.6.** *Předpokládejme, že v oboru* $\mathbf{R}$ *existují NSD všech dvojic prvků a buď* $p \in R$ *ireducibilní prvek. Platí-li* $p \mid a \cdot b$, *pak* $p \mid a$ *nebo* $p \mid b$.

*Důkaz.* Předpokládejme, že $p \nmid a$. Pak $\mathrm{NSD}(a, p) = 1$, protože je $p$ ireducibilní, a tedy podle Lemmatu 5.5

$$\mathrm{NSD}(pb, ab) = b \cdot \mathrm{NSD}(p, a) = b.$$

Ovšem $p$ je společným dělitelem $pb$ a $ab$, tedy $p \mid \mathrm{NSD}(pb, ab) = b$. □

*Důkaz Věty 5.4.* ($\Rightarrow$) Předpokládejme, že je obor $\mathbf{R}$ Gaussovský. Podmínka (1) byla dokázána v Tvrzení 5.3, zbývá ověřit (2). Pro spor předpokládejme existenci takové posloupnosti a označme

$$a_1 = b_1^{k_1^{(1)}} b_2^{k_2^{(1)}} \cdot \ldots \cdot b_n^{k_n^{(1)}}$$

ireducibilní rozklad prvku $a_1$. Protože $a_i \mid a_1$ pro všechna $i = 2, 3, \dots$, podle Tvrzení 5.1

$$a_i \parallel b_1^{k_1^{(i)}} b_2^{k_2^{(i)}} \cdot \ldots \cdot b_n^{k_n^{(i)}}$$

pro nějaká $k_1^{(i)}, \dots, k_n^{(i)}$, přičemž

$$\begin{aligned} k_1^{(1)} &\geq k_1^{(2)} \geq k_1^{(3)} \geq \dots \\ &\dots \\ k_n^{(1)} &\geq k_n^{(2)} \geq k_n^{(3)} \geq \dots \end{aligned}$$

Protože $a_{i+1} \nparallel a_i$, musí pro každé $i$ existovat $j$ takové, že $k_j^{(i)} > k_j^{(i+1)}$. Tedy součet exponentů $k_1^{(i)} + \dots + k_n^{(i)}$ s rostoucím $i$ ostře klesá. Protože je tento součet nezáporné celé číslo, nemůže se snižovat do nekonečna. Spor.

($\Leftarrow$) Opět provedeme ve dvou krocích. Začneme důkazem, že každý prvek má ireducibilní rozklad, a poté ukážeme, že jsou tyto rozklady jednoznačné.

Pro spor předpokládejme, že nějaký prvek $a$ nemá ireducibilní rozklad, $0 \neq a \nparallel 1$. Indukcí zkonstruujeme posloupnost, která protiřečí bodu (2).

(i) Položme $a_1 = a$. Tedy $a_1 \nparallel 1$ a nemá ireducibilní rozklad.
(ii) Předpokládejme, že $a_i \nparallel 1$ a nemá ireducibilní rozklad. Speciálně, prvek $a_i$ není sám ireducibilní, a tedy $a_i = b \cdot c$ pro nějaká $b, c \nparallel 1$. Kdyby $b$ i $c$ měly ireducibilní rozklad, pak by ho měl i $a_i$, takže aspoň jedno z nich, nechť je to třeba $b$, ireducibilní rozklad nemá. Položme $a_{i+1} = b$. Tedy $a_{i+1}$ je vlastní dělitel $a_i$ a nemá ireducibilní rozklad.

Tato posloupnost $a_1, a_2, \dots$ protiřečí předpokladu (2), tedy každý prvek musí mít ireducibilní rozklad.

Na závěr dokážeme jednoznačnost rozkladu. Pro spor předpokládejme, že některé prvky nemají jednoznačný rozklad na ireducibilní činitele; mezi nimi zvolme takové $a$, jehož rozklad je nejkratší. Označme tento nejkratší rozklad $a_1 \cdot \ldots \cdot a_n$ a uvažujme nějaký jiný rozklad $b_1 \cdot \ldots \cdot b_m$ téhož prvku. Protože je $a_1$ ireducibilní, podle Lemmatu 5.6 musí $a_1$ dělit některé $b_i$. Protože jsou všechna $b_j$ ireducibilní a $a_1 \nparallel 1$, máme $a_1 \parallel b_i$. Pak ale $a' = a_2 \cdot \ldots \cdot a_n \parallel \cdot b_1 \cdot \ldots b_{i-1} \cdot b_{i+1} \cdot \ldots \cdot b_m$ je prvek s kratším nejednoznačným rozkladem, spor. □

Srovnejte důkaz ($\Leftarrow$) s důkazem Základní věty aritmetiky!

Na Větu 5.4 lze pohlížet jako na charakterizaci Gaussovskosti pomocí termínů uspořádání: obor $\mathbf{R}$ je Gaussovský právě tehdy, když je uspořádaná množina $(\bar{R}, |)$ svaz a zároveň v ní neexistuje nekonečný ostře klesající řetězec.

## 6. Eukleidovské obory

**Cíl.** *Budeme se zabývat obory, ve kterých, zjednodušeně řečeno, lze dělit se zbytkem. Dělitelnost se pak chová hezky: NSD je možné počítat pomocí Eukleidova algoritmu, platí Bézoutova rovnost, a tudíž jde o Gaussovské obory. Druhá část sekce popisuje metodu, jak dokázat, že daný obor není Eukleidovský. Definujeme tzv. ideály a podíváme se na obory, v nichž je každý ideál hlavní.*

## 6.1. **Eukleidův algoritmus.**

**Definice.** *Eukleidovskou normou* na oboru $\mathbf{R}$ rozumíme zobrazení

$$\nu : R \to \mathbb{N} \cup \{0\}$$

splňující

(0) $\nu(0) = 0$;
(1) pokud $a \mid b \neq 0$, pak $\nu(a) \leq \nu(b)$;
(2) pro všechna $a, b \in R$, $b \neq 0$, existují $q, r \in R$ taková, že

$$a = bq + r \quad \text{a} \quad \nu(r) < \nu(b).$$

Obor $\mathbf{R}$ se nazývá *Eukleidovský*, pokud na něm existuje Eukleidovská norma.

Eukleidovská norma nám umožňuje „měřit“ prvky daného oboru s ohledem na jejich dělitelnost. Podmínka (2) říká, že pro každou dvojici $a, b \neq 0$ existuje „podíl“ $q$ a „zbytek“ $r$ (bez nároku na jejich jednoznačnost!), přičemž zbytek je menší než prvek, kterým dělíme.

**Příklad.** Řada Gaussovských oborů je také Eukleidovská:

- Tělesa jsou Eukleidovské obory. Eukleidovskou normou je např. $\nu(0) = 0$ a $\nu(a) = 1$ pro všechna $a \neq 0$.
- Obor $\mathbb{Z}$ je Eukleidovský. Normou je absolutní hodnota, tj. $\nu(a) = |a|$.
- Obor $\mathbb{Z}[i]$ (Gaussovská celá čísla) je Eukleidovský. Normou je $\nu(z) = |z|^2$, jak bude dokázáno později (Tvrzení 7.2).
  Obecněji, některé obory $\mathbb{Z}[\sqrt{s}]$ jsou Eukleidovské, např. pro $s = -1, \pm 2, 3$, některé ne, např. pro $s = -3, 5$. V uvedených případech je normou
  $$\nu(a + b\sqrt{s}) = |a^2 - sb^2|.$$
- Obor $\mathbb{Z}[\omega]$ (Eisensteinova celá čísla), kde $\omega = e^{2\pi i/3}$ je komplexní třetí odmocnina z jedné, je Eukleidovský. Normou je $\nu(z) = |z|^2$.
- Obor $\mathbf{T}[x]$ je Eukleidovský pro libovolné těleso $\mathbf{T}$. Normou je
  $$\nu(f) = 1 + \deg f.$$
  (Proč ne pouze $\deg f$? Protože 0 musí být jediný prvek s normou 0).

**Příklad.** Ne každý Gaussovský obor je Eukleidovský: např. obor $\mathbb{Z}[x]$ nebo obory polynomů více proměnných.

Všimněte si, že zobrazení $f \mapsto 1 + \deg f$ není Eukleidovskou normou pro obor $\mathbb{Z}[x]$: např. pro polynomy $3x$ a $2x$ neexistují $q, r \in \mathbb{Z}[x]$ splňující $3x = q \cdot 2x + r$ a $\deg r = 0$ — jediným řešením by bylo $q = \frac{3}{2} \notin \mathbb{Z}[x]$. Pozor, toto není důkaz faktu, že obor $\mathbb{Z}[x]$ není Eukleidovský! Bylo by třeba dokázat, že *jakékoliv* zobrazení $\mathbb{Z}[x] \to \mathbb{N} \cup \{0\}$ nesplňuje podmínky Eukleidovské normy. Přímý důkaz by byl zřejmě složitý, v závěru sekce však uvidíme trik, který úlohu činí snadnou: viz Věta 6.4.

Dělitelnost se v Eukleidovských oborech chová hezky: NSD je možné počítat pomocí Eukleidova algoritmu, platí Bézoutova rovnost a pomocí Věty 5.4 dokážeme také existenci a jednoznačnost ireducibilních rozkladů.

**Eukleidův algoritmus.** Buď $\mathbf{R}$ Eukleidovský obor.

- `VSTUP:` $a, b \in R$, $\nu(a) \geq \nu(b)$.
- `VÝSTUP:` $\mathrm{NSD}(a, b)$ a $u, v \in R$ splňující $\mathrm{NSD}(a, b) = u \cdot a + v \cdot b$.

- $a_0 = a, \quad u_0 = 1, \quad v_0 = 0.$
  $a_1 = b, \quad u_1 = 0, \quad v_1 = 1.$
  $a_{i+1} = r, \quad u_{i+1} = u_{i-1} - u_i q, \quad v_{i+1} = v_{i-1} - v_i q$, kde $q, r$ zvolíme tak, aby
  $$a_{i-1} = a_i q + r \text{ a } \nu(r) < \nu(a_i).$$
  Pokud $a_{i+1} = 0$, odpověz $a_i$, $u_i$, $v_i$.

?

**Věta 6.1.** *Eukleidův algoritmus nalezene v Eukleidovském oboru* $\mathbf{R}$ *pro jakýkoliv vstup* $a, b \in R$ *hodnotu* $\mathrm{NSD}(a, b)$ *a nějaká* $u, v \in R$ *splňující*

$$\mathrm{NSD}(a, b) = u \cdot a + v \cdot b.$$

*Důkaz.* Vzhledem k tomu, že $\nu(a_0) \geq \nu(a_1) > \nu(a_2) > \nu(a_3) > \ldots \geq 0$, algoritmus se musí po konečně mnoha krocích zastavit; označme $K$ číslo kroku, ve kterém se tak stane. Je třeba dokázat, že

$$\mathrm{NSD}(a, b) = a_K = u_K \cdot a + v_K \cdot b.$$

Vzhledem k tomu, že $\mathrm{NSD}(a_K, 0) = a_K$, stačí dokázat, že NSD dvou po sobě jdoucích prvků posloupnosti $a_0, a_1, \ldots, a_K$ se nemění, tj. že

(1) pro každé $i = 1, \ldots, K$ platí $\mathrm{NSD}(a_{i-1}, a_i) = \mathrm{NSD}(a_i, a_{i+1})$;
(2) pro každé $i = 0, \ldots, K$ platí $a_i = u_i \cdot a + v_i \cdot b$.

Obě tvrzení plynou z vyjádření

$$a_{i-1} = a_i q + a_{i+1}.$$

Pro důkaz (1) si stačí uvědomit, že dvojice $a_{i-1}, a_i$ má stejné společné dělitele jako dvojice $a_i, a_{i+1}$ (jde o analogii Lemmatu 2.2). Indukcí ověříme (2). Pro $i = 0, 1$ výrok zřejmě platí. Dále, předpokládáme-li $a_{i-1} = u_{i-1}a + v_{i-1}b$ a $a_i = u_i a + v_i b$, pak

$$\begin{aligned} a_{i+1} &= a_{i-1} - a_i q = (u_{i-1}a + v_{i-1}b) - (u_i a + v_i b) \cdot q \\ &= (u_{i-1} - u_i q) \cdot a + (v_{i-1} - v_i q) \cdot b = u_{i+1}a + v_{i+1}b. \end{aligned}$$

□

**Lemma 6.2.** *Buď* $\mathbf{R}$ *Eukleidovský obor a* $a, b \in R$, $a, b \neq 0$.

(1) *Pokud* $a \parallel b$, *pak* $\nu(a) = \nu(b)$.
(2) *Pokud* $a \mid b$ *a* $b \nmid a$, *pak* $\nu(a) < \nu(b)$.

Poznamenejme, že implikace $\nu(a) = \nu(b) \Rightarrow a \parallel b$ neplatí: např. v oborech polynomů jsou jistě neasociované polynomy stejného stupně!

*Důkaz.* (1) Je-li $a \parallel b$, tedy $a \mid b$ a $b \mid a$, pak $\nu(a) \leq \nu(b) \leq \nu(a)$, tedy $\nu(a) = \nu(b)$. (2) Jistě $\nu(a) \leq \nu(b)$, pro spor tedy předpokládejme, že $\nu(a) = \nu(b)$. Napišme

- $b = au$ pro nějaké $u \in R$,
- $a = bq + r$ pro nějaká $q, r \in R$, $\nu(r) < \nu(b) = \nu(a)$.

Protože $b \nmid a$, máme $r \neq 0$. Dosazením získáme vyjádření $r = a - bq = a - auq = a(1 - uq)$. Z toho plyne, že $a \mid r$, tedy $\nu(a) \leq \nu(r)$, spor. □

**Důsledek 6.3.** *Eukleidovské obory jsou Gaussovské.*

*Důkaz.* Podle Věty 5.4 stačí dokázat, že v Eukleidovských oborech existují NSD a neexistují nekonečné posloupnosti vlastních dělitelů. První fakt jsme dokázali ve Větě 6.1 a druhý plyne bezprostředně z bodu (2) předešlého lemmatu: v takové posloupnosti by ostře klesala norma, což nejde. □

6.2. **Hlavní ideály.**

Účelem tohoto odstavce je především předvést metodu důkazu, že daný obor $\mathbf{R}$ není Eukleidovský: dokážeme, že v Eukleidovských oborech je každý ideál hlavní. Díky tomu místo důkazu, že *žádné* zobrazení nesplňuje podmínky na Eukleidovskou normu, stačí v $\mathbf{R}$ najít *nějaký* ideál, který není hlavní.

**Definice.** *Ideálem* v oboru $\mathbf{R}$ rozumíme libovolnou podmnožinu $I \subseteq R$ takovou, že $0 \in I$ a kdykoliv $a, b \in I$ a $u \in R$, pak také $-a \in I$, $a + b \in I$ a $a \cdot u \in I$.

Příkladem jsou množiny $n\mathbb{Z} = \{nz : z \in \mathbb{Z}\} = \{u \in \mathbb{Z} : n \mid u\}$ v oboru $\mathbb{Z}$. (Žádné jiné ideály v oboru $\mathbb{Z}$ nejsou, jak plyne z Věty 6.4.) Tento příklad lze zobecnit:

**Definice.** *Hlavním ideálem* v oboru $\mathbf{R}$ rozumíme podmnožinu

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

pro libovolné $a \in R$.

Je zřejmé, že jde skutečně o ideál: 0 je dělitelná čímkoliv, součet i rozdíl dvou prvků dělitelných $a$ je dělitelný $a$ a stejně tak libovolný násobek. Např. $0R = \{0\}$ a $1R = R$ jsou ideály v každém oboru.

Hlavní ideály hrají v teorii dělitelnosti důležitou roli z následujícího důvodu:

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

(Dokažte si toto snadné pozorování sami!)

**Věta 6.4.** *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. □

Hlavní ideál $aR$, který obsahuje dva nesoudělné prvky $b, c$, je roven celému $R$: protože $b, c \in aR$, tj. $a \mid b$ i $a \mid c$, musí být $a \parallel 1$, z čehož plyne $aR = R$. Toto pozorování lze snadno použít k hledání ideálů, které nejsou hlavní.

**Příklad.** Ukážeme, že obor $\mathbb{Z}[x]$ není Eukleidovský. 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. Z Věty 6.4 dostáváme, že $\mathbb{Z}[x]$ není Eukleidovský obor.

**Příklad.** Ukážeme, že obor $\mathbf{R}[x_1, \ldots, x_k]$ (kde $\mathbf{R}$ je libovolný obor a $k > 1$) není Eukleidovský. 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. Z Věty 6.4 dostáváme, že $\mathbf{R}[x_1, \ldots, x_k]$ není Eukleidovský obor.

**Definice.** Řekneme, že $\mathbf{R}$ je *obor integrity hlavních ideálů*, pokud je v $\mathbf{R}$ každý ideál hlavní.

Čili právě jsme dokázali, že Eukleidovské obory jsou obory integrity hlavních ideálů. Opačná implikace neplatí, ale vymyslet nějaký protipříklad není snadné: možná nejjednodušším příkladem je obor $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$. Důkaz tohoto faktu je však poměrně obtížný.

Obory integrity hlavních ideálů jsou velmi zajímavým předmětem studia samy o sobě, my se však jimi hlouběji zabývat nebudeme. Jedinou ukázkou za všechny nám budiž následující věta, která zařazuje tuto třídu do hierarchie oborů z hlediska dělitelnosti.

**Věta 6.5.** *Obory integrity hlavních ideálů jsou Gaussovské.*

*Důkaz.* Buď $\mathbf{R}$ obor integrity hlavních ideálů. Podle Věty 5.4 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 $b \mid a$. Přitom pokud je $d$ společným dělitelem $a, b$, pak $aR \subseteq dR$ a $bR \subseteq dR$, tedy $cR \subseteq dR$ a $d \mid c$. Čili $c = \mathrm{NSD}(a, b)$.

(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 $a_1R \neq a_2R \neq a_3R \neq \ldots$ Označme $I = \bigcup_{i=1}^{\infty} a_iR$. Tato množina také tvoří ideál (dokáže se podle vzoru Tvrzení 11.2), 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 $aR + bR$ (viz též Tvrzení 19.3), a protože tento ideál obsahuje $\mathrm{NSD}(a, b)$, dostáváme $\mathrm{NSD}(a, b) = au + bv$ pro nějaké $u, v \in R$.

## SHRNUTÍ

V předchozím textu jsme dokázali následující hierarchií oborů integrity:

$$\textit{Eukleidovský obor} \Longrightarrow \textit{OIHI} \Longrightarrow \textit{Gaussovský obor}$$

Některé vlastnosti těchto tříd jsou shrnuty v následující tabulce:

| | ired. rozklady | ex. NSD | Bézout. rovnost | Eukleidův alg. |
|---|---|---|---|---|
| Eukleidovské | Věta 6.3 | Věta 6.1 | Věta 6.1 | Věta 6.1 |
| OIHI | Věta 6.5 | Věta 6.5 | ano | NE |
| Gaussovské | definice | Věta 5.3 | NE | NE |
| obecné obory | NE | NE | NE | NE |

A na závěr pár příkladů:

| | |
|---|---|
| Eukleidovské | tělesa, $\mathbb{Z}$, $\mathbf{T}[x]$ ($\mathbf{T}$ těleso), $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i\sqrt{2}]$ |
| OIHI, ne Ekleidovské | $\mathbb{Z}[\frac{1+i\sqrt{19}}{2}]$ |
| Gaussovské, ne OIHI | $\mathbb{Z}[x]$, $\mathbf{R}[x, y, \dots]$ ($\mathbf{R}$ Gaussovský) |
| negaussovské | $\mathbb{Z}[\sqrt{5}]$, $\mathbb{Z}[i\sqrt{3}]$ |

Rozšířením celých čísel a oborům polynomů se budeme věnovat podrobněji v následujících dvou sekcích.

## 7. * Rozšíření celých čísel

**Cíl.** *Teorii předchozích dvou sekcí aplikujeme na obory $\mathbb{Z}[\sqrt{s}]$. Zvláštní pozornost bude věnována Gaussovským celým číslům.*

Mezi nejdůležitější rozšíření oboru celých čísel patří tzv. *kvadratická rozšíření*, tj. obory typu $\mathbb{Z}[\sqrt{s}]$. Pro některá $s$ se dělitelnost chová pěkně (jsou to dokonce Eukleidovské obory), pro některá naopak velmi špatně (nejsou ani Gaussovské).

V této sekci se soustředíme výhradně na kvadratická rozšíření, pro obecnější teorii doporučujeme libovolnou knihu o algebraické teorii čísel. Základním nástrojem k řešení úloh týkajících se dělitelnosti je norma.

### 7.1. Obory $\mathbb{Z}[\sqrt{s}]$.

V tomto odstavci bude $s$ značit číslo, jež není dělitelné druhou mocninou žádného prvočísla, a $\nu$ zobrazení

$$\nu : \mathbb{Z}[\sqrt{s}] \to \mathbb{N} \cup \{0\}, \qquad a + b\sqrt{s} \mapsto |a^2 - sb^2|.$$

Je dobré mít na paměti, že pro $s < 0$ je $\nu(u) = |u|^2$ (obyčejná absolutní hodnota komplexního čísla), díky čemuž se dá často aplikovat geometrický náhled na situaci.

**Tvrzení 7.1.** *Pro každá $u, v \in \mathbb{Z}[\sqrt{s}]$ platí*

(1) $\nu(u \cdot v) = \nu(u) \cdot \nu(v)$,
(2) $\nu(u) = 1 \;\Leftrightarrow\;$ *$u$ je invertibilní.*

*Důkaz.* (1) Označme $u = a + b\sqrt{s}$ a $v = c + d\sqrt{s}$. Pak

$$\begin{aligned}\nu(u \cdot v) &= \nu((ac + sbd) + (ad + bc)\sqrt{s}) \\ &= |a^2c^2 + 2sabcd + s^2b^2d^2 - s(a^2d^2 + 2abcd + b^2c^2)| \\ &= |a^2c^2 + s^2b^2d^2 - sa^2d^2 - sb^2c^2)| \\ &= |a^2 - sb^2| \cdot |c^2 - sd^2| = \nu(u) \cdot \nu(v).\end{aligned}$$

(2) Pokud $\nu(a + b\sqrt{s}) = |a^2 - sb^2| = 1$, pak $a^2 - sb^2 = (a - b\sqrt{s})(a + b\sqrt{s}) = \pm 1$, a tedy $a + b\sqrt{s} \parallel 1$. Opačná implikace plyne z (1): je-li $u \parallel 1$, tj. existuje $v$ takové, že $uv = 1$, pak $1 = \nu(1) = \nu(uv) = \nu(u)\nu(v)$, a tedy $\nu(u) = \nu(v) = 1$. □

**Příklad.** Podmínku (2) lze s úspěchem využít pro hledání *invertibilních* prvků.

- V oboru $\mathbb{Z}[i]$ máme $\nu(a + bi) = a^2 + b^2$, tedy
$$\nu(u) = 1 \;\Leftrightarrow\; u = \pm 1, u = \pm i.$$
- V oboru $\mathbb{Z}[i\sqrt{2}]$ máme $\nu(a + bi) = a^2 + 2b^2$, tedy
$$\nu(u) = 1 \;\Leftrightarrow\; u = \pm 1.$$

- V oboru $\mathbb{Z}[\sqrt{2}]$ máme $\nu(a+bi) = |a^2 - 2b^2|$. Řešením rovnice $\nu(u) = 1$ je např. $\pm 1$, ale také $\pm 1 \pm \sqrt{2}$, $\pm 3 \pm 2\sqrt{2}$, atd. Je vidět, že existuje nekonečně mnoho invertibilních prvků, např. $(1+\sqrt{2})^n$ pro libovolné $n$.

Podmínka (1) říká, že pokud $u \mid v$, pak $\nu(u) \mid \nu(v)$. Navíc, pokud je $u$ vlastní dělitel, pak $1 \neq \nu(u) \neq \nu(v)$. Tyto vlastnosti lze s úspěchem využít pro hledání *ireducibilních rozkladů*. Jednak, je-li $\nu(u)$ prvočíslo, pak je $u$ zaručeně ireducibilní. Opačná implikace neplatí, např. v $\mathbb{Z}[i]$ je prvek 3 ireducibilní, ačkoliv má normu 9. Uvedená vlastnost však pomáhá k nalezní dělitele či k důkazu ireducibility: např. pro zmíněný prvek 3 v $\mathbb{Z}[i]$, pokud by existoval netriviální rozklad, pak jedině na dva prvky normy 3; prvky normy 3 ale v $\mathbb{Z}[i]$ nejsou.

**Příklad.** Dokončíme důkaz započatý v Sekci 5, že $\mathbb{Z}[\sqrt{5}]$ není Gaussovský obor. Zbývá dokázat, že prvky 2 a $\pm 1 + \sqrt{5}$ jsou ireducibilní v oboru $\mathbb{Z}[\sqrt{5}]$. Protože je jejich norma rovna 4, netriviální rozklad by nutně byl na součin dvou prvků normy 2. V oboru $\mathbb{Z}[\sqrt{5}]$ ovšem žádné prvky s normou 2 nejsou: je-li $u = a + b\sqrt{5}$ a $a, b$ mají opačnou paritu, pak je $\nu(u)$ liché, a mají-li stejnou paritu, pak je $\nu(u)$ dělitelné 4.

7.2. **Gaussovská celá čísla.**
Pro některé obory $\mathbb{Z}[\sqrt{s}]$ je uvedené zobrazení $\nu$ Eukleidovskou normou. Ukážeme tento fakt pro Gaussovská celá čísla.

**Tvrzení 7.2.** *Zobrazení $\nu$ je Eukleidovská norma na oboru $\mathbb{Z}[i]$.*

*Důkaz.* Je třeba ověřit podmínky z definice Eukleidovské normy. Podmínka (0) je zřejmá a (1) plyne z Tvrzení 7.1. Pro důkaz (2) uvažujme $a, b \in \mathbb{Z}[i]$, $b \neq 0$, a položme

$$z = \frac{a}{b} \in \mathbb{C}$$

(přesný podíl v $\mathbb{C}$). Buď $q$ nejbližší prvek $\mathbb{Z}[i]$ k prvku $z$ (tj. takový, pro který je $|z-q|$ minimální); je-li takových více, zvolme libovolný z nich. Položme

$$r = a - bq.$$

Pak zřejmě $bq + r = a$ a zbývá dokázat, že $\nu(r) < \nu(b)$. Jaká je vzdálenost $q$ a $z$? V nejhorším případě je $z$ uprostřed čtverce s celočíselnými vrcholy, tedy určitě $|z-q| \leq \frac{\sqrt{2}}{2} < 1$. Proto

$$\nu(r) = |r|^2 = |a - bq|^2 = |b|^2 \cdot |\frac{a}{b} - q|^2 = |b|^2 \cdot |z-q|^2 < |b|^2 = \nu(b).$$

□

Pro obory $\mathbb{Z}[i\sqrt{2}]$ či $\mathbb{Z}[e^{2\pi i/3}]$ lze důkaz provést zcela analogicky, protože i zde platí $\nu(u) = |u|^2$ a jediný rozdíl tak je v odhadu $|z-q|$. Pro $\mathbb{Z}[i\sqrt{3}]$ už důkaz neprojde, protože střed obdélníka má vzdálenost od vrcholu rovnou 1. Ve skutečnosti tento obor není ani Gaussovský (dokažte!).

Pro obory $\mathbb{Z}[\sqrt{s}]$ pro $s$ kladné schází geometrická představa. Pro $s = 2, 3$ však funguje podobný algoritmus dělení: stačí zaokrouhlit koeficienty přesného podílu. Důkaz odhadu normy zbytku je však o něco komplikovanější.

Studium různých rozšíření oboru celých čísel není nijak samoúčelné, matematici se k těmto oborům dostali při řešení řady jiných úloh. K rozvoji teorie nezanedbatelně přispěly např. pokusy dokázat tímto způsobem Velkou Fermatovu větu (tj.

dokázat, že neexistují nenulová celá čísla $x, y, z$ splňující $x^n + y^n = z^n$ pro nějaké $n \geq 3$). Už Leonhard Euler použil v roce 1753 počítání v oboru $\mathbb{Z}[i\sqrt{3}]$ k řešení Velké Fermatovy věty pro exponent 3 a asi největšího úspěchu touto metodou dosáhl Kummer v polovině 19. století, když se mu povedlo vyřešit všechny exponenty menší než 100 kromě $37, 59, 67, 74$. (K důkazu Velké Fermatovy věty nakonec vedla úplně jiná metoda, ale to už je jiná historka.)

Pro ilustraci ukážeme řešení jedné speciální diofantické rovnice. Metoda využívá řadu teoretických vlastností oboru $\mathbb{Z}[i]$, např. existenci NSD a jednoznačnost rozkladů na ireducibilní prvky.

**Úloha.** Řešte v oboru celých čísel rovnici

$$x^2 + 1 = y^3.$$

*Řešení.* Nejprve rozložíme $x^2+1 = (x+i)(x-i)$ a dokážeme, že jsou čísla $x+i, x-i$ nesoudělná. Platí $\mathrm{NSD}(x+i, x-i) = \mathrm{NSD}(x+i, 2i) = \mathrm{NSD}(x-i, 2i)$, a protože $2i = (1+i)^2$, musí být výsledek jedno z čísel $1, 1+i, (1+i)^2$. Pokud je $x$ sudé, pak je $\nu(x+i)$ liché, a tedy $\mathrm{NSD}(x+i, x-i) = 1$. Pokud je $x$ liché, pak je $\nu(x+i) = \nu(x-i) \equiv 2 \pmod 4$ (dosaďte $x = 2k+1$), a tedy $(1+i)^2$ nedělí $x+i$ ani $x-i$ (tj. v ireducibilním rozkladu těchto čísel je $1+i$ nejvýše jednou). Protože je součin $(x+i)(x-i)$ třetí mocninou, počet čísel $1+i$ v jeho ireducibilním rozkladu musí být dělitelný třemi; čili jediná možnost je, že tam není žádné. Tedy $\mathrm{NSD}(x+i, x-i) = 1$.

Dokázali jsme, že $x+i$ a $x-i$ jsou nesoudělné v $\mathbb{Z}[i]$. Protože jejich součin je třetí mocninou čísla $y$, každé z nich musí být třetí mocninou nějakého prvku $\mathbb{Z}[i]$. Uvažujme takové $a+bi$: z rovnosti $(a+bi)^3 = (a^3 - ab^2) + (a^2b - b^3)i = x+i$ plyne $b(a^2 - b^2) = 1$, což má jediné celočíselné řešení: $b = -1$, $a = 0$. To dává jediné celočíselné řešení původní rovnice $x = 0$, $y = 1$. □

## 8. Obory polynomů a podílová tělesa

> **Cíl.** *Budeme se zabývat otázkou, jak funguje dělitelnost v oborech polynomů. Zavedeme podílová tělesa jako formalizaci pojmu zlomek a ukážeme, jak spolu souvisí dělitelnost v oboru polynomů nad daným oborem a nad jeho podílovým tělesem.*

Obory polynomů jedné proměnné nad *tělesem* $\mathbf{T}$ se z hlediska dělitelnosti chovají tak pěkně, jak to jen jde. Známý algoritmus dělení dává (jednoznačně určený) podíl a zbytek. Obory $\mathbf{T}[x]$ jsou tedy Eukleidovské, platí v nich Bézoutova rovnost a každý polynom má právě jeden rozklad na ireducibilní polynomy.

Pro polynomy nad obecným oborem integrity podíl a zbytek existovat nemusí: viz příklad s dělením $3x : 2x$ v Sekci 6. Při provádění algoritmu dělení totiž mohou vycházet *zlomky*. Pojem zlomku máme zažitý ve formě racionálních čísel. Jak jej však formalizovat pro obecné obory integrity? Odpovědí je *podílové těleso*.

Po zavedení podílových těles ukážeme, jak řešit úlohy týkající se dělitelnosti pro polynomy nad obecnými obory. Stručně řečeno, všechny operace budeme provádět se zlomky (nad podílovým tělesem) a na závěr výsledek interpretujeme v původním oboru — viz Věty 8.5 a 8.8. Důsledkem uvedených pozorování bude Gaussova věta 8.9, která říká, že obor polynomů nad Gaussovským oborem je Gaussovský.

8.1. **Konstrukce podílového tělesa.**

Tak jako lze obor celých čísel rozšířit do tělesa racionálních čísel, každý obor integrity $\mathbf{R}$ lze rozšířit na tzv. *podílové těleso*, které lze zkonstruovat jako „těleso zlomků“, jejichž čitatel i jmenovatel jsou prvky daného oboru. Konstrukce probíhá následujícím způsobem.

Definujeme relaci $\sim$ na množině $R \times (R \setminus \{0\})$ předpisem

$$(a,b) \sim (c,d) \quad \iff \quad ad = bc.$$

Není těžké nahlédnout, že jde o ekvivalenci: reflexivita je zřejmá, symetrie plyne z komutativity násobení a tranzitivitu získáme následujícím výpočtem: je-li $(a,b) \sim (c,d) \sim (e,f)$, tedy $ad = bc$ a $cf = de$, rozlišíme dva případy:

- pokud $c = 0$, pak $a = e = 0$ (protože $b, d \neq 0$), a tedy $af = be = 0$;
- pokud $c \neq 0$, pak vynásobíme obě rovnosti, dostaneme $adcf = bcde$ a vykrátíme prvkem $cd \neq 0$.

V obou případech $af = be$, tj. $(a,b) \sim (e,f)$ (ke krácení potřebujeme předpoklad, že $\mathbf{R}$ je obor integrity!).

Pro jednoduchost vyjadřování budeme značit blok $[(a,b)]_\sim$ této ekvivalence jako zlomek $\frac{a}{b}$. Uvažujme množinu $Q$ všech bloků této ekvivalence (tj. všech zlomků) a definujme na ní operace

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad -\frac{a}{b} = \frac{-a}{b}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \qquad 0 = \frac{0}{1}, \qquad 1 = \frac{1}{1}.$$

(Aby jmenovatel zůstal nenulový, potřebujeme předpoklad, že $\mathbf{R}$ je obor integrity!)

**Tvrzení 8.1.** *Množina $Q$ s právě definovanými operacemi tvoří těleso, tzv.* podílové těleso *oboru* $\mathbf{R}$.

*Důkaz.* Ověříme postupně všechny axiomy:

- Asociativita sčítání: $\frac{a}{b}+(\frac{c}{d}+\frac{e}{f}) = \frac{a}{b}+\frac{cf+de}{df} = \frac{adf+b(cf+de)}{bdf} = \frac{adf+bcf+bde}{bdf} = \frac{ad+bc}{bd} + \frac{e}{f} = (\frac{a}{b} + \frac{c}{d}) + \frac{e}{f}$.
- Komutativita sčítání: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{cb+da}{db} = \frac{c}{d} + \frac{a}{b}$.
- Nula: $\frac{a}{b} + \frac{0}{1} = \frac{a\cdot 1+b\cdot 0}{b\cdot 1} = \frac{a}{b}$.
- Odčítání: $\frac{a}{b} + \frac{-a}{b} = \frac{ab+(-ab)}{b^2} = \frac{0}{b^2} = 0$.
- Asociativita a komutativita násobení plyne okamžitě z týchž vlastností oboru $\mathbf{R}$.
- Jednotka: $\frac{a}{a} \cdot \frac{1}{1} = \frac{a\cdot 1}{a\cdot 1} = \frac{a}{a}$.
- Distributivita: $\frac{a}{b} \cdot (\frac{c}{d} + \frac{e}{f}) = \frac{acf+ade}{bdf} = \frac{abcf+abde}{b^2df} = \frac{ac}{bd} + \frac{ae}{bf}$.

Navíc $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1}$ pro každé $\frac{a}{b} \neq 0$, čili $\mathbf{Q}$ je těleso. □

**Příklad.**

- Podílové těleso oboru $\mathbb{Z}$ je těleso $\mathbb{Q}$.
- Podílové těleso oboru $\mathbb{Z}[i]$ je těleso $\mathbb{Q}(i)$ sestávající ze všech čísel $a + bi$, $a, b \in \mathbb{Q}$.
- Podílové těleso oboru $\mathbf{R}[x]$ je těleso racionálních funkcí nad $\mathbf{R}$.

8.2. **Gaussovo lemma.**

Buď $\mathbf{R}$ nějaký obor integrity a $\mathbf{Q}$ jeho podílové těleso. Dělitelnost v oborech $\mathbf{R}[x]$ a $\mathbf{Q}[x]$ spolu těsně souvisí: pro *primitivní* polynomy $f, g \in R[x]$ dokážeme, že

(1) $f \mid g$ v $\mathbf{R}[x] \iff f \mid g$ v $\mathbf{Q}[x]$;

(2) $f$ je ireducibilní v $\mathbf{R}[x] \iff f$ je ireducibilní v $\mathbf{Q}[x]$;
(3) $\mathrm{NSD}_{\mathbf{R}[x]}(f,g) = \mathrm{NSD}_{\mathbf{Q}[x]}(f,g)$.

Díky tomu můžeme při práci s primitivními polynomy používat zlomky a přesto dostaneme správný výsledek.

**Definice.** Buď $f = \sum_{i=0}^{n} a_i x^i$ polynom.

- *Obsahem* polynomu $f$ rozumíme $\mathrm{ct}(f) = \mathrm{NSD}(a_0, \ldots, a_n)$.
- *Primitivní částí* polynomu $f$ rozumíme $\mathrm{pp}(f) = \sum_{i=0}^{n} \frac{a_i}{\mathrm{ct}(f)} x^i$.
- Polynom $f$ nazýváme *primitivní*, jestliže $\mathrm{ct}(f) = 1$.

Např. polynom $f = 3x^2 + 6x - 3$ má v oboru $\mathbb{Z}[x]$ obsah $\mathrm{ct}(f) = 3$ a primitivní část $\mathrm{pp}(f) = x^2 + 2x - 1$. V oborech polynomů nad tělesem je zřejmě každý polynom primitivní.

Je zřejmé, že pokud $f \mid g$ a $g$ je primitivní, pak i $f$ je primitivní. Klíčovým pozorováním je fakt, že platí i opačné tvrzení.

**Věta 8.2** (Gaussovo lemma)**.** *Buď $\mathbf{R}$ Gaussovský obor a $f, g \in R[x]$ primitivní polynomy. Pak $f \cdot g$ je primitivní polynom.*

*Důkaz.* Označme $f = \sum_{i=0}^{n} a_i x^i$ a $g = \sum_{i=0}^{m} b_i x^i$ a předpokládejme, že $f \cdot g$ není primitivní polynom, tedy že $\mathrm{ct}(f) \neq 1$. Protože je $\mathbf{R}$ Gaussovský obor, existuje ireducibilní prvek $u \in R$, který dělí $\mathrm{ct}(f \cdot g)$, tj. který dělí všechny koeficienty součinu $f \cdot g$. Zvolme nejmenší $j$ takové, že $u \nmid a_j$ a nejmenší $k$ takové, že $u \nmid b_k$ (protože jsou polynomy $f, g$ primitivní, $u$ nemůže dělit všechny jejich koeficienty). Podívejme se na $(j+k)$-tý koeficient polynomu $f \cdot g$:

$$c_{j+k} = a_0 b_{j+k} + \ldots + a_{j-1} b_{k+1} + a_j b_k + a_{j+1} b_{k-1} + \ldots + a_{j+k} b_0.$$

Protože $u \mid a_i$ pro všechna $i < j$, máme

$$u \mid a_0 b_{j+k} + \ldots + a_{j-1} b_{k+1}.$$

Protože $u \mid b_i$ pro všechna $i < k$, máme

$$u \mid a_{j+1} b_{k-1} + \ldots + a_{j+k} b_0.$$

Tedy $u$ dělí všechny členy kromě $a_j b_k$. Ten naopak $u$ dělitelný není, protože $u$ je ireducibilní a nedělí ani $a_j$, ani $b_k$. Dostáváme, že $u \nmid c_{j+k}$, spor. □

Tedy polynom $f \cdot g$ je primitivní právě tehdy, když jsou oba polynomy $f, g$ primitivní. Gaussovo lemma umožňuje dát do souvislosti dělitelnost v oborech $\mathbf{R}[x]$ a $\mathbf{Q}[x]$.

**Tvrzení 8.3.** *Buď $\mathbf{R}$ Gaussovský obor, $\mathbf{Q}$ jeho podílové těleso a $f, g$ primitivní polynomy z $\mathbf{R}[x]$. Pak $f \mid g$ v $\mathbf{Q}[x]$ právě tehdy, když $f \mid g$ v $\mathbf{R}[x]$.*

*Důkaz.* Předpokládejme, že $f \mid g$ v $\mathbf{Q}[x]$, tj. že existuje $h \in Q[x]$ splňující $g = fh$. Zvolme $k \in Q$ tak, aby $kh$ byl primitivní polynom z $\mathbf{R}[x]$. Pak $kg = f \cdot kh$, na pravé straně je součin primitivních polynomů, takže podle Gaussova lemmatu je $kg$ také primitivní polynom. Ovšem i $g$ je primitivní, takže $k$ musí být invertibilní prvek z $\mathbf{R}$ a dostáváme, že $kh \parallel h \in R[x]$.

Zpětná implikace je triviální. □

První aplikace je vztah ireducibility v $\mathbf{R}[x]$ a v $\mathbf{Q}[x]$.

**Lemma 8.4.** *Buď $\mathbf{R}$ Gaussovský obor, $\mathbf{Q}$ jeho podílové těleso a $f$ primitivní polynom z $\mathbf{R}[x]$. Pak je $f$ ireducibilní v $\mathbf{R}[x]$ právě tehdy, když je ireducibilní v $\mathbf{Q}[x]$.*

*Důkaz.* Dokážeme následující ekvivalentní tvrzení: $f$ má vlastního dělitele v $\mathbf{R}[x]$ právě tehdy, když má vlastního dělitele v $\mathbf{Q}[x]$.

($\Rightarrow$) Protože je $f$ primitivní, jakýkoliv vlastní dělitel má stupeň aspoň 1. Tedy jde zároveň o vlastního dělitele v $\mathbf{Q}[x]$.

($\Leftarrow$) Nechť $g$ je vlastní dělitel $f$ v $\mathbf{Q}[x]$. Pak existuje $k \in Q$ takové, že $kg$ je primitivní polynom z $\mathbf{R}[x]$. Přitom $kg \mid f$ v $\mathbf{Q}[x]$, tedy podle Tvrzení 8.3 je $kg$ vlastní dělitel $f$ v $\mathbf{R}[x]$. □

**Věta 8.5.** *Buď $\mathbf{R}$ Gaussovský obor, $\mathbf{Q}$ jeho podílové těleso a $f$ polynom z $\mathbf{R}[x]$. Pak je $f$ ireducibilní v $\mathbf{R}[x]$ právě tehdy, když*

- $\deg f = 0$ *a $f$ je ireducibilní v $\mathbf{R}$; nebo*
- $\deg f > 0$, *$f$ je primitivní a ireducibilní v $\mathbf{Q}[x]$.*

*Důkaz.* Vzhledem k tomu, že se každý polynom rozkládá na obsah a primitivní část, musí být v případě ireducibility jedna z těchto částí triviální a druhá ireducibilní. □

**Příklad.**

- Polynom $2x - 2$ je ireducibilní v $\mathbb{Q}[x]$, ale není ireducibilní v $\mathbb{Z}[x]$, protože není primitivní.
- Polynom 2 není ireducibilní v $\mathbb{Q}[x]$, protože je invertibilní, ale je ireducibilní v $\mathbb{Z}[x]$.

Druhá aplikace je existence NSD v $\mathbf{R}[x]$.

**Lemma 8.6.** *Buď $\mathbf{R}$ obor integrity a $f, g$ polynomy z $\mathbf{R}[x]$. Pak*

$$\mathrm{NSD}_{\mathbf{R}[x]}(f, g) = \mathrm{NSD}_{\mathbf{R}}(\mathrm{ct}(f), \mathrm{ct}(g)) \cdot \mathrm{NSD}_{\mathbf{R}[x]}(\mathrm{pp}(f), \mathrm{pp}(g))$$

*za předpokladu, že oba NSD na pravé straně rovnosti existují.*

*Důkaz.* Předpokládejme, že pravá strana existuje, označme tento prvek $r$; dokážeme, že $r = \mathrm{NSD}(f, g)$. Protože $\mathrm{NSD}_{\mathbf{R}}(\mathrm{ct}(f), \mathrm{ct}(g))$ dělí $\mathrm{ct}(f)$ i $\mathrm{ct}(g)$, a zároveň $\mathrm{NSD}_{\mathbf{R}[x]}(\mathrm{pp}(f), \mathrm{pp}(g))$ dělí $\mathrm{pp}(f)$ i $\mathrm{pp}(g)$, tak jejich součin $r$ dělí oba polynomy $f, g$, čili $r$ je společný dělitel. Dokážeme, že je to největší společný dělitel: pokud nějaký $h$ dělí $f$ i $g$, pak $\mathrm{ct}(h)$ dělí $\mathrm{ct}(f)$ i $\mathrm{ct}(g)$, tedy $\mathrm{ct}(h) \mid \mathrm{NSD}_{\mathbf{R}}(\mathrm{ct}(f), \mathrm{ct}(g))$; analogicky $\mathrm{pp}(h) \mid \mathrm{NSD}_{\mathbf{R}[x]}(\mathrm{pp}(f), \mathrm{pp}(g))$ a dostáváme $h \mid r$. □

**Lemma 8.7.** *Buď $\mathbf{R}$ obor integrity, $\mathbf{Q}$ jeho podílové těleso a $f, g$ primitivní polynomy z $\mathbf{R}[x]$. Pak $\mathrm{NSD}_{\mathbf{R}[x]}(f, g)$ existuje a je roven primitivnímu polynomu $h$ splňujícímu $h = \mathrm{NSD}_{\mathbf{Q}[x]}(f, g)$.*

*Důkaz.* Takový polynom $h$ jistě můžeme z dané třídy asociovanosti vybrat (připomeňme, že NSD je určen až na asociovanost). Přitom $h$ dělí $f$,$g$ v $\mathbf{Q}[x]$, tedy podle Tvrzení 8.3 i v $\mathbf{R}[x]$ a kdykoliv máme jiný společný dělitel $d \mid f, g$ v $\mathbf{R}[x]$, pak jistě $d \mid h$ v $\mathbf{Q}[x]$, a tedy podle Tvrzení 8.3 i v $\mathbf{R}[x]$. □

Z předchozích dvou lemmat ihned plyne následující vztah:

**Věta 8.8.** *Buď $\mathbf{R}$ Gaussovský obor, $\mathbf{Q}$ jeho podílové těleso a $f, g$ polynomy z $\mathbf{R}[x]$. Pak $\mathrm{NSD}_{\mathbf{R}[x]}(f, g)$ existuje a platí*

$$\mathrm{NSD}_{\mathbf{R}[x]}(f, g) = \mathrm{NSD}_{\mathbf{R}}(\mathrm{ct}(f), \mathrm{ct}(g)) \cdot \mathrm{NSD}_{\mathbf{Q}[x]}(\mathrm{pp}(f), \mathrm{pp}(g))$$

**Příklad.**

$\mathrm{NSD}_{\mathbb{Z}[x]}(4x^2+8x+4, -6x^2+6) = \mathrm{NSD}_{\mathbb{Z}}(4,-6)\cdot\mathrm{NSD}_{\mathbb{Q}[x]}(x^2+2x+1, x^2-1) = 2(x+1).$

**Věta 8.9** (Gaussova)**.** *Buď* $\mathbf{R}$ *Gaussovský obor a* $X$ *libovolná neprázdná množina. Pak* $\mathbf{R}[X]$ *je také Gaussovský obor.*

*Důkaz.* (A) Gaussovu větu nejprve dokážeme pro polynomy jedné proměnné, tj. případ $X = \{x\}$. Použijeme Větu 5.4: NSD v $\mathbf{R}[x]$ existují podle Věty 8.8. A je-li $f_1, f_2, f_3, \ldots$ posloupnost vlastních dělitelů, pak $\deg f_1 \geq \deg f_2 \geq \deg f_3 \geq \cdots \geq 0$, a tedy existuje $n$ takové, že $\deg f_n = \deg f_{n+1} = \ldots$ Označíme-li $a_i$ vedoucí koeficient polynomu $f_i$, pak $a_n, a_{n+1}, \ldots$ je posloupnost vlastních dělitelů v $\mathbf{R}$, spor.

(B) Pokud je množina $X$ konečná, můžeme postupovat indukcí podle $|X|$ s využitím části (A), neboť $\mathbf{R}[x_1, \ldots, x_n] \simeq (\mathbf{R}[x_1, \ldots, x_{n-1}])[x_n]$. Pokud je $X$ nekonečná, využijeme pozorování, že pokud $Y \subseteq X$ a $0 \neq g \in R[Y]$, pak $f \mid g$ implikuje $f \in R[Y]$. Čili jsou-li dány $f, g \in R[X]$, ve skutečnosti $f, g$ obsahují jen konečné množství proměnných, tedy existuje $Y \subset X$ konečná taková, že $f, g \in R[Y]$ a $\mathrm{NSD}_{\mathbf{R}[X]}(f,g) = \mathrm{NSD}_{\mathbf{R}[Y]}(f,g)$. Podobně, každá posloupnost dělitelů obsahuje pouze konečně mnoho proměnných, neboť její první člen má tuto vlastnost; situace se tedy opět převádí na problém oboru konečně mnoha proměnných. □

8.3. *** Eisensteinovo kritérium.**

Pro zjištení ireducibility daného celočíselného polynomu se v jistých případech může hodit následující kritérium.

**Tvrzení 8.10** (Eisensteinovo kritérium)**.** *Buď* $\mathbf{R}$ *Gaussovský obor a* $f = \sum_{i=0}^{n} a_i x^i$ *primitivní polynom z* $\mathbf{R}[x]$*. Pokud existuje ireducibilní prvek* $p \in R$ *splňující* $p \mid a_0$*,* $p \mid a_1$*,* $\ldots$*,* $p \mid a_{n-1}$ *a* $p^2 \nmid a_0$*, pak je polynom* $f$ *ireducibilní v* $\mathbf{R}[x]$*.*

*Důkaz.* Uvažujme rozklad $f = gh$, kde $g = \sum_{i=0}^{k} b_i x^i$ a $h = \sum_{i=0}^{l} c_i x^i$ jsou polynomy z $\mathbf{R}[x]$ stupně alespoň 1. Protože $p \mid a_0 = b_0 c_0$, platí $p \mid b_0$ nebo $p \mid c_0$, ale určitě ne oboje zároveň, protože $p^2 \nmid a_0$. Nechť je to bez újmy na obecnosti $b_0$. Protože $p \mid a_1 = b_0 c_1 + b_1 c_0$ a $p \nmid c_0$, musí $p \mid b_1$. Protože $p \mid a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$ a $p \nmid c_0$, musí $p \mid b_2$. Tímto způsobem zjistíme, že $p$ dělí všechny koeficienty $b_i$, tedy $p \mid f$, což je spor s primitivitou. □

Příkladem použití Eisensteinova kritéria je ireducibilita polynomu $x^n \pm a$ v $\mathbb{Z}[x]$ (kde $a$ není dělitelné čtvercem prvočísla), jehož kořeny jsou právě $n$-té komplexní odmocniny z $\pm a$. (Zkuste si to dokázat přímo už jen pro $a = 2$!)

## 9. Kořeny polynomů

**Cíl.** *Budeme se zabývat v různých souvislostech dvěma otázkami: kolik mají polynomy kořenů a jak je nalézt. Dokážeme, že polynom stupně* $n$ *má nejvýše* $n$ *kořenů. Podíváme se na otázku, která čísla lze vyjádřit jako kořen celočíselného polynomu, a uvedeme kritérium existence racionálního kořene celočíselného polynomu. Ukážeme Cardanovy vzorce pro výpočet kořenů polynomů stupně* $\leq 4$ *a stručně nastíníme Newtonovu metodu na výpočet kořene obecné funkce. Na závěr zmíníme větu o interpolaci.*

**Definice.** Prvek $a \in R$ se nazývá *kořen* polynomu $f \in R[x]$, pokud $f(a) = 0$.

Kořeny polynomů hrály důležitou roli v počátcích moderní matematiky. Otázka *jak kořeny spočítat* vedla k rozvoji algebry už ve středověku (Cardanovy vzorce) a dala vzniknout komplexním číslům, která se objevovala jako řešení. V 19. století pak Abelův a především Galoisův důkaz neexistence vzorců pro výpočet kořenů polynomů stupně 5 a více významně přispěl ke vzniku teorie grup. Začneme tím, kolik kořenů lze vlastně očekávat.

## 9.1. Počet kořenů.

Připomeňme ještě jednou algoritmus dělení polynomů se zbytkem. Jak jsme uvedli, při dělení mohou vycházet zlomky. To ovšem pouze v tom případě, když je vedoucí koeficient dělence (nebo nějakého polynomu, který vznikne v průběhu výpočtu) nedělitelný vedoucím koeficientem dělitele. Z toho plyne, že pokud je tento koeficient roven 1, tj. pokud je dělitel *monický*, dělení projde v libovolném $\mathbf{R}[x]$ a výsledkem bude (jednoznačně určený) zbytek i podíl z $\mathbf{R}[x]$.

Důsledkem je následující vztah kořenů k dělitelům daného polynomu.

**Tvrzení 9.1.** *Buď $\mathbf{R}$ obor integrity, $f \in R[x]$ a $a \in R$. Pak $a$ je kořen polynomu $f$ právě tehdy, když $x - a \mid f$.*

*Důkaz.* ($\Leftarrow$) Předpokládejme, že $x - a \mid f$. Pak $f = (x - a) \cdot g$ pro nějaké $g \in R[x]$ a dosadíme-li do $f$ prvek $a$, dostaneme

$$f(a) = (a - a) \cdot g(a) = 0 \cdot g(a) = 0.$$

($\Rightarrow$) Buď $q, r$ podíl a zbytek po dělení polynomu $f$ polynomem $x - a$ (ty existují, neboť dělíme monickým polynomem). Tedy $f = (x - a) \cdot q + r$ a $r$ je konstantní polynom (zbytek musí mít menší stupeň než dělitel). Dosadíme-li prvek $a$, dostaneme

$$0 = f(a) = (a - a) \cdot q(a) + r(a) = 0 \cdot q(a) + r = r,$$

takže $r = 0$ a $x - a \mid f$. □

**Věta 9.2.** *Buď $\mathbf{R}$ obor integrity, $0 \neq f \in R[x]$ a $\deg f = n$. Pak má polynom $f$ nejvýše $n$ kořenů.*

*Důkaz.* Budeme postupovat indukcí podle stupně polynomu $f$. Je-li $\deg f = 0$, tj. $f$ je nenulový konstantní polynom, pak žádné kořeny nemá. Nyní předpokládejme, že tvrzení platí pro všechny polynomy stupně nejvýše $n$. Je-li $\deg f = n + 1$, pak jsou dvě možnosti. Buď polynom $f$ nemá žádný kořen, v tom případě tvrzení platí. Nebo má polynom $f$ nějaký kořen $a$ a v tom případě jej lze podle předchozího lemmatu napsat jako $f = (x - a) \cdot g$ pro nějaký polynom $g$ stupně $n$. Je-li $b$ nějaký jiný kořen, tj. $f(b) = (b - a) \cdot g(b) = 0$, pak, protože jde o obor integrity, musí být buď $b = a$ nebo $g(b) = 0$. Protože má polynom $g$ nejvýše $n$ kořenů, má polynom $f$ nejvýše $n + 1$ kořenů. □

**Příklad.** Počet kořenů polynomu $f$ samozřejmě může být menší než $\deg f$: např. polynom $x^2 + 1$ nemá nad $\mathbb{Z}$ žádný kořen a nad $\mathbb{Z}_2$ má jeden.

**Poznámka.** Věta 9.2 neplatí, není-li $\mathbf{R}$ oborem integrity, ale např. jen komutativním okruhem s jednotkou. Předpoklad jsme použili v poslední fázi důkazu, když z $f(b) = (b - a) \cdot g(b) = 0$ plynulo $b - a = 0$ nebo $g(b) = 0$. Uvažte např. polynom $2x \in \mathbb{Z}_4[x]$ nebo $x^2 + x \in \mathbb{Z}_6[x]$. První z nich má kořeny $0, 2$, druhý $0, 2, 3, 5$.

**Poznámka.** Věta 9.2 neplatí, není-li **R** oborem integrity, ale např. jen nekomutativním tělesem — celá teorie dělitelnosti funguje jinak. Příkladem je polynom $x^4 - 1$ nad okruhem kvaternionů, jeho kořeny jsou $\pm 1$, $\pm i$, $\pm j$, $\pm k$ (viz definice kvaternionové grupy v Sekci 13).

9.2. *** Algebraická a transcendentní čísla.**

Zvláštní význam v historii hrály kořeny celočíselných polynomů. Otázka, která čísla lze takto získat, přispěla ke vzniku teorie množin. Ukážeme si geniální Cantorovu myšlenku, která ukazuje, že skoro každé číslo je transcendentní, aniž bychom museli uvést byť jediný příklad.

**Definice.** Reálné číslo $a$ se nazývá *algebraické*, pokud existuje nenulový polynom $f \in \mathbb{Z}[x]$ takový, že $f(a) = 0$. V opačném případě se $a$ nazývá *transcendentní*.

**Příklad.**

- Racionální čísla jsou algebraická: racionální číslo $\frac{a}{b}$ je kořenem polynomu $bx - a$.
- Některá iracionální čísla jsou algebraická: např. $\sqrt{2}$ je kořenem polynomu $x^2 - 2$. I některá složitější iracionální čísla jsou algebraická: např. $\sqrt{2} + \sqrt{3}$ (zkuste najít příslušný polynom!). Obecně platí, že součet, součin apod. algebraických čísel je algebraické číslo, viz Tvrzení 26.3.
- Ač matematici dlouho tušili, že je řada čísel transcendentních, nedařilo se jim tuto vlastnost o žádném čísle dokázat. První prokazatelně transcendentní číslo předvedl v roce 1840 francouzský matematik Joseph Liouville: byl jím součet řady $\sum_{i=0}^{\infty} 10^{-i!}$, tj. číslo, které má v desetinném rozvoji jedničku právě na místech tvaru $n!$, jinak nuly. V roce 1873 dokázal Charles Hermite, že číslo $e$ je transcendentní, a až v roce 1882 našel Ferdinand von Lindemann důkaz transendence čísla $\pi$.
- O to více udivil matematiky v roce 1874 Georg Cantor, když dokázal, že *skoro všechna reálná čísla jsou transcendentní*.

Ač všechny důkazy transcendence konkrétních čísel jako $e$ nebo $\pi$ jsou poměrně komplikované, Cantorův důkaz je překvapivě jednoduchý.

*Spočetnou* množinou rozumíme takovou nekonečnou množinu, jejíž prvky lze seřadit do posloupnosti indexované přirozenými čísly (tj. jde o množinu stejně velkou jako $\mathbb{N}$). Všechny ostatní (tj. větší) nekonečné množiny nazýváme *nespočetné*.

Např. množina $\mathbb{Z}$ je spočetná: $0, 1, -1, 2, -2, 3, -3, \ldots$ Dokonce i množina $\mathbb{Q}$ je spočetná: seřaďte kladná racionální čísla do posloupnosti podle součtu čitatele a jmenovatele (ty se stejným součtem seřaďte libovolně) a vložte záporná čísla analogickým trikem.

**Tvrzení 9.3.** *Množina algebraických reálných čísel je spočetná.*

*Důkaz.* Definujme *index polynomu* $f = a_0 + a_1 x + \ldots + a_n x^n \neq 0$ jako číslo $|a_0| + |a_1| + \ldots + |a_n| + n$. Všimněte si, že existuje jen konečně mnoho polynomů daného indexu (např. index 1: $f = \pm 1$; index 2: $f = \pm 2$, $f = \pm x$; index 3: $f = \pm 3$, $f = \pm 2x$, $f = \pm x \pm 1$, $f = \pm x^2$), všechny celočíselné polynomy tedy lze seřadit do posloupnosti podle vzrůstajícího indexu. Přitom každý nenulový polynom má jen konečně mnoho kořenů, tedy nahrazením polynomu za jeho kořeny získáme posloupnost obsahující všechna algebraická čísla. □

**Tvrzení 9.4.** *Množina reálných čísel je nespočetná.*

*Důkaz.* Kdyby byla množina reálných čísel spočetná, byl by jistě spočetný i interval $\langle 0, 1)$, a tudíž bychom mohli seřadit čísla z tohoto intervalu do posloupnosti

$$a_1 = 0, a_{11}a_{12}a_{13}\dots$$
$$a_2 = 0, a_{21}a_{22}a_{23}\dots$$
$$a_3 = 0, a_{31}a_{32}a_{33}\dots$$
$$\dots$$

Nyní definujme číslo $b = 0, b_1b_2b_3\dots$ tak, že $b_1 \neq a_{11}$, $b_2 \neq a_{22}$, atd. Toto číslo nemůže být na seznamu, neboť se od $i$-tého prvku liší v $i$-té pozici rozvoje. Což je spor s tím, že tam měla být všechna čísla z intervalu $(0, 1)$. (K tomu, aby byl tento argument korektní, je třeba se vyhnout rozvojům končícím samými devítkami.) □

Tedy reálných čísel je mnohem více než algebraických. Vhledem k tomu, že spočetné množiny mají míru 0, tvrzení lze interpretovat tak, že skoro všechna reálná čísla jsou transcendentní (ve smyslu: náhodné reálné číslo je s pravděpodobností 1 transcendentní).

9.3. **Racionální kořeny.**

Následující tvrzení lze použít k najití všech racionálních kořenů daného celočíselného polynomu.

**Tvrzení 9.5.** *Buď* $\mathbf{R}$ *obor integrity a* $\mathbf{Q}$ *jeho podílové těleso. Má-li polynom* $f = \sum_{i=0}^{n} a_i x^i \in R[x]$ *kořen* $\frac{r}{s} \in Q$ *(předpokládáme* $r, s$ *nesoudělná), pak* $r \mid a_0$ *a* $s \mid a_n$.

*Důkaz.* Dosaďme prvek $\frac{r}{s}$ do $f$. Protože $\sum_{i=0}^{n} a_i(\frac{r}{s})^i = 0$, přenásobením prvkem $s^n$ dostáváme

$$a_0s^n + a_1rs^{n-1} + a_2r^2s^{n-2} + \ldots + a_{n-1}r^{n-1}s + a_nr^n = 0.$$

Protože $r$ dělí všechny členy $a_1rs^{n-1}, \ldots, a_nr^n$, musí dělit i první člen $a_0s^n$. Protože jsou $r, s$ nesoudělná, musí $r \mid a_0$. Analogicky, protože $s$ dělí všechny členy $a_0s^n, \ldots, a_{n-1}r^{n-1}s$, musí dělit i poslední člen $a_nr^n$, tedy $s \mid a_n$. □

**Příklad.** Polynom $2x^6 - 3x^4 + 2x^3 - x + 1 \in \mathbb{Z}[x]$ nemá racionální kořen. Podle Tvrzení 9.5 jsou jedinými kandidáty čísla $\pm 1$ a $\pm\frac{1}{2}$. Dosazením zjistíme, že ani jeden z nich kořenem není.

9.4. *** Cardanovy vzorce.**

V tomto odstavci odvodíme tzv. *Cardanovy vzorce* na výpočet kořenů polynomů stupně 2, 3, 4. Na závěr nastíníme, proč vzorce pro polynomy vyšších stupnů neexistují.

Výpočty budeme provádět v oboru komplexních čísel, i když většina tvrzení je platná obecně v libovolném tělese charakteristiky 0, kde existuje druhá a třetí odmocnina každého prvku.

Řešení *kvadratických* rovnic lze vysledovat až k starověkým matematikům, návod v téměř moderní podobě se nachází např. v knize matematika Al-Chorezmího z 9. století (ukázku z této knihy najdete na úvodní stránce skript). Vzorec pro řešení rovnice

$$ax^2 + bx + c = 0$$

můžeme odvodit takto: substitucí $x = y - \frac{b}{2a}$ dostaneme rovnici

$$y^2 = \frac{b^2 - 4ac}{4a^2},$$

tedy

$$y = \pm\frac{\sqrt{b^2 - 4ac}}{2a}$$

a zpětným dosazením dostaneme

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

(Zde i později neuvádíme některé mezivýpočty. Doporučujeme čtenáři, aby si všechna tvrzení ověřoval samostatně!)

Klíčovou fintou byla substituce, která nás zbavila prostředního členu; podobně budeme postupovat i při odvození vzorců vyšších stupňů. První využil tento trik k odvození vzorce pro řešení rovnic třetího stupně Nicolo Tartaglia (okolo 1530) a pro rovnice čtvrtého stupně Lodovico Ferrari (zhruba ve stejné době); jejich výsledky byly ovšem publikovány v knize Girolama Cardana, a tak se vžilo mylné označení *Cardanovy vzorce*.

Substituce obecně funguje takto: máme-li rovnici $n$-tého stupně

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

tedy ekvivalentně

$$x^n + \frac{a_{n-1}}{a_n}x^{n-1} + \ldots + \frac{a_1}{a_n}x + \frac{a_0}{a_n} = 0,$$

substituujeme $x = y - \frac{a_{n-1}}{na_n}$. Po roznásobení získáme ekvivalentní rovnici s nulovým koeficientem u $y^{n-1}$.

Nejprve předvedeme *Tartagliův postup* na řešení <u>kubické</u> rovnice

$$x^3 + bx + c = 0.$$

Všimněte si, že pro libovolné $u, v$ platí

$$(u - v)^3 + 3uv(u - v) + (v^3 - u^3) = 0.$$

Řešení původní rovnice tedy budeme hledat ve tvaru $x = u - v$, přičemž pro koeficienty dostáváme rovnosti

$$b = 3uv, \qquad c = v^3 - u^3.$$

Nyní již není těžké vyjádřit $u, v$ pomocí koeficientů $b, c$: dosazením $v = \frac{b}{3u}$ do druhé rovnice dostáváme

$$u^6 + cu^3 - \frac{b^3}{27} = 0,$$

což je kvadratická rovnice s neznámou $u^3$; označíme-li $D = c^2 + \frac{4}{27}b^3$, jeden pár řešení můžeme vyjádřit jako

$$u = \sqrt[3]{\frac{-c + \sqrt{D}}{2}}, \qquad v = \sqrt[3]{\frac{c + \sqrt{D}}{2}},$$

čímž jsme získali jeden kořen

$$x_0 = u - v$$

daného polynomu. (Bohužel, druhý pár řešení $u^3 = \frac{-c-\sqrt{D}}{2}$, $v^3 = \frac{c-\sqrt{D}}{2}$ dává stejný kořen.) Zbylé dva kořeny pak můžeme dopočítat tak, že vydělíme původní polynom

monočlenem $x-x_0$ a vyřešíme kvadratickou rovnici. Alternativně, není těžké ověřit, že všechny tři kořeny našeho polynomu lze vyjádřit jako

$$x_0 = u - v, \qquad x_1 = \omega u - \omega^2 v, \qquad x_2 = \omega^2 u - \omega v,$$

kde $\omega = e^{\frac{2\pi i}{3}} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ je komplexní třetí odmocnina z jedné.

**Příklad.** Vyřešíme rovnici

$$x^3 - 6x - 9 = 0.$$

Soustava $3uv = -6$, $v^3 - u^3 = -9$ má řešení $u = \sqrt[3]{\frac{9+7}{2}} = 2$, $v = \sqrt[3]{\frac{-9+7}{2}} = -1$, kořeny tedy jsou

$$x_0 = u - v = 3, \quad x_1 = \omega u - \omega^2 v = \frac{-3+\sqrt{3}i}{2}, \quad x_2 = \omega^2 u - \omega v = \frac{-3-\sqrt{3}i}{2}.$$

Na závěr předvedeme *Ferrariho postup* na řešení kvartické rovnice

$$x^4 + bx^2 + cx + d = 0.$$

Napišme rovnici ve tvaru

$$x^4 + 2ux^2 + u^2 = -bx^2 - cx - d + 2ux^2 + u^2 = (2u - b)x^2 - cx + (u^2 - d)$$

kde $u$ je jakýsi zatím neznámý parametr. Všimněte si, že levou stranu lze napsat jako $(x^2 + u)^2$. Kdybychom i pravou stranu uměli napsat jako druhou mocninu, mohli bychom obě strany odmocnit a získat tak kvadratickou rovnici pro $x$. Aby pravá strana byla mocninou, diskriminant musí být roven nule, tj.

$$c^2 - 4(2u - b)(u^2 - d) = 0.$$

Tím dostáváme rovnici třetího stupně pro $u$, přičemž nějaký její kořen $u_0$ nalezneme pomocí Tartagliova vzorce. S tímto $u_0$ můžeme obě strany dané rovnice odmocnit a získáme dvě kvadratické rovnice:

$$x^2 + u_0 = (2u_0 - b)x - \frac{c}{2} \qquad \text{a} \qquad x^2 + u_0 = -(2u_0 - b)x + \frac{c}{2}.$$

Tak nalezneme všechny čtyři kořeny původní rovnice. Ačkoliv popsaný postup připomíná spíše algoritmus než vzorec, v principu je možné vyjádřit všechna čtyři řešení pomocí koeficientů dané rovnice, operací $+, -, \cdot, :$ a druhých a třetích odmocnin.

**Příklad.** Vyřešíme rovnici

$$x^4 + x^2 + 4x - 3 = 0.$$

Diskriminant vede na rovnici $-2u^3 + u^2 - 6u + 7 = 0$, která má řešení např. $u_0 = 1$. Původní rovnici upravíme na tvar $(x^2 + 1)^2 = (x - 2)^2$, a tak stačí řešit rovnice

$$x^2 + 1 = x - 2 \qquad \text{a} \qquad x^2 + 1 = -x + 2.$$

Řešením jsou čísla

$$x_{0,1} = \frac{1 \pm \sqrt{11}i}{2} \qquad \text{a} \qquad x_{2,3} = \frac{-1 \pm \sqrt{5}}{2}.$$

Pro rovnice *pátého* stupně se nedařilo najít vzorec ani 200 let po Cardanovi. Koncem 18. století přišel Paolo Ruffini s argumentem, že žádný vzorec, který by používal pouze čtyři základní opearce a odmocniny, neexistuje. Důkaz však nebyl korektní a dokončil jej v roce 1824 Niels Henrik Abel. Až *Galoisova teorie* ale vysvětlila, proč tomu tak je a proč je stupeň 5 hraniční.

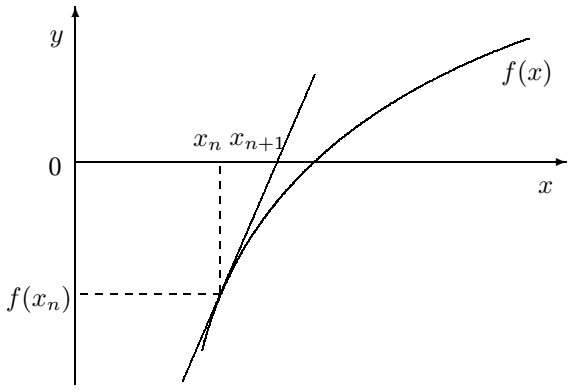
Aby bylo jasno, některé polynomy pátého stupně tzv. *řešitelné v radikálech* jsou: např. kořeny polynomu $x^5-1$ jsou číslo 1 a dále kořeny polynomu $1+x+x^2+x^3+x^4$, který je řešitelný Ferrariho vzorcem. Avšak existují polynomy stupně 5, jejichž žádný kořen uvedeným způsobem vyjádřit nelze: např. polynom $x^5 - x + 1$, nebo obecně např. jakýkoliv ireducibilní polynom prvočíselného stupně $n \geq 5$, který má právě dva imaginární a $n - 2$ reálných kořenů (cvičení: zkuste takový pomocí Eisensteinova kritéria najít!).

Galoisova věta pak dává návod, jak rozhodnout, zda je daný polynom řešitelný v radikálech: stačí spočítat tzv. *Galoisovu grupu* tohoto polynomu; tato grupa je *řešitelná* právě tehdy, když je dotyčný polynom řešitelný v radikálech. Co je to grupa, se dozvíte v následujících kapitolách. Galoisovou grupou daného polynomu se rozumí grupa všech $\mathbb{Q}$-automorfismů rozkladového nadtělesa tohoto polynomu (viz Sekce 26). Pojem řešitelnosti grupy v těchto skriptech rozebírán nebude, viz libovolná základní učebnice teorie grup. Uveďme jen, že pro malé grupy je celkem snadné řešitelnost testovat. Galoisova grupa polynomu stupně $n$ je podgrupou grupy $\mathbf{S}_n$. Tato grupa je pro $n < 5$ řešitelná a pro $n \geq 5$ řešitelná není (plyne ihned z poznámek na konci Sekce 17). A to je ten pravý důvod, proč vzorce existují jen po stupeň 4. Pro podrobnější informace o Galoisově teorii odkazujeme na nějakou učebnici komutativní algebry.

### 9.5. * Newtonova metoda.

Na závěr si ve zkratce ukážeme obecnou *Newtonovu metodu*, která slouží k *přibližnému* výpočtu kořene rovnice $f(x) = 0$ pro diferencovatelnou funkci $f$ na reálných číslech. Ve výpočetní praxi se k nalezení kořenů polynomu stupně $> 2$ používá právě nějaká varianta tohoto algoritmu, neboť málokdy je potřeba kořen zjistit přesně.

Buď $x_0$ nějaká aproximace hledaného kořene. Budeme konstruovat posloupnost $x_1, x_2, \ldots$ postupně zpřesňující tento odhad.



Všimněte si, že platí $f'(x_n) = \frac{-f(x_n)}{x_{n+1}-x_n}$ (protilehlá ku přilehlé), a tedy novou (lepší) aproximaci dostaneme z předchozí volbou

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

Dá se dokázat, že pro *hezké funkce* $f$ a *při vhodné volbě* $x_0$ konverguje posloupnost $x_0, x_1, x_2, \dots$ k nějakému kořeni, a to kvadratickou rychlostí (tj. existuje konstanta $C$ taková, že pro všechna $n$ platí $|x_{n+1} - x| \leq C \cdot |x_n - x|^2$). Co přesně znamená *hezká funkce* a *vhodná volba* $x_0$ necháme na starosti numerické matematice.

9.6. **Věta o interpolaci.**

S kořeny polynomů souvisí tzv. *interpolace*: předepíšeme-li hodnoty v $n$ bodech, existuje právě jeden polynom stupně $< n$, který v těchto bodech nabývá daných hodnot.

**Věta 9.6** (o interpolaci)**.** *Buď* $\mathbf{T}$ *těleso a uvažujme po dvou různé body* $a_1, \dots, a_n \in T$ *a libovolné hodnoty* $u_1, \dots, u_n \in T$*. Pak existuje právě jeden polynom* $f \in T[x]$ *stupně* $< n$ *splňující* $f(a_i) = u_i$ *pro všechna* $i = 1, \dots, n$*.*

Není těžké nahlédnout, že řešením je polynom

$$f = \sum_{i=1}^{n} \left( u_i \cdot \prod_{j \neq i} \frac{x - a_j}{a_i - a_j} \right),$$

říká se mu někdy *Lagrangeův interpolační polynom.*

*Důkaz.* Dosazením do uvedeného vzorce snadno zjistíme, že

$$f(a_k) = 0 + \ldots + 0 + u_k \cdot \prod_{j \neq k} \frac{a_k - a_j}{a_k - a_j} + 0 + \ldots + 0 = u_k.$$

Zbývá dokázat jednoznačnost. Uvažujme dva polynomy $f, g$ stupně $< n$ splňující $f(a_i) = g(a_i) = u_i$ pro všechna $i$ a označme $h = f - g$. Pak $h(a_i) = 0$ pro všechna $i$, tedy podle Tvrzení 9.1 $x - a_i \mid h$ pro každé $i$ a z ireducibility těchto polynomů plyne také $(x - a_1) \cdot \ldots \cdot (x - a_n) \mid h$. Protože $\deg h < n$, musí být $h = 0$, tj. $f = g$. □

Pokud se čtenáři zdá, že důkaz jednoznačnosti velmi připomíná důkaz Čínské věty o zbytcích, tak to není náhoda. Ač to na první pohled nevypadá, obě věty se dají společně popsat v řeči izomorfismu jistých faktorokruhů a jsou důsledkem tzv. Zobecněné Čínské věty o zbytcích, která je předmětem Sekce 22.3.

**Důsledek 9.7.** *Buď* $\mathbf{T}$ konečné *těleso. Pak pro každou funkci* $f : T \to T$ *existuje právě jeden polynom* $g$ *stupně* $< |T|$ *takový, že* $f(a) = g(a)$ *pro každé* $a \in T$*.*

*Důkaz.* Interpolujme v bodě $a$ hodnotou $f(a)$, pro každé $a \in T$. □

Pro *nekonečná* tělesa samozřejmě nic takového platit nemůže, přesto polynomy hrají důležitou roli i v reálné analýze: *Weierstrassova věta* říká, že každou spojitou reálnou funkci na omezeném uzavřeném intervalu lze polynomem libovolně přesně aproximovat (tj. pro každou spojitou $f : [u, v] \to \mathbb{R}$ a každé $\varepsilon > 0$ existuje polynom $g \in \mathbb{R}[x]$ takový, že $|f(a) - g(a)| < \varepsilon$ pro každé $a \in [u, v]$).

## 10. * Vícenásobné kořeny a lineární diferenční rovnice

**Cíl.** *Násobnost kořene daného polynomu souvisí s kořeny derivací tohoto polynomu. Uvedená věta má pěknou aplikaci v důkazu algoritmu na řešení soustav lineárních diferenčních rovnic.*

### 10.1. **Vícenásobné kořeny.**

Tvrzení 9.1 umožňuje definovat násobnost kořene daného polynomu.

**Definice.** Řekneme, že $a \in R$ je *$n$-násobný kořen* polynomu $f \in R[x]$, pokud

$$(x-a)^n \mid f \quad \text{a} \quad (x-a)^{n+1} \nmid f.$$

Z analýzy jsou dobře známy derivace funkcí a speciálně také polynomů nad reálnými čísly. V oboru reálných čísel má derivace jistý geometrický význam (tečna grafu) a tak se také definuje (pomocí $\varepsilon, \delta$-kalkulu). Pro polynomy se z této definice odvodí jistý vzorec, ve kterém figurují koeficienty původního polynomu.

V obecných oborech se geometrická představa ztrácí (co je tečna grafu funkce na celých číslech?). Přesto má smysl derivaci zavést, a to pomocí zmíněného vzorce. Na geometrii můžeme zapomenout, ale algebraické vlastnosti zůstávají: viz Lemma 10.1 a především Věta 10.2.

Protože se ve vzorci vyskytují přirozená čísla, musíme si ujasnit, co znamenají v obecném oboru $\mathbf{R}$: pod přirozeným číslem $n$ budeme rozumět prvek

$$\underbrace{1+1+\ldots+1}_{n} \in R.$$

*Charakteristikou* oboru $\mathbf{R}$ pak rozumíme nejmenší $n$ takové, že

$$\underbrace{1+1+\ldots+1}_{n} = 0,$$

pokud takové $n$ existuje, resp. 0 v opačném případě.

**Definice.** Definujeme *derivaci polynomu* $f = \sum_{i=0}^{n} a_i x^i$ předpisem

$$f' = \sum_{i=0}^{n-1} (i+1) a_{i+1} x^i$$

a derivace vyšších řádů induktivně

$$f^{(0)} = f \quad \text{a} \quad f^{(k+1)} = (f^{(k)})'.$$

**Lemma 10.1.** *Buď $\mathbf{R}$ obor integrity, $f, g \in R[x]$ a $n \in \mathbb{N}$. Pak*

(1) $(f+g)^{(n)} = f^{(n)} + g^{(n)}$;
(2) $(f \cdot g)^{(n)} = \sum_{i=0}^{n} \binom{n}{i} \cdot f^{(i)} \cdot g^{(n-i)}$ [Leibnitzova formule];
(3) $(f^n)' = n \cdot f^{n-1} \cdot f'$.

Důkaz je pouze technický výpočet a doporučujeme čtenáři jej provést samostatně. Níže je uveden stručný návod.

*Princip důkazu.* (1) Indukcí podle $n$. Pro $n = 1$, je-li $f = \sum a_i x^i$, $g = \sum b_i x^i$, pak $f' + g'$ i $(f+g)'$ lze rozepsat na $\sum (i+1)(a_{i+1} + b_{i+1}) x^i$. Indukční krok plyne z $(f+g)^{(n)} = ((f+g)^{(n-1)})' = (f^{(n-1)} + g^{(n-1)})' = (f^{(n-1)})' + (g^{(n-1)})' = f^{(n)} + g^{(n)}$.

(2) Indukcí podle $n$. Pro $n = 1$, je-li $f = \sum a_i x^i$, $g = \sum b_i x^i$, pak $(fg)'$ i $fg' + f'g$ lze rozepsat na $\sum_i (i+1)(\sum_{j+k=i+1} a_j b_k) x^i$. V indukčním kroku využijte známý vzorec $\binom{n}{i} + \binom{n}{i+1} = \binom{n+1}{i+1}$.

(3) se dokáže snadno indukcí pomocí (2). □

Násobnost kořene daného polynomu úzce souvisí s kořeny derivací tohoto polynomu. Vztah popisuje následující věta.

**Věta 10.2.** *Buď* $\mathbf{R}$ *obor integrity,* $0 \neq f \in R[x]$, $a \in R$ *a předpokládejme, že charakteristika oboru* $\mathbf{R}$ *je buď* 0, *nebo je větší než* $\deg f$. *Pak jsou následující tvrzení ekvivalentní:*

(1) $a$ *je* $n$*-násobný kořen polynomu* $f$*;*
(2) $f^{(0)}(a) = \ldots = f^{(n-1)}(a) = 0$ *a* $f^{(n)}(a) \neq 0$.

*Důkaz.* (1) $\Rightarrow$ (2). Protože je $a$ $n$-násobný kořen polynomu $f$, můžeme napsat

$$f = (x-a)^n \cdot g$$

pro nějaký polynom $g$ splňující $g(a) \neq 0$. Pomocí Leibnitzovy formule spočítáme $k$-tou derivaci polynomu $f$ pro $k \leq n$:

$$\begin{aligned} f^{(k)} &= \sum_{i=0}^{k} \binom{k}{i} \cdot ((x-a)^n)^{(i)} \cdot g^{(k-i)} \\ &= \sum_{i=0}^{k} \binom{k}{i} \cdot n(n-1) \cdot \ldots \cdot (n-i+1) \cdot (x-a)^{n-i} \cdot g^{(k-i)}. \end{aligned}$$

Je-li $k < n$, v každém členu součtu je $x - a$ v nenulové mocnině, a tak dostáváme

$$f^{(k)}(a) = \sum_{i=0}^{k} 0 = 0.$$

Je-li $k = n$, pak

$$f^{(n)} = \binom{n}{n} \cdot n! \cdot g^{(0)} + \sum_{i=0}^{n-1} \binom{n}{i} \cdot n(n-1) \cdot \ldots \cdot (n-i+1) \cdot (x-a)^{n-i} \cdot g^{(n-i)}$$

a ze stejného důvodu

$$f^{(n)}(a) = 1 \cdot n! \cdot g(a) + \sum_{i=0}^{n-1} 0 = n! \cdot g(a).$$

Kdyby $f^{(n)}(a) = 0$, měli bychom (z definice oboru integrity) buď $n! = 0$, nebo $g(a) = 0$. Přitom $g(a) \neq 0$ (viz začátek důkazu), takže by bylo $n! = n(n-1) \cdot \ldots \cdot 1 = 0$. Opět, z definice oboru integrity, některý z prvků $1, \ldots, n$ by musel být roven nule. A to je ve sporu s předpokladem na charakteristiku oboru $\mathbf{R}$.

(2) $\Leftarrow$ (1) Protože $f^{(0)}(a) = f(a) = 0$, prvek $a$ je kořen polynomu $f$. Musí to tedy být $m$-násobný kořen pro nějaké $m \geq 1$. Užitím výše dokázané implikace dostáváme, že $f^{(0)}(a) = \ldots = f^{(m-1)}(a) = 0$ a $f^{(m)}(a) \neq 0$, a tudíž $m = n$. □

**Úloha.** Spočtěte násobnost kořene 1 polynomu $f = x^4 + x^3 + x^2 + x + 1$ v $\mathbb{Z}_5[x]$.

*Řešení.* Postupně spočteme $f(1) = 0$; $f' = 4x^3 + 3x^2 + 2x + 1$, tedy $f'(1) = 0$; $f'' = 2x^2 + x + 2$, tedy $f''(1) = 0$; $f''' = 4x + 1$, tedy $f'''(1) = 0$; a nakonec $f'''' = 4$. Čili 1 je 4-násobný kořen. A skutečně, roznásobením snadno ověříme, že $(x-1)^4 = f$. Předpoklady věty jsou splněny, neboť charakteristika $\mathbb{Z}_5$ je 5. □

**Úloha.** Nalezněte všechny dvojnásobné komplexní kořeny polynomu $f = x^8 + x + 6$.

*Řešení.* Je-li $a$ alespoň dvojnásobným kořenem polynomu $f$, pak je společným kořenem polynomů $f, f'$, tedy $x - a$ dělí oba tyto polynomy, a tedy dělí také $\mathrm{NSD}(f, f')$. Jak snadno spočteme Eukleidovým algoritmem, $\mathrm{NSD}(f, f') = 1$, tedy $f$ žádné vícenásobné kořeny nemá. □

**Poznámka.** Je-li charakteristika oboru $\mathbf{R}$ příliš malá, věta neplatí: může se stát, že $f^{(n)}(a) = 0$. Podíváme-li se na závěr důkazu, zjistíme problém v tom, že může nastat $n! = 0$. Např. polynom $f = x^4 + x^3 \in \mathbb{Z}_3[x]$ má trojnásobný kořen 0, avšak $f' = x^3$, a tak $f'' = f''' = f'''' = \cdots = 0$.

Věta 10.2 má řadu aplikací. Za všechny uveďme algoritmus na řešení jistého typu lineárních diferenčních rovnic. Věta zde umožňuje výpočetně uchopit pojem násobnosti kořene.

10.2. **Lineární diferenční rovnice.**

V celém odstavci budeme uvažovat těleso $\mathbf{T}$ charakteristiky 0, které je *algebraicky uzavřené* (tj. každý polynom z $\mathbf{T}[x]$ má v $\mathbf{T}$ tolik kořenů, kolik je jeho stupeň; viz poslední kapitola). Pro jakékoliv aplikace si vystačíme s tělesem

$$\mathbf{T} = \mathbb{C}.$$

**Definice.** *Soustavou diferenčních rovnic* nad tělesem $\mathbf{T}$ rozumíme rovnice

$$F_n(x_n, \ldots, x_{n+k}) = 0, \qquad n = 0, 1, 2, \ldots,$$

kde $F_n : T^{k+1} \to T$ jsou nějaká zobrazení. *Řešením* této soustavy je posloupnost $(x_n)_{n=0}^{\infty}$ prvků tělesa $\mathbf{T}$ takových, že jsou tyto rovnice splněny pro každé $n$.
Soustavu diferenčních rovnic nazýváme

- *lineární* stupně $k$, pokud pro všechna $n$

$$F_n(y_0, \ldots, y_k) = a_{n0}y_0 + a_{n1}y_1 + \ldots + a_{nk}y_k - c_n, \quad a_{nk} \neq 0.$$

- *homogenní*, pokud $c_n = 0$ pro všechna $n$;
- *s konstantními koeficienty*, pokud $F_0 = F_1 = F_2 = \ldots$

*Počátečními podmínkami* pro lineární diferenční rovnici stupně $k$ rozumíme hodnoty $x_0, \ldots, x_{k-1}$.

V případě konstatních koeficientů lze tedy hovořit o jedné rovnici. My se budeme zajímat o *homogenní lineární diferenční rovnice s konstantními koeficienty*, tj. rovnice tvaru

$$(\dagger) \qquad a_0x_n + a_1x_{n+1} + \ldots + a_kx_{n+k} = 0, \qquad n = 0, 1, 2, \ldots,$$

kde $a_0, a_1, \ldots, a_k$ jsou koeficienty z $\mathbf{T}$, $a_k \neq 0$. Všimněte si, že tato rovnice má vždy nějaké řešení (např. posloupnost samých nul) a jsou-li dány počáteční podmínky, pak je řešení této rovnice právě jedno.

*Charakteristickým polynomem* rovnice (†) rozumíme polynom

$$\chi = a_0 + a_1x + a_2x^2 + \ldots a_kx^k \in T[x].$$

Označme $u_1, \dots, u_m$ jeho kořeny v $\mathbf{T}$ a $s_1, \dots, s_m$ jejich násobnosti (díky algebraické uzavřenosti máme $s_1 + \cdots + s_m = k$).

**Věta 10.3.** *Každá posloupnost, která je řešením rovnice* (†)*, lze vyjádřit jako lineární kombinace posloupností*

$$(u_j^n),\ (n \cdot u_j^n),\ (n^2 \cdot u_j^n),\ \dots,\ (n^{s_j-1} \cdot u_j^n), \qquad j = 1, \dots, m.$$

*(Lineární kombinace se rozumí ve vektorovém prostoru všech posloupností nad* $\mathbf{T}$*.)*

Jsou-li dány počáteční podmínky, dosadíme do obecného řešení hodnoty $n = 0, \dots, k-1$, čímž vyjde soustava lineárních rovnic, jejímž řešením jsou koeficienty v té lineární kombinaci. Než Větu 10.3 dokážeme, ilustrujeme algoritmus na několika příkladech.

**Příklad** (Geometrická posloupnost)**.** Řešme rovnici

$$x_{n+1} = 2x_n$$

s počáteční podmínkou $x_0 = 1$. Charakteristický polynom této rovnice je $\chi = x - 2$. Polynom $\chi$ má jeden jednonásobný kořen $x = 2$, řešení tedy má tvar $x_n = a \cdot 2^n$ pro nějaký koeficient $a$. Z počáteční podmínky, dosazením $n = 0$, dopočteme $1 = x_0 = a \cdot 2^0 = a$. Tedy, jak každý ví,

$$x_n = 2^n.$$

**Příklad** (Fibonacciho posloupnost)**.** Řešme rovnici

$$x_{n+1} = x_n + x_{n-1}$$

s počátečními podmínkami $x_0 = 0$, $x_1 = 1$. Charakteristický polynom této rovnice je $\chi = x^2 - x - 1$ a jeho kořeny jsou $u_1 = \frac{1+\sqrt{5}}{2}$ a $u_2 = \frac{1-\sqrt{5}}{2}$, oba jednonásobné. Řešení tedy má tvar

$$x_n = a \cdot u_1^n + b \cdot u_2^n$$

pro nějaká $a, b$. Z počátečních podmínek, dosazením $n = 0, 1$, získáme soustavu $a + b = 0$, $au_1 + bu_2 = 1$, čili $a = \frac{1}{\sqrt{5}}$, $b = -\frac{1}{\sqrt{5}}$ a

$$x_n = \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2}\right)^n.$$

**Příklad.** Řešme rovnici

$$x_{n+1} = x_n + x_{n-1} - x_{n-2}$$

s počátečními podmínkami $x_0 = 0$, $x_1 = 1$, $x_2 = 1$. Charakteristický polynom této rovnice je $\chi = x^3 - x^2 - x + 1$ a jeho kořeny jsou $u_1 = 1$ a $u_2 = -1$, přičemž kořen $u_1$ je dvojnásobný. Řešení tedy má tvar

$$x_n = a \cdot 1^n + b \cdot n \cdot 1^n + c \cdot (-1)^n = a + b \cdot n + c \cdot (-1)^n$$

pro nějaká $a, b, c$. Z počátečních podmínek, dosazením $n = 0, 1, 2$, získáme soustavu $a + c = 0$, $a + b - c = 1$, $a + 2b + c = 1$ a jejím výpočtem řešení

$$x_n = \frac{1}{4} + \frac{1}{2} \cdot n - \frac{1}{4} \cdot (-1)^n = \left[\frac{n+1}{2}\right].$$

Věta 10.3 je důsledkem následujících dvou lemmat.

**Lemma 10.4.** *Řešení rovnice* (†) *tvoří podprostor vektorového prostoru všech posloupností nad* $\mathbf{T}$*.*

*Důkaz.* Potřebujeme dokázat uzavřenost množiny všech řešení na operace vektorových prostorů. Předně si všimněte, že nulová posloupnost je řešením. A pokud posloupnosti $(x_i)$ a $(y_i)$ jsou řešení, tj. pokud pro všechna $n$

$$\sum_{i=0}^{k} a_i x_{n+i} = 0 \qquad \text{a} \qquad \sum_{i=0}^{k} a_i y_{n+i} = 0,$$

pak i $u \cdot (x_i) = (ux_i)$ a $(x_i) + (y_i) = (x_i + y_i)$ jsou řešení, neboť

$$\sum_{i=0}^{k} a_i u x_{n+i} = u \cdot \sum_{i=0}^{k} a_i x_{n+i} = u \cdot 0 = 0$$

a

$$\sum_{i=0}^{k} a_i (x_{n+i} + y_{n+i}) = \sum_{i=0}^{k} a_i x_{n+i} + \sum_{i=0}^{k} a_i y_{n+i} = 0 + 0 = 0$$

pro všechna $n$. □

**Lemma 10.5.** *Posloupnosti*

$$(u_j^n),\ (n \cdot u_j^{n-1}),\ (n(n-1) \cdot u_j^{n-2}),\ \ldots,\ (n(n-1)\cdots(n-s_j+2) \cdot u_j^{n-s_j+1}),$$

*$j = 1, \ldots, m$, tvoří bázi podprostoru všech řešení rovnice* (†).

*Důkaz.* Dimenze tohoto podprostoru je zřejmě $\leq k$, protože řešení rovnice (†) jsou dána jednoznačně svými prvními $k$ hodnotami. Stačí tedy dokázat, že (1) jsou tyto posloupnosti skutečně řešením rovnice (†) a že (2) jsou lineárně nezávislé.

(1) Uvažujme $j \in \{1, \ldots, m\}$ a $l \in \{0, \ldots, s_j - 1\}$. Dokážeme, že $l$-tá posloupnost odpovídající $j$-tému kořeni je skutečně řešením, tj. že pro každé $n$

$$\sum_{i=0}^{k} a_i (n+i)(n+i-1)\cdots(n+i-l+1) \cdot u_j^{n+i-l} = 0.$$

Označíme-li $f$ polynom

$$f = x^n \cdot \chi = \sum_{i=0}^{k} a_i x^{n+i},$$

můžeme uvedenou rovnost napsat jako

$$f^{(l)}(u_j) = 0.$$

Protože $u_j$ je $s_j$-násobný kořen polynomu $\chi$ i $f$, podle Věty 10.2 tato rovnost platí.

(2) Uvažujme prvních $k$ hodnot posloupností ze znění lemmatu jako vektory $(x_0, \ldots, x_{k-1}) \in T^k$. Kdyby byly dané posloupnosti lineárně závislé, pak by byly jistě lineárně závislé i tyto vektory v prostoru $\mathbf{T}^k$. Napišme je po řádcích do matice:

$$\begin{pmatrix}
\vdots & \vdots & \vdots & & \vdots \\
1 & u_j & u_j^2 & \ldots & u_j^{k-1} \\
0 & 1 & 2u_j & \ldots & (k-1)u_j^{k-2} \\
0 & 0 & 2 & \ldots & (k-1)(k-2)u_j^{k-3} \\
\vdots & \vdots & \vdots & & \vdots \\
0 & 0 & 0 & \ldots & (k-1)(k-2)\cdots(k-s_j+1)u_j^{k-s_j} \\
\vdots & \vdots & \vdots & & \vdots
\end{pmatrix}$$

Tato matice by byla singulární, tedy i její *sloupcové* vektory by byly lineárně závislé; označíme-li $c_0, \dots, c_{k-1}$ koeficienty, aspoň jeden nenulový, s nimiž lze ze sloupcových vektorů lineárně nakombinovat nulový vektor, máme pro každé $j = 1, \dots, m$

$$\sum_{i=0}^{k-1} c_i u_j^i = 0, \quad \sum_{i=0}^{k-1} c_i i u_j^{i-1} = 0, \quad \dots, \quad \sum_{i=0}^{k-1} c_i i(i-1)\cdots(i-s_j+2) u_j^{i-s_j+1} = 0.$$

Nyní uvažujme polynom $f = \sum_{i=0}^{k-1} c_i x^i$. Uvedené rovnosti lze přepsat jako

$$f^{(0)}(u_j) = 0, \quad f^{(1)}(u_j) = 0, \quad \dots, \quad f^{(s_j-1)}(u_j) = 0.$$

Podle Věty 10.2 má tedy polynom $f$ pro každé $j = 1, \dots, m$ kořen $u_j$ násobnosti nejméně $s_j$, čili celkem má nejméně $k$ kořenů (včetně násobnosti). Což je ve sporu s tím, že $\deg f \leq k-1$. □

*Důkaz Věty 10.3.* Vzhledem k Lemmatu 10.4 lze znění věty přeložit tak, že posloupnosti

$$(u_j^n),\ (n \cdot u_j^n),\ (n^2 \cdot u_j^n),\ \dots,\ (n^{s_j-1} \cdot u_j^n), \qquad j = 1, \dots, m$$

tvoří bázi podprostoru řešení. Zbývá dokázat, že tyto posloupnosti generují tentýž podprostor jako posloupnosti

$$(u_j^n),\ (n \cdot u_j^{n-1}),\ (n(n-1) \cdot u_j^{n-2}),\ \dots,\ (n(n-1)\cdots(n-s_j+2) \cdot u_j^{n-s_j+1})$$

ze znění Lemmatu 10.5. Přenásobením konstantou $u_j$ získáme ekvivalentní sadu posloupností

$$(u_j^n),\ (n \cdot u_j^n),\ (n(n-1) \cdot u_j^n),\ \dots,\ (n(n-1)\cdots(n-s_j+2) \cdot u_j^n)$$

a je vidět, že tuto sadu získáme z první (a naopak) pomocí lineárních kombinací. □

Diferenční rovnice v praxi mají zpravidla reálné koeficienty i počáteční podmínky. Při řešení přesto můžeme narazit na komplexní čísla: charakteristický polynom může mít imaginární kořeny. Výsledné řešení pak bude vyjádřeno pomocí komplexních čísel, přestože všechny hodnoty posloupnosti jsou reálné. To není hezké. Jak se komplexních čísel zbavit?

Kdykoliv má polynom $\chi$ imaginární kořen $z = a + bi = r \cdot (\cos\varphi + i \sin\varphi)$, $b \neq 0$, pak má také kořen $\bar{z} = a - bi = r \cdot (\cos\varphi - i \sin\varphi)$, a protože podle Moivreovy věty $z^n = r^n \cdot (\cos n\varphi + i \sin n\varphi)$ a $\bar{z}^n = r^n \cdot (\cos n\varphi - i \sin n\varphi)$, v bázi prostoru řešení můžeme nahradit *komplexní* posloupnosti

$$(n^i \cdot z^n) \qquad \text{a} \qquad (n^i \cdot \bar{z}^n)$$

za *reálné* posloupnosti

$$(n^i \cdot r^n \cdot \cos n\varphi) \qquad \text{a} \qquad (n^i \cdot r^n \cdot \sin n\varphi).$$

**Příklad.** Řešme rovnici

$$x_{n+2} = -x_n$$

s počátečními podmínkami $x_0 = 1$ a $x_1 = 2$. Charakteristický polynom této rovnice je $\chi = x^2 + 1$ a jeho kořeny jsou $u_1 = i$ a $u_2 = -i$. Řešení podle Věty 10.3 tedy má tvar

$$x_n = a \cdot i^n + b \cdot (-i)^n$$

pro nějaká $a, b$. Z počátečních podmínek dostaneme soustavu $a+b=1$, $ai-bi=2$, čili $a=\frac{1}{2}-i$, $b=\frac{1}{2}+i$ a

$$x_n = \left(\frac{1}{2}-i\right)\cdot i^n + \left(\frac{1}{2}+i\right)\cdot(-i)^n.$$

To nám do chování posloupnosti dává pramalý vhled. Užitím uvedeného triku budeme hledat řešení tvaru

$$x_n = a\cdot\cos\frac{n\pi}{2} + b\cdot\sin\frac{n\pi}{2}$$

pro nějaká $a, b$ (protože $i=\cos\frac{\pi}{2}+i\sin\frac{\pi}{2}$). Z počátečních podmínek dostaneme soustavu $a=1$ a $b=2$ a hned vidíme, že

$$x_n = \cos\frac{n\pi}{2} + 2\sin\frac{n\pi}{2}.$$

**Poznámka.** Dokázali jsme, že obecné řešení rovnice (†) s reálnými koeficienty je lineární kombinací posloupností tvaru

$$(f(n)\cdot r^n\cdot\cos n\varphi) \qquad \text{a} \qquad (f(n)\cdot r^n\cdot\sin n\varphi),$$

kde $f$ je polynom a $r, \varphi$ reálná čísla. Jde tedy o kombinaci polynomiálního a exponenciálního růstu či klesání a oscilace.

## Obecné algebry

### 11. Algebry

**Cíl.** *Abstraktním konceptem, který stojí za celou moderní algebrou, je množina s danou sadou operací, tzv. algebra. Seznámíme se se základními strukturními pojmy jako podalgebra, generátory, direktní součin a budeme zkoumat zobrazení, která zachovávají operace, tzv. homomorfismy. Hlouběji se podíváme na pojem izomorfismu, tj. na otázku, kdy jsou dvě struktury z algebraického hlediska totožné.*

11.1. **Algebry.**
V této chvíli by měl být čtenář seznámen se základy dvou klasických algebraických disciplín: s lineární algebrou a se základy komutativní algebry. Obě teorie začínaly podobnou definicí: zavedla se jistá struktura (vektorový prostor, obor integrity) jako *množina*, na níž jsou definovány nějaké *operace* splňující jistou sadu *axiomů*. Tento přístup vede k abstraktnímu pojmu algebry.

**Definice.** *$n$-ární operací* na množině $A$ rozumíme zobrazení z $A^n = A \times \ldots \times A$ do $A$. Speciálně, 0-ární operace je zobrazení z jednoprvkové množiny do $A$, tedy *konstanta*. Místo 1-ární říkáme *unární*, místo 2-ární říkáme *binární*.

**Definice.** *Typem algebry* rozumíme zobrazení $\tau : \Omega \to \mathbb{N} \cup \{0\}$, kde $\Omega$ je nějaká množina (nazývá se *množina symbolů*, nebo též *jazyk*). *Algebra typu* $\tau$ je dvojice $\mathbf{A} = (A, F)$, kde $A$ je neprázdná množina (*nosná množina, universum*) a $F$ je zobrazení z množiny $\Omega$ do množiny všech operací na $A$ přiřazující symbolu $\omega$ nějakou $\tau(\omega)$-ární operaci $F_\omega$ na $A$. Výsledek operace $F_\omega$ na prvcích $a_1, \ldots, a_{\tau(\omega)}$ zapisujeme jako

$$F_\omega(a_1, \ldots, a_{\tau(\omega)}).$$

Často se typ zapisuje zkráceně jako $(n_1, \ldots, n_k)$ (formálně vzato, uvažujte $\Omega = \{1, \ldots, k\}$) a algebry tohoto typu jako $(A, f_1, \ldots, f_k)$, kde $f_i$ je $n_i$-ární operace odpovídající $i$-tému symbolu.

Binární operace se zpravidla značí symboly $+, \cdot, *, \circ$ apod., pro unární operace se často používá $', -$ či $^{-1}$ (jako horní index, čti „inverz“).

Tučným písmem budeme vždy značit *algebry*, zatímco normálním písmem jejich *nosné množiny*. Není-li výslovně uvedeno jinak, označíme-li algebru $\mathbf{A}$, předpokládáme, že její nosná množina je $A$, a naopak. V běžné mluvě se rozdíl mezi algebrou a její nosnou množinou často stírá a v ručním zápise je (nedobrým) zvykem značit algebru i její nosnou množinu stejně, byť, formálně vzato, jde o různé věci. V tištěném textu je budeme striktně rozlišovat s výjimkou zavedených značení typu $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ apod.

Studiem obecných algeber se zabývá obor univerzální algebra. V tomto kurzu se soustředíme na několik speciálních tříd algeber: obory integrity, grupy, okruhy a

tělesa. V kapitole věnované obecným algebrám se seznámíme s pojmy, které tyto teorie sdílí: podalgebry, direktní součiny a homomorfismy.

**Příklad.**

- *Tělesa* i *obory integrity* jsou algebry typu $(2,1,2,0,0)$ v jazyce $\Omega = \{+,-,\cdot,0,1\}$. Např. na množině $\mathbb{Z}$ se tyto symboly mohou interpretovat jako obyčejné sčítání, odčítání a násobení, čímž vzniká obor $\mathbb{Z} = (\mathbb{Z},+,-,\cdot,0,1)$. Nebo na množině $\{0,\dots,p-1\}$ jako sčítání, odčítání a násobení modulo $p$, čímž pro prvočíslo $p$ vzniká těleso $\mathbb{Z}_p$.
  Poznamenejme, že dělení ani invertování v tělese nelze považovat za operaci, neboť není definováno všude: $0^{-1}$ neexistuje.
- Algebra $(M_n(\mathbf{T}),+,-,\cdot,0)$, kde $M_n(\mathbf{T})$ značí množinu všech matic $n \times n$ nad tělesem $\mathbf{T}$, je jako algebra typu $(2,1,2,0)$ základním příkladem struktury zvané *okruhy*. (Jejich axiomy vzniknou z axiomů těles vypuštěním existence inverzních prvků a komutativity násobení.)
- *Grupy* jsou algebry typu $(2,1,0)$ v jazyce $\Omega = \{*,',e\}$. Jejich axiomy říkají, že binární operace $*$ je asociativní, má jednotku $e$ a existují inverzní prvky značené $'$. Základními příklady jsou algebra $(S_n,\circ,^{-1},id)$, kde $S_n$ značí množinu všech permutací na $n$-prvkové množině, $*$ se interpretuje jako skládání permutací, $'$ jako invertování a $e$ jako identická permutace; a algebra $(GL_n(\mathbf{T}),\cdot,^{-1},E)$, kde $GL_n(\mathbf{T})$ značí množinu všech regulárních matic $n \times n$ nad tělesem $\mathbf{T}$, s operacemi maticového násobení, invertování a jednotkovou maticí.
- Libovolný *svaz* $(X,\leq)$ lze považovat za algebru typu $(2,2)$ s operacemi $\vee,\wedge$.
- Logické hodnoty 0,1 s operacemi konjunkce, disjunkce a negace tvoří tzv. dvouprvkovou *Booleovu algebru* $(\{0,1\},\wedge,\vee,\neg,0,1)$.
- *Unární algebry* jsou algebry typu $(1,1,\dots,1)$. Unární algebry s jednou operací si lze představit jako orientované grafy, kde výstupní stupeň každého vrcholu je 1. S více operacemi pak jako několik takových různě barevných grafů přes sebe.
- Vektorový prostor $\mathbf{V}$ nad tělesem $\mathbf{T}$ lze považovat za algebru

  $$(V,+,-,0,f_a : a \in T)$$

  typu $(2,1,0,1,1,1,1,\dots)$, kde $f_a(v) = av$ jsou unární operace skalárního násobení prvkem $a \in T$. Uvědomte si, že násobení vektoru skalárem nelze považovat za binární operaci ve výše uvedeném smyslu, neboť jde o zobrazení $T \times V \to V$. Proto je třeba skalární násobení rozbít do řady unárních operací $f_a : V \to V$, pro každé $a \in T$ jedna.

Vzhledem k tomu, že všechny uvedené příklady mají pouze konstanty, unární a binární operace, budeme pro přehlednost v dalším textu uvažovat pouze algebry s operacemi arity $\leq 2$. Obecné definice jsou pro úplnost uvedeny na konci této kapitoly.

## 11.2. **Podalgebry.**

**Definice.** Řekneme, že podmnožina $B \subseteq A$ je *uzavřena* na

- binární operaci $*$, pokud pro každé $a,b \in B$ platí $a * b \in B$;
- unární operaci $'$, pokud pro každé $b \in B$ platí $b' \in B$;
- nulární operaci (konstantu) $c$, pokud $c \in B$.

Algebra $\mathbf{B}$ se nazývá *podalgebrou* algebry $\mathbf{A}$, pokud je množina $B \subseteq A$ je uzavřena na všechny operace algebry $\mathbf{A}$ a operace algebry $\mathbf{B}$ jsou restrikcemi operací algebry $\mathbf{A}$ na množinu $B$. Značíme $\mathbf{B} \leq \mathbf{A}$.
Je-li podmnožina $\emptyset \neq B \subseteq A$ uzavřena na všechny operace algebry $\mathbf{A}$, řekneme že *tvoří podalgebru* algebry $\mathbf{A}$.

**Příklad.** $(\mathbb{N}, +, \cdot) \leq (\mathbb{Z}, +, \cdot) \leq (\mathbb{Q}, +, \cdot) \leq (\mathbb{R}, +, \cdot)$.

**Příklad.** Množina $\mathbb{N}$ netvoří podalgebru algebry $(\mathbb{Z}, +, -)$, protože např. $1-2 \notin \mathbb{N}$.

**Příklad.** Množina $\{z \in \mathbb{C} : |z| = 1\}$ tvoří podalgebru algebry $(\mathbb{C}, \cdot)$, nikoliv však algebry $(\mathbb{C}, +)$: součin libovolných dvou komplexních čísel s absolutní hodnotou 1 má absolutní hodnotu 1, avšak např. $|1 + 1| \neq 1$.

**Tvrzení 11.1.** *Buď $\mathbf{A}$ algebra a $\mathbf{B}_i$, $i \in I$, její podalgebry. Pak $\bigcap_{i\in I} B_i$ je buď prázdná množina, nebo tvoří podalgebru algebry $\mathbf{A}$.*

Jde-li o podalgebru, budeme ji značit $\bigcap_{i\in I} \mathbf{B}_i$.

*Důkaz.* Je-li

- $*$ binární operace na $\mathbf{A}$ a $a, b \in \bigcap_{i\in I} B_i$, pak $a, b \in B_i$ pro každé $i$, tedy $a * b \in B_i$ pro každé $i$, a tedy $a * b \in \bigcap_{i\in I} B_i$;
- $'$ unární operace na $\mathbf{A}$ a $b \in \bigcap_{i\in I} B_i$, pak $b \in B_i$ pro každé $i$, tedy $b' \in B_i$ pro každé $i$, a tedy $b' \in \bigcap_{i\in I} B_i$;
- $c$ konstanta na $\mathbf{A}$, pak $c \in B_i$ pro každé $i$, a tedy $c \in \bigcap_{i\in I} B_i$.

Tedy množina $\bigcap_{i\in I} B_i$ je uzavřena na všechny operace, čili je-li neprázdná, tvoří podalgebru algebry $\mathbf{A}$. □

Pro sjednocení obdobné tvrzení neplatí: uvažujte např. algebru $(\mathbb{Z}, +)$ a podalgebry tvořené množinami $2\mathbb{Z}$ a $3\mathbb{Z}$: pak $2, 3 \in 2\mathbb{Z} \cup 3\mathbb{Z}$, avšak $2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$. Platí ale následující:

**Tvrzení 11.2.** *Buď $\mathbf{A}$ algebra a $\mathbf{B}_1 \leq \mathbf{B}_2 \leq \mathbf{B}_3 \leq \ldots$ její podalgebry. Pak $\bigcup_{i\in\mathbb{N}} B_i$ tvoří podalgebru algebry $\mathbf{A}$.*

*Důkaz.* Je-li

- $*$ binární operace na $\mathbf{A}$ a $a, b \in \bigcup_{i\in\mathbb{N}} B_i$, pak $a \in B_i$ pro nějaké $i$ a $b \in B_j$ pro nějaké $j$, tedy $a, b \in B_{\max(i,j)}$, tedy $a * b \in B_{\max(i,j)}$, a tedy $a * b \in \bigcup_{i\in\mathbb{N}} B_i$;
- $'$ unární operace na $\mathbf{A}$ a $b \in \bigcup_{i\in\mathbb{N}} B_i$, pak $b \in B_i$ pro nějaké $i$, tedy $b' \in B_i$, a tedy $b' \in \bigcup_{i\in\mathbb{N}} B_i$;
- $c$ konstanta na $\mathbf{A}$, pak $c \in B_i$ pro každé $i$, a tedy $c \in \bigcup_{i\in\mathbb{N}} B_i$.

Tedy množina $\bigcup_{i\in\mathbb{N}} B_i$ je uzavřena na všechny operace algebry $\mathbf{A}$. □

**Definice.** Nejmenší podalgebra algebry $\mathbf{A}$ obsahující danou podmnožinu $X \subset A$ se nazývá *podalgebra generovaná množinou $X$* a značí se $\langle X\rangle_{\mathbf{A}}$. Řekneme, že algebra $\mathbf{A}$ je generovaná množinou $X$, pokud $\langle X\rangle_{\mathbf{A}} = \mathbf{A}$. Často píšeme zkráceně $\langle a_1, \ldots, a_n\rangle$ místo $\langle\{a_1, \ldots, a_n\}\rangle$.

**Tvrzení 11.3.** *Je-li $\emptyset \neq X \subseteq A$, pak $\langle X\rangle_{\mathbf{A}}$ existuje.*

*Důkaz.* Vezmeme průnik všech podalgeber algebry $\mathbf{A}$ obsahujících množinu $X$. Tento je podle Tvrzení 11.1 opět podalgebrou, která obsahuje množinu $X$ a zřejmě je ze všech takových podalgeber nejmenší. □

Prvky podalgebry $\langle X\rangle_{\mathbf{A}}$ lze najít tak, že začneme s prvky množiny $X$ a aplikováním operací algebry $\mathbf{A}$ získáváme postupně další prvky. Ve chvíli, kdy už žádnou operací algebry $\mathbf{A}$ nedostaneme nic nového, tj. když už je zkonstruovaná množina *uzavřená* na operace algebry $\mathbf{A}$, získali jsme celou $\langle X\rangle_{\mathbf{A}}$.

**Příklad.**
$\langle 1\rangle_{(\mathbb{Z},+)} = \mathbb{N}$: opakováním operace $+$ získáme z prvku 1 právě všechna přirozená čísla.

**Příklad.**

- $(\mathbb{N},+) = \langle 1\rangle$, $(\mathbb{Z},+) = \langle 1,-1\rangle$, $(\mathbb{Z},+,-) = \langle 1\rangle$.
  V první algebře každý prvek dostaneme jako $1+1+\ldots+1$. U celých čísel potřebujeme nagenerovat i záporná čísla a k tomu potřebujeme prvek $-1$ (nulu dostaneme jako $1+(-1)$). V poslední algebře však máme operaci $-$, takže $-1$ nagenerujeme z jedničky.
- $(\mathbb{N},\cdot) = \langle 1, p : p \text{ je prvočíslo}\rangle$ díky základní větě aritmetiky. Tato algebra není generována žádnou konečnou množinou.
- Algebra $(S_n,\circ)$ je generována množinou všech transpozic, jak bylo dokázáno v kurzu lineární algebry (každá permutace lze napsat jako složení transpozic).

Označme $\mathrm{Sub}(\mathbf{A})$ množinu všech podmnožin $A$ uzavřených na operace algebry $\mathbf{A}$ a uvažujme uspořádanou množinu

$$\mathbf{Sub}(\mathbf{A}) = (\mathrm{Sub}(\mathbf{A}),\subseteq).$$

**Tvrzení 11.4.** *Uspořádaná množina* $\mathbf{Sub}(\mathbf{A})$ *je úplným svazem. Přitom pro každou neprázdnou množinu* $\mathcal{M}\subseteq\mathrm{Sub}(\mathbf{A})$ *platí*

$$\inf\mathcal{M} = \bigcap\mathcal{M} \quad a \quad \sup\mathcal{M} = \langle\bigcup\mathcal{M}\rangle_{\mathbf{A}}.$$

*Důkaz.* Podle Tvrzení 11.1 je průnik uzavřených podmnožin opět uzavřená podmnožina, evidentně největší mezi těmi, které jsou obsaženy ve všech množinách z $\mathcal{M}$. Tedy existují infima a podle Tvrzení 1.1 jde o úplný svaz. Přitom nejmenší podmnožina, která obsahuje všechny prvky z každé $B\in\mathcal{M}$, je $\bigcup\mathcal{M}$; a nejmenší podalgebra, která obsahuje $\bigcup\mathcal{M}$, je podalgebra touto množinou generovaná. □

Přestože $\mathrm{Sub}(\mathbf{A})\subseteq P(A) = \{B : B\subseteq A\}$, svaz $\mathbf{Sub}(\mathbf{A})$ není podsvazem svazu $(P(A),\subseteq)$. Průsek v obou svazech je sice průnik, avšak spojení v $\mathbf{Sub}(\mathbf{A})$ není sjednocení!

## 11.3. **Direktní součiny.**

**Definice.** *Direktním součinem* algeber $\mathbf{A}_i = (A_i,F_i)$, $i=1,\ldots,n$, stejného typu rozumíme algebru

$$\mathbf{A}_1\times\cdots\times\mathbf{A}_n = (A_1\times\cdots\times A_n, F),$$

jejíž operace jsou definovány následovně:

- jsou-li $*_1,\ldots,*_n$ navzájem si odpovídající binární operace algeber $\mathbf{A}_1,\ldots,\mathbf{A}_n$, pak odpovídající operaci $*$ v algebře $\mathbf{A}_1\times\cdots\times\mathbf{A}_n$ definujeme předpisem
  $$(a_1,\ldots,a_n)*(b_1,\ldots,b_n) = (a_1 *_1 b_1,\ldots,a_n *_n b_n)$$
  pro každé $a_1,b_1\in A_1,\ \ldots,\ a_n,b_n\in A_n$.

- jsou-li $'^1, \dots, '^n$ navzájem si odpovídající unární operace algeber $\mathbf{A}_1, \dots, \mathbf{A}_n$, pak odpovídající operaci $'$ v algebře $\mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ definujeme předpisem
$$(a_1, \dots, a_n)' = ((a_1)'^1, \dots, (a_n)'^n)$$
pro každé $a_1 \in A_1$, …, $a_n \in A_n$.
- jsou-li $c_1, \dots, c_n$ navzájem si odpovídající konstanty algeber $\mathbf{A}_1, \dots, \mathbf{A}_n$, pak odpovídající konstantu $c$ v algebře $\mathbf{A}_1 \times \cdots \times \mathbf{A}_n$ definujeme předpisem
$$c = (c_1, \dots, c_n).$$

Tedy operace provádíme po složkách, podobně jako s vektory. Pod pojmem *navzájem si odpovídající operace* rozumíme operace přiřazené témuž symbolu $\omega \in \Omega$.

11.4. **Homomorfismy.**
Zobrazením mezi dvěma matematickými objekty, která zachovávají jejich strukturu, se říká homomorfismy. Tento pojem by měl čtenář znát např. z diskrétní matematiky pro grafy, nebo z lineární algebry pro vektorové prostory. Zde tento pojem zavedeme pro obecné algebry.

**Definice.** Buď $\mathbf{A}$ a $\mathbf{B}$ algebry stejného typu. Zobrazení $\varphi : A \to B$ se nazývá *homomorfismus* algeber $\mathbf{A}$, $\mathbf{B}$, píšeme $\varphi : \mathbf{A} \to \mathbf{B}$, pokud

- pro každou binární operaci $*$ algebry $\mathbf{A}$ a odpovídající operaci $\circ$ algebry $\mathbf{B}$ platí pro každé $a, b \in A$
$$\varphi(a * b) = \varphi(a) \circ \varphi(b);$$
- pro každou unární operaci $'$ algebry $\mathbf{A}$ a odpovídající operaci $''$ algebry $\mathbf{B}$ platí pro každé $a \in A$
$$\varphi(a') = \varphi(a)'';$$
- pro každou konstantu $c$ algebry $\mathbf{A}$ a odpovídající konstantu $d$ algebry $\mathbf{B}$ platí
$$\varphi(c) = d.$$

Používá se následující terminologie:

- *monomorfismus*, neboli *vnoření*, je prostý homomorfismus (někdy se značí šipkou $\hookrightarrow$),
- *epimorfismus* je homomorfismus na (někdy se značí šipkou $\twoheadrightarrow$),
- *izomorfismus* je homomorfismus, který je bijekcí (užívá se symbol $\simeq$),

a dále

- *endomorfismem* algebry $\mathbf{A}$ rozumíme homomorfismus z $\mathbf{A}$ do $\mathbf{A}$,
- *automorfismem* algebry $\mathbf{A}$ rozumíme izomorfismus z $\mathbf{A}$ do $\mathbf{A}$.

**Definice.** Buď $\varphi : \mathbf{A} \to \mathbf{B}$ homomorfismus. Definujeme

- *jádro* homomorfismu $\varphi$ předpisem
$$\ker(\varphi) = \{(a, b) \in A \times A : \varphi(a) = \varphi(b)\};$$
- *obraz* homomorfismu $\varphi$ předpisem
$$\mathrm{Im}(\varphi) = \{b \in B : b = \varphi(a) \text{ pro nějaké } a \in A\}.$$

**Tvrzení 11.5.** *Buď $\varphi : \mathbf{A} \to \mathbf{B}$ homomorfismus. Pak*

(1) $\ker(\varphi)$ *je ekvivalence na množině $A$;*
(2) $\mathrm{Im}(\varphi)$ *tvoří podalgebru algebry* $\mathbf{B}$.

*Důkaz.* (1) je očividná. (2) Je-li

- $*$ binární operace na $\mathbf{A}$ a $\circ$ odpovídající operace na $\mathbf{B}$, pak pro $b_1, b_2 \in \mathrm{Im}(\varphi)$ můžeme napsat $b_1 = \varphi(a_1)$ a $b_2 = \varphi(a_2)$ pro nějaká $a_1, a_2 \in A$, a tedy $b_1 \circ b_2 = \varphi(a_1) \circ \varphi(a_2) = \varphi(a_1 * a_2) \in \mathrm{Im}(\varphi)$;
- $'$ unární operace na $\mathbf{A}$ a $''$ odpovídající operace na $\mathbf{B}$, pak pro $b \in \mathrm{Im}(\varphi)$ můžeme napsat $b = \varphi(a)$ pro nějaké $a \in A$, a tedy $b'' = \varphi(a)'' = \varphi(a') \in \mathrm{Im}(\varphi)$;
- $c$ konstanta na $\mathbf{A}$ a $d$ odpovídající konstanta na $\mathbf{B}$, pak $d = \varphi(c) \in \mathrm{Im}(\varphi)$.

□

**Příklad.**

- Zobrazení $(\mathbb{C}, \cdot) \to (\mathbb{R}, \cdot)$, $z \mapsto |z|$, je homomorfismus, neboť $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$. Jeho jádrem je ekvivalence, jejíž bloky jsou soustředné kružnice se středem v nule. Jeho obrazem jsou nezáporná reálná čísla.
- Zobrazení $(\mathbb{C}, +) \to (\mathbb{R}, +)$, $z \mapsto |z|$, *není* homomorfismus, neboť $|1 + (-1)| = 0$, ovšem $|1| + |-1| = 2$.
- Zobrazení $(\mathbb{R}, +) \to (\mathbb{R}, \cdot)$, $x \mapsto 2^x$, je homomorfismus, neboť $2^{x+y} = 2^x \cdot 2^y$. Jeho jádro je triviální, jeho obrazem jsou všechna kladná reálná čísla.
- Zobrazení $(\mathbb{Z}, +, \cdot) \to (\{0, \ldots, n-1\}, +_{\bmod n}, \cdot_{\bmod n})$, $x \mapsto x \bmod n$, je epimorfismus. Jeho jádrem je ekvivalence $\equiv \pmod n$.

Úlohy typu „najděte všechny homomorfismy $\mathbf{A} \to \mathbf{B}$“ lze řešit mnoha způsoby, předvedeme dva typické. První metoda vychází z toho, že homomorfismy jsou určeny svými hodnotami na generátorech (podobně jako u vektorových prostorů).

**Úloha.** Najděte všechny homomorfismy $(\mathbb{N}, +) \to (\mathbb{N}, +)$.

*Řešení.* Uvažujme homomorfismus $\varphi$. Protože $(\mathbb{N}, +) = \langle 1 \rangle$, z hodnoty v bodě 1 dopočteme hodnoty ve všech bodech: je-li $\varphi(1) = k$, pak

$$\varphi(n) = \varphi(\underbrace{1 + \ldots + 1}_{n}) = \underbrace{\varphi(1) + \ldots + \varphi(1)}_{n} = kn.$$

Přitom je vidět, že pro libovolné $k \in \mathbb{N}$ je zobrazení $n \mapsto kn$ homomorfismus. □

Je-li generátorů příliš mnoho, jako v následujícím případě, můžeme zkusit využít existence prvků se zvláštními vlastnostmi.

**Úloha.** Najděte všechny homomorfismy $(\mathbb{Z}, \cdot) \to (\mathbb{Z}, +)$.

*Řešení.* Uvažujme homomorfismus $\varphi$. Protože $\varphi(0) = \varphi(0 \cdot 0) = \varphi(0) + \varphi(0)$, musí být $\varphi(0) = 0$. Z toho plyne $0 = \varphi(0) = \varphi(n \cdot 0) = \varphi(n) + \varphi(0) = \varphi(n)$ pro každé $n$. Existuje tedy jediný homomorfismus $n \mapsto 0$. □

**Tvrzení 11.6.** *Buď $\mathbf{A}, \mathbf{B}, \mathbf{C}$ algebry stejného typu a $\varphi : \mathbf{A} \to \mathbf{B}$ a $\psi : \mathbf{B} \to \mathbf{C}$ homomorfismy. Pak*

(1) *složené zobrazení $\psi \circ \varphi$ je homomorfismus $\mathbf{A} \to \mathbf{C}$;*
(2) *je-li $\varphi$ izomorfismus, pak inverzní zobrazení $\varphi^{-1}$ je izomorfismus $\mathbf{B} \to \mathbf{A}$.*

*Důkaz.* (1) Ověříme, že $\psi \circ \varphi$ zachovává všechny operace.

- Jsou-li $*$, $+$ a $\cdot$ odpovídající binární operace na $\mathbf{A}$, $\mathbf{B}$ a $\mathbf{C}$ , pak

$$\forall a_1, a_2 \in A \quad \varphi(a_1 * a_2) = \varphi(a_1) + \varphi(a_2),$$
$$\forall b_1, b_2 \in B \quad \psi(b_1 + b_2) = \psi(b_1) \cdot \psi(b_2),$$

a tedy pro všechna $a_1, a_2 \in A$

$$(\psi \circ \varphi)(a_1 * a_2) = \psi(\varphi(a_1 * a_2)) = \psi(\varphi(a_1) + \varphi(a_2)) \\ = \psi(\varphi(a_1)) \cdot \psi(\varphi(a_2)) = (\psi \circ \varphi)(a_1) \cdot (\psi \circ \varphi)(a_2).$$

- Jsou-li $'$, $''$ a $'''$ odpovídající unární operace na $\mathbf{A}$, $\mathbf{B}$ a $\mathbf{C}$ , pak
$$\forall a \in A \quad \varphi(a') = (\varphi(a))'', \qquad \forall b \in B \quad \psi(b'') = (\psi(b))'''$$
a tedy
$$\forall a \in A \quad (\psi \circ \varphi)(a') = \psi(\varphi(a')) = \psi(\varphi(a)'') = \psi(\varphi(a))''' = (\psi \circ \varphi)(a)'''.$$
- Jsou-li $c$, $d$ a $e$ odpovídající konstanty na $\mathbf{A}$, $\mathbf{B}$ a $\mathbf{C}$ , pak $\varphi(c) = d$, $\psi(d) = e$, a tedy $(\psi \circ \varphi)(c) = \psi(\varphi(c)) = \psi(d) = e$.

(2) Ověříme, že $\varphi^{-1}$ zachovává všechny operace.

- Jsou-li $*$ a $+$ odpovídající binární operace na $\mathbf{A}$ a $\mathbf{B}$, pak pro všechna $b_1, b_2 \in B$
$$b_1 + b_2 = \varphi(\varphi^{-1}(b_1)) + \varphi(\varphi^{-1}(b_2)) = \varphi(\varphi^{-1}(b_1) * \varphi^{-1}(b_2)),$$
a tedy
$$\varphi^{-1}(b_1 + b_2) = \varphi^{-1}(\varphi(\varphi^{-1}(b_1) * \varphi^{-1}(b_2))) = \varphi^{-1}(b_1) * \varphi^{-1}(b_2).$$
- Jsou-li $'$ a $''$ odpovídající unární operace na $\mathbf{A}$ a $\mathbf{B}$, pak pro všechna $b \in B$
$$b'' = \varphi(\varphi^{-1}(b))'' = \varphi(\varphi^{-1}(b)'),$$
a tedy
$$\varphi^{-1}(b'') = \varphi^{-1}(\varphi(\varphi^{-1}(b)')) = \varphi^{-1}(b)'.$$
- Jsou-li $c$ a $d$ odpovídající konstanty na $\mathbf{A}$ a $\mathbf{B}$, pak $\varphi(c) = d$, a tedy $\varphi^{-1}(d) = c$.

□

11.5. **Izomorfní algebry.**

Řekneme, že algebry $\mathbf{A}$ a $\mathbf{B}$ jsou *izomorfní*, značíme $\mathbf{A} \simeq \mathbf{B}$, pokud existuje izomorfismus $\mathbf{A} \to \mathbf{B}$, tj. vzájemně jednoznačné zobrazení mezi nosnými množinami, které zachovává všechny operace. Tento pojem si lze představit jako „kopírování algeber“: máme-li algebru $\mathbf{A}$, pro jednoduchost uvažujme binární $\mathbf{A} = (A, *)$, a bijektivní zobrazení $\varphi : A \to B$, můžeme na $B$ „překopírovat“ operaci $*$ předpisem

$$a \circ b = \varphi(\varphi^{-1}(a) * \varphi^{-1}(b)).$$

Z Tvrzení 11.6(2) plyne, že $\varphi$ bude izomorfismus algeber $(A, *)$ a $(B, \circ)$; každý izomorfismus si lze představit tímto způsobem. Je vidět, že izomorfní algebry mají stejné „algebraické vlastnosti“ (nebudeme se pouštět do toho, co to přesně znamená), jedna je kopií druhé, pouze došlo k přejmenování prvků.

**Příklad.** Algebry

$$(\{0, 1\}, +_{\bmod 2}) \quad \text{a} \quad (\{1, -1\}, \cdot)$$

jsou izomorfní. Podívejme se na tabulky těchto operací:

| $+$ | $0$ | $1$ |
|---|---|---|
| $0$ | $0$ | $1$ |
| $1$ | $1$ | $0$ |

| $\cdot$ | $1$ | $-1$ |
|---|---|---|
| $1$ | $1$ | $-1$ |
| $-1$ | $-1$ | $1$ |

Tyto tabulky vypadají podobně: jedna je kopií druhé, pokud přepíšeme $0 \mapsto 1$, $1 \mapsto -1$. A skutečně, toto zobrazení je, jak snadno ověříte, izomorfismus.

**Příklad.** Algebry

$$(\mathbb{C}, +) \quad \text{a} \quad (\mathbb{R}, +) \times (\mathbb{R}, +)$$

jsou izomorfní. Intuitivně, komplexní čísla se sčítají tak, že se sčítají jejich reálné složky, jednu algebru z druhé dostaneme přepisem $a + bi \mapsto (a, b)$. Formálně, toto zobrazení je, jak snadno ověříte, izomorfismus.

Poznamenejme ještě, že jde o analogii pojmu *izomorfismus grafů* známý z diskrétní matematiky: dva grafy jsou izomorfní, pokud existuje bijekce mezi jejich vrcholy, která zachovává hrany, tj. vrcholy $x, y$ jsou spojeny hranou v jednom grafu právě tehdy, když jsou jejich obrazy spojeny hranou v druhém grafu. Tedy druhý graf je kopií prvního, pouze s jinými názvy vrcholů.

**Tvrzení 11.7.** *Relace $\simeq$ je ekvivalencí na třídě všech algeber daného typu.*

*Důkaz.* Reflexivita plyne z toho, že identita je izomorfismus. Symetrie z toho, že inverzní zobrazení k izomorfismu je izomorfismus. A tranzitivita z toho, že složení izomorfismů je izomorfismus. □

Obtížnější úlohou je dokázat, že dané dvě algebry *nejsou izomorfní*. Jsou-li, stačí napsat nějaký izomorfismus. Nejsou-li, musíme nějak dokázat, že žádné zobrazení mezi nimi izomorfismem není.

**Příklad.** Algebry $(\mathbb{Z}, \cdot)$ a $(\mathbb{Z}, +)$ *nejsou* izomorfní, protože, jak jsme ukázali v minulém odstavci, jediný homomorfismus je $n \mapsto 0$.

Najít všechny homomorfismy ovšem zpravidla není snadné, často se tedy hledá tzv. *invariant*. To je vlastnost $V$ taková, že kdykoliv jsou nějaké algebry $\mathbf{A}, \mathbf{B}$ izomorfní a $\mathbf{A}$ má vlastnost $V$, pak $\mathbf{B}$ má vlastnost $V$. Např.

- počet prvků algebry je invariantem (mezi různě velkými množinami neexistuje vůbec žádná bijekce);
- minimální počet generátorů je invariantem;
- rovnosti (komutativita, asociativita, apod.);
- existence význačných prvků (např. vlastnosti typu „$\exists x \forall y\ x * y = x$“, což v lidském jazyce říká, že existuje tzv. *nulový prvek* vzhledem k operaci $*$);
- pro grupy jsou velmi účinným invariantem řády prvků, viz Sekce 14.1.

Obecně lze říci, že invariantem je jakákoliv vlastnost, kterou lze vyjádřit pomocí kvantifikátorů, proměnných, logických spojek, rovnítka a operací daných algeber (tj. tzv. *formulí 1. řádu* v daném jazyce). Případně lze využívat dalších pojmů, které jsou podobným způsobem definovány.

**Příklad.** Algebry

$$(\mathbb{C}, \cdot) \quad \text{a} \quad (\mathbb{R}, \cdot) \times (\mathbb{R}, \cdot)$$

nejsou izomorfní. (Zobrazení $a+bi \mapsto (a, b)$ evidentně izomorfismus není, komplexní čísla se nenásobí po složkách.) Invariantem je např. vlastnost „$\forall x \exists y\ y \cdot y = x$“, která říká, že pro každý prvek existuje jeho druhá odmocnina. Algebra $(\mathbb{C}, \cdot)$ tuto vlastnost má, zatímco v algebře $(\mathbb{R}, \cdot) \times (\mathbb{R}, \cdot)$ jsou prvky, které odmocnit nelze, např. $(-1, -1)$. Zbývá dokázat, že to je skutečně invariant. Mějme tedy algebru $\mathbf{A}$ s touto vlastností a izomorfismus $\varphi : \mathbf{A} \to \mathbf{B}$. Zvolme prvek $a \in B$. Jak najít prvek $b \in B$ splňující $b \cdot b = a$? Protože je $\varphi$ bijekce, existuje $x \in A$ takové, že $\varphi(x) = a$. K němu existuje $y \in A$ s vlastností $y \cdot y = x$, položme tedy $b = \varphi(y)$. Pak $a = \varphi(x) = \varphi(y \cdot y) = \varphi(y) \cdot \varphi(y) = b \cdot b$.

**Příklad.** Algebry

$$(\mathbb{N}, +) \quad \text{a} \quad (\mathbb{R}, +)$$

nejsou izomorfní hned z několika důvodů. Předně, nejsou stejně velké. Dále $(\mathbb{N}, +) = \langle 1 \rangle$, kdežto algebru $(\mathbb{R}, +)$ nelze nagenerovat jedním prvkem. Kromě toho v $(\mathbb{R}, +)$ existuje nulový prvek (invariant „$\exists x \forall y\ y + x = y$“), v $\mathbb{N}$ nikoliv. (Dokažte sami, že jsou uvedené vlastnosti invariantem!)

## 12. * Algebry v obecném jazyce

**Cíl.** *V některých aplikacích (zejména v informatice) se hodí zavést algebry obecného typu, bez omezení na aritu operací. V této sekci uvádíme obecné definice pojmů z předchozí sekce.*

Zopakujme, že *typem algebry* rozumíme zobrazení $\tau : \Omega \to \mathbb{N} \cup \{0\}$ a že *algebra typu* $\tau$ je dvojice $\mathbf{A} = (A, F)$, kde $A$ je neprázdná množina a $F$ je zobrazení z množiny $\Omega$ do množiny všech operací na $A$ přiřazující symbolu $\omega$ nějakou $\tau(\omega)$-ární operaci $F_\omega$ na $A$. Výsledek operace $F_\omega$ na prvcích $a_1, \ldots, a_{\tau(\omega)}$ zapisujeme jako $F_\omega(a_1, \ldots, a_{\tau(\omega)})$.

**Definice.** Řekneme, že podmnožina $B \subseteq A$ je *uzavřena* na $n$-ární operaci $f$, pokud pro každé $a_1, \ldots, a_n \in B$ platí $f(a_1, \ldots, a_n) \in B$. Algebra $\mathbf{B}$ se nazývá *podalgebrou* algebry $\mathbf{A}$, pokud je množina $B \subseteq A$ je uzavřena na všechny operace algebry $\mathbf{A}$ a operace algebry $\mathbf{B}$ jsou restrikcemi operací algebry $\mathbf{A}$ na množinu $B$.

I v obecném případě je průnik uzavřených podmnožin a sjednocení řetězce uzavřených podmnožin uzavřená podmnožina a uzavřené podmnožiny algebry $\mathbf{A}$ také tvoří úplný svaz $\mathbf{Sub}(\mathbf{A})$. Stejně jako v předchozí sekci se definuje podalgebra generovaná danou podmnožinou a dokáže se její existence.

**Definice.** *Kartézský součin* množin $A_i$, $i \in I$, je množina

$$\prod_{i \in I} A_i = \{f : I \to \bigcup_{i \in I} A_i : f(i) \in A_i \text{ pro všechna } i\}.$$

Je-li $I = \{1, \ldots, n\}$, zapisujeme zobrazení $f$ zpravidla jako vektor $(a_i = f(i))$, tj.

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) : a_i \in A_i \text{ pro všechna } i\}.$$

**Definice.** *Direktní součin* algeber $\mathbf{A}_i = (A_i, F_i)$, $i \in I$, stejného typu, je algebra

$$\prod_{i \in I} \mathbf{A}_i = (\prod_{i \in I} A_i, F),$$

kde operace $F_\omega$ je definována předpisem

$$F_\omega(f_1, \ldots, f_{\tau(\omega)}) : i \mapsto (F_i)_\omega(f_1(i), \ldots, f_{\tau(\omega)}(i))$$

pro každé $\omega \in \Omega$ a $f_1, \ldots, f_{\tau(\omega)} \in \prod_{i \in I} A_i$. Tedy je-li $I = \{1, \ldots, n\}$ a užijeme-li „vektorové značení“, operace se provádějí po složkách.

**Definice.** Buď $\mathbf{A} = (A, F)$ a $\mathbf{B} = (B, G)$ algebry stejného typu. Zobrazení $\varphi : A \to B$ se nazývá *homomorfismus* algeber $\mathbf{A}$, $\mathbf{B}$, pokud

$$\varphi(F_\omega(a_1, \ldots, a_{\tau(\omega)})) = G_\omega(\varphi(a_1), \ldots, \varphi(a_{\tau(\omega)}))$$

pro každé $\omega \in \Omega$ a $a_1, \ldots, a_{\tau(\omega)} \in A$.

Stejně jako v předchozí sekci se zavedou pojmy mono-, epi-, izo-, endo- a automorfismu, jádro a obraz a analogicky se dokáže tvrzení o skládání a invertování homomorfismu. Všechna pozorování o izomorfních algebrách lze příslušně zobecnit.

# Grupy

## 13. Základní vlastnosti

**Cíl.** *Zavedeme pojem grupy a uvedeme řadu příkladů. Pro grupy adaptujeme pojmy z předchozí kapitoly (podgrupy, generátory, homomorfismy atd.) a na závěr dokážeme dvě věty o reprezentaci: každou grupu lze (až na izomorfismus) považovat za grupu permutací a každou konečnou grupu za grupu regulárních matic.*

### 13.1. **Abelovské grupy.**

Přemýšleli jste někdy o „vektorovém prostoru nad $\mathbb{Z}$“? Tak tomu se říká abelovská grupa. Jde o poměrně užitečnou strukturu: např. řadu v praxi používaných kryptosystémů lze interpretovat jako počítání v jistých konečných abelovských grupách. Teorie abelovských grup také pomáhá vyjasnit řadu věcí v teorii čísel.

**Definice.** *Abelovskou grupou* nazýváme algebru $\mathbf{A} = (A, *, ', e)$ typu $(2, 1, 0)$ splňující pro každé $a, b, c \in A$

(1) $a * (b * c) = (a * b) * c$,
(2) $a * b = b * a$,
(3) $a * e = a$,
(4) $a * a' = e$.

Prvku $e$ se říká *jednotka*, prvku $a'$ *inverzní prvek* k $a$.

V konkrétních příkladech bývá typickou trojicí operací $+, -, 0$, pak hovoříme o *aditivním zápise* (a místo $x + (-y)$ píšeme $x - y$); resp. trojice $\cdot, ^{-1}, 1$, tzv. *multiplikativní zápis*.

**Příklad.**

- (Aditivní) grupa celých čísel
$$\mathbb{Z} = (\mathbb{Z}, +, -, 0).$$
- *Cyklické grupy*
$$\mathbb{Z}_n = (\{0, 1, \dots, n-1\}, +_{\bmod n}, -_{\bmod n}, 0)$$
s operacemi $+, -$ modulo $n$.
- Pro libovolné těleso $\mathbf{T}$ lze uvažovat
  - *aditivní grupu* $(T, +, -, 0)$ a
  - *multiplikativní grupu* $\mathbf{T}^* = (T \setminus \{0\}, \cdot, ^{-1}, 1)$.

  (Připomeňme tělesa $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ a pro kryptografii zvláště užitečná konečná tělesa.)
- Obecněji, *grupa invertibilních prvků* $\mathbf{R}^*$ daného komutativního okruhu s jednotkou $\mathbf{R}$. Pro nás budou nejdůležitější grupy $\mathbb{Z}_n^*$. (Viz níže.)

- Grupa komplexních jednotek $(\{z \in \mathbb{C} : |z| = 1\}, \cdot, ^{-1}, 1)$ a její podgrupy. Mezi nimi jmenujme např. grupy $\mathbb{C}_n$ sestávající ze všech kořenů polynomu $x^n - 1$ a tzv. *Prüferovu p-grupu* $\mathbb{C}_{p^\infty} = \bigcup_{k=1}^{\infty} \mathbb{C}_{p^k}$ sestávající ze všech komplexních čísel $z$ splňujících $z^{p^k} = 1$ pro nějaké $k$.
- Existuje řada geometrických i algebraických konstrukcí abelovských grup, z nichž některé mají významné aplikace v kryptografii (viz Diffie-Hellmanův protokol, který budeme diskutovat později). Mezi nejdůležitější patří konstrukce pomocí eliptických křivek a pomocí kvadratických rozšíření těles.

**Poznámka.** Přestože existuje řada nejrůznějších konstrukcí konečných abelovských grup, ve skutečnosti jich je, *až na izomorfismus*, poměrně málo: Věta 15.1 říká, že každá konečná abelovská grupa je izomorfní direktnímu součinu cyklických grup

$$\mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_n^{k_n}},$$

kde $p_1^{k_1}, \ldots, p_n^{k_n}$ jsou nějaké mocniny prvočísel. Problém je v tom, že nalézt uvedený izomorfismus může být velmi těžké. (Nekonečných abelovských grup je spousta.)

**Tvrzení 13.1.** *Označme $R^*$ množinu všech invertibilních prvků daného komutativního okruhu s jednotkou $\mathbf{R}$. Pak $\mathbf{R}^* = (R^*, \cdot, ^{-1}, 1)$ je abelovská grupa.*

*Důkaz.* Předně ujasněme, co rozumíme operací $^{-1}$: je-li $a$ invertibilní, existuje (právě jeden) prvek $b$ splňující $a \cdot b = 1$. Definujeme $a^{-1} = b$.

Množina $R^*$ je uzavřena na všechny operace, neboť 1 je invertibilní a jsou-li $a, b$ invertibilní, pak $(a \cdot b) \cdot (a^{-1} \cdot b^{-1}) = (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) = 1$, tedy $a \cdot b$ je invertibilní také. Axiomy grup jsou splněny přímo z definice komutativního okruhu. □

**Příklad.**

- V oboru $\mathbb{Z}$ jsou invertibilní pouze prvky $\pm 1$. Tedy $\mathbb{Z}^*$ je dvouprvková grupa.
- V oboru $\mathbb{Z}[i]$ jsou invertibilní pouze prvky $\pm 1, \pm i$. Tedy $\mathbb{Z}[i]^*$ je čtyřprvková grupa a není těžké nahlédnout, že $\mathbb{Z}[i]^* \simeq \mathbb{Z}_4$.
- V oboru $\mathbf{R}[x]$ jsou invertibilní právě polynomy stupně 0, jejichž člen je invertibilní v oboru $\mathbf{R}$. Tedy $\mathbf{R}[x]^* = \mathbf{R}^*$.

**Příklad.** Prvky grupy $\mathbb{Z}_n^*$ jsou právě všechna čísla $a \in \{1, \ldots, n-1\}$ nesoudělná s $n$. (Připomeňme, že operací je násobení modulo $n$). Soudělná čísla zřejmě invertibilní být nemohou: je-li $d = \mathrm{NSD}(a, n)$, pak $d \mid ab \bmod n$ pro libovolné $b$, výsledek tedy nemůže být 1. Naopak, jsou-li $a, n$ nesoudělná, jsou dva způsoby, jak nalézt inverzní prvek:

- pomocí *Eulerovy věty*: protože $a^{\varphi(n)} \equiv 1 \pmod{n}$, inverzní prvek k $a$ je

$$a^{\varphi(n)-1} \bmod n.$$

- pomocí *Eukleidova algoritmu*: spočteme Bézoutovy koeficienty $u, v$ splňující $1 = \mathrm{NSD}(a, n) = ua + vn$, a protože $ua \equiv 1 \pmod{n}$, inverzní prvek k $a$ je

$$u \bmod n.$$

A jak to je se slíbenou analogií „vektorového prostoru nad $\mathbb{Z}$“? Všimněte si, že vektorový prostor se definuje jako abelovská grupa, na které je zavedeno skalární

násobení splňující jisté axiomy. Definujme tedy pro každé $a \in A$ a $n \in \mathbb{Z}$

$$n \times a = \begin{cases} e & n = 0 \\ \underbrace{a * a * \cdots * a}_{n} & n > 0 \\ \underbrace{a' * a' * \cdots * a'}_{-n} & n < 0 \end{cases}$$

Tedy v aditivním zápise máme $n \times a = a + \ldots + a = na$ a v multiplikativním $n \times a = a \cdot \ldots \cdot a = a^n$. Za pomoci Tvrzení 13.2 je celkem snadným (i když trochu pracným) cvičením ověřit, že pro všechna $a, b \in A$ a $m, n \in \mathbb{Z}$ je

$$(m+n) \times a = (m \times a) * (n \times a), \qquad (m \cdot n) \times a = m \times (n \times a),$$
$$m \times (a * b) = (m \times a) * (m \times b), \qquad (-m) \times a = (m \times a)',$$

tj. že jsou splněny všechny axiomy vektorových prostorů až na to, že $\mathbb{Z}$ není těleso. Odborně se takovým algebrám říká $\mathbb{Z}$-*moduly*. (Viz též Sekce 20.)

13.2. **Obecné grupy.**

Motivací pro vznik teorie obecných (nekomutativních) grup bylo studium transformací dané množiny, a to jak diskrétních (permutace na konečné množině), tak např. geometrických (akce regulárních matic na vektorech). Teorie obecných grup se ubírá dost jiným směrem než teorie grup abelovských, avšak úplné základy v rozsahu úvodní sekce mají společné. Abychom ušetřili čas a síly, začneme budovat obě teorie společně. Další dvě sekce se pak budou týkat téměř výhradně grup abelovských, zatímco zbytek kapitoly bude převážně o grupách obecných.

**Definice.** *Grupou* nazýváme algebru $\mathbf{G} = (G, *, ', e)$ typu $(2, 1, 0)$ splňující pro každé $a, b, c \in G$

(1) $a * (b * c) = (a * b) * c$,
(2) $a * e = e * a = a$,
(3) $a * a' = a' * a = e$.

Prvku $e$ se říká *jednotka*, prvku $a'$ *inverzní prvek* k $a$.

Tedy abelovské grupy jsou takové grupy, jejichž binární operace je komutativní. Poznamenejme, že algebry $(G, *)$ splňující podmínku (1) se nazývají *pologrupy* a algebry $(G, *, e)$ splňující podmínky (1) a (2) se nazývají *monoidy*.

Stejně jako v abelovských grupách se obvykle používá aditivní a zejména multiplikativní zápis (i my tak budeme činit v dalších sekcích).

**Příklad.**

- *Symetrická grupa*

$$\mathbf{S}_X = (\{\pi : \pi \text{ je permutace na množině } X\}, \circ, ^{-1}, id),$$

kde $\circ$ značí skládání permutací, $^{-1}$ invertování permutací a $id$ identitu (tj. zobrazení $x \mapsto x$). Je-li $X = \{1, \ldots, n\}$, pak místo $\mathbf{S}_X$ píšeme $\mathbf{S}_n$. Mezi jejími podgrupami zmiňme např.
  - *alternující grupu* $\mathbf{A}_n$ všech sudých permutací;
  - *dihedrální grupu* $\mathbf{D}_{2n}$ všech symetrií pravidelného $n$-úhelníka;
  - nejrůznější grupy symetrií geometrických těles, automorfismů grafů a dalších struktur, ...

- *Obecná lineární grupa*

$$\mathbf{GL}_n(\mathbf{T}) = (\{A : A \text{ je regulární matice } n \times n \text{ nad tělesem } \mathbf{T}\}, \cdot, ^{-1}, E),$$

kde $\cdot$ značí maticové násobení, $^{-1}$ invertování (regulárních) matic a $E$ jednotkovou matici. Mezi jejími podgrupami zmiňme např.
  - *speciální lineární grupu* $\mathbf{SL}_n(\mathbf{T})$ všech matic s determinantem 1;
  - *ortogonální grupu* $\mathbf{O}_n(\mathbf{T})$ všech ortogonálních matic, tj. takových $A$, co splňují $AA^T = E$. (Nad tělesem $\mathbb{R}$ to odpovídá maticím, jejichž řádky, resp. sloupce, jsou ortonormální vektory vzhledem k standardnímu skalárnímu součinu.)
- *Kvaternionová grupa* $\mathbf{Q}$ na množině $\{\pm 1, \pm i, \pm j, \pm k\}$ s násobením daným předpisy

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ik = -ki = -j, \quad jk = -kj = i.$$

Jde o rozšíření grupy $\{\pm 1, \pm i\} \leq \mathbb{C}^*$ a rozšířit lze i samo těleso komplexních čísel na tzv. *kvaterniony*, což jsou „čísla“ tvaru $a+bi+cj+dk$, $a, b, c, d \in \mathbb{R}$. Kvaterniony tvoří nekomutativní těleso.

Symetrické a lineární grupy jsou v jistém smyslu charakteristické příklady, neboť každou grupu lze vnořit do nějaké symetrické grupy (*Cayleyova reprezentace*) a každou konečnou grupu lze vnořit do nějaké obecné lineární grupy nad libovolným tělesem (*lineární reprezentace*) — viz Věty 13.7 a 13.8.

**Příklad.** Oblíbenou kratochvílí je hledání malých grup. Následující tabulka obsahuje seznam všech (až na izomorfismus) nejvýše 11-prvkových grup a několik obecných výsledků; zde $p$ značí libovolné prvočíslo. (Tj. každá grupa s $n$ prvky je izomorfní právě jedné z grup uvedených v pravém sloupci.)

| $n$ | grupy s $n$ prvky |
|---|---|
| 1 | $\mathbb{Z}_1$ |
| 2 | $\mathbb{Z}_2$ |
| 3 | $\mathbb{Z}_3$ |
| 4 | $\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$ |
| 5 | $\mathbb{Z}_5$ |
| 6 | $\mathbb{Z}_6,\ \mathbf{S}_3 = \mathbf{D}_6$ |
| 7 | $\mathbb{Z}_7$ |
| 8 | $\mathbb{Z}_8,\ \mathbb{Z}_2 \times \mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathbf{D}_8,\ \mathbf{Q}$ |
| | $\dots$ |
| $p$ | $\mathbb{Z}_p$ |
| $p^2$ | $\mathbb{Z}_{p^2},\ \mathbb{Z}_p \times \mathbb{Z}_p$ |
| $2p$ | $\mathbb{Z}_{2p},\ \mathbf{D}_{2p}$ |

V současné době je znám seznam všech grup až do velikosti 2047.

Podobně jako u oborů integrity se do definice grupy nevešla řada elementárních vlastností:

**Tvrzení 13.2.** *Buď* $\mathbf{G} = (G, *, ', e)$ *grupa a* $a, b, c \in G$. *Pak*

(1) *jestliže* $a * c = b * c$ *nebo* $c * a = c * b$, *pak* $a = b$ (krácení);
(2) *jestliže* $a * u = a$ *nebo* $u * a = a$ *pro nějaké* $u \in A$, *pak* $u = e$ (jednoznačnost jednotky);

(3) *jestliže* $a*u = e$ *nebo* $u*a = e$ *pro nějaké* $u \in A$, *pak* $u = a'$ (jednoznačnost inverzních prvků)*;*
(4) $(a')' = a$*;*
(5) $(a * b)' = b' * a'$.

*Důkaz.* (1) Je-li $a * c = b * c$, pak také $(a * c) * c' = (b * c) * c'$ a použitím všech tří axiomů dostaneme $(a * c) * c' = a * (c * c') = a * e = a$ a podobně $(b * c) * c' = b$. Tedy $a = b$. Analogicky pro $c * a = c * b$.

(2) Je-li $a * u = a = a * e$, krácením dostáváme $u = e$. Analogicky pro $u * a = a$.

(3) Je-li $a * u = e = a * a'$, krácením dostáváme $u = a'$. Analogicky pro $u * a = e$.

(4) Protože $a' * a = e$, z jednoznačnosti inverzů dostáváme $a = (a')'$.

(5) Protože $(a*b)*(b'*a') = a*(b*b')*a' = a*e*a' = a*a' = e$, z jednoznačnosti inverzů dostáváme $(a * b)' = b' * a'$. □

Stejně jako pro abelovské grupy zavedeme značení $n \times a$ pro $a * a * \cdots * a$, resp. $a' * a' * \cdots * a'$. Pomocí vlastností (4),(5) lze ověřit, že pro všechna $a, b$ a $m, n \in \mathbb{Z}$

$$(m + n) \times a = (m \times a) * (n \times a), \qquad (m \cdot n) \times a = m \times (n \times a),$$
$$m \times (a * b) = (m \times a) * (m \times b), \qquad (-m) \times a = (m \times a)'.$$

13.3. **Podgrupy, direktní součiny, homomorfismy.**
Místo podalgeber grupy $\mathbf{G} = (G, *, ', e)$ mluvíme o *podgrupách*. Tedy podmnožina $H \subseteq G$ tvoří podgrupu grupy $\mathbf{G}$, pokud je uzavřena na všechny operace, tj. pokud $e \in H$, $a' \in H$ a $a * b \in H$ pro každé $a, b \in H$. Píšeme $\mathbf{H} \leq \mathbf{G}$. Podgrupy $\mathbf{G}$ a $\{e\}$ nazýváme *nevlastní*. Je zřejmé, že podgrupy splňují všechny axiomy grup a jsou to tedy také grupy.

Zopakujme, že nejmenší podgrupa grupy $\mathbf{G}$ obsahující danou množinu $X \subseteq G$ se nazývá *podgrupa generovaná množinou* $X$ a značí se $\langle X \rangle_{\mathbf{G}}$.

**Tvrzení 13.3.** *Buď* $\mathbf{G} = (G, *, ', e)$ *grupa a* $\emptyset \neq X \subseteq G$. *Pak*

$$\langle X \rangle_{\mathbf{G}} = \{(k_1 \times x_1) * (k_2 \times x_2) * \ldots * (k_n \times x_n) : n \in \mathbb{N}, x_1, \ldots, x_n \in X,\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

Tedy v aditivním zápise by bylo

$$\langle X \rangle_{\mathbf{G}} = \{k_1 x_1 + k_2 x_2 + \ldots + k_n x_n : n \in \mathbb{N}, x_1, \ldots, x_n \in X,\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

a v multiplikativním zápise

$$\langle X \rangle_{\mathbf{G}} = \{x_1^{k_1} \cdot x_2^{k_2} \cdot \ldots \cdot x_n^{k_n} : n \in \mathbb{N}, x_1, \ldots, x_n \in X,\ k_1, \ldots, k_n \in \mathbb{Z}\}.$$

*Důkaz.* Označme $M = \{k_1 x_1 + k_2 x_2 + \ldots + k_n x_n : x_1, \ldots, x_n \in X,\ k_1, \ldots, k_n \in \mathbb{Z}\}$. Předně je třeba si uvědomit, že libovolný prvek množiny $M$ lze nagenerovat z množiny $X$: protože $x_i \in X$, máme také $x_i' \in \langle X \rangle$, tudíž také $k_i \times x_i \in \langle X \rangle$, a tedy i výsledek operace $*$ na těchto prvcích náleží $\langle X \rangle$.

Zbývá ověřit, že množina $M$ tvoří podgrupu. Uzavřenost na $*$ je zřejmá, výsledek operace na dva prvky uvedeného tvaru je opět prvek uvedeného tvaru (pro větší $n$). Z Tvrzení 13.2 plyne, že $((k_1 \times x_1) * \ldots * (k_n \times x_n))' = (-k_1 \times x_1) * \ldots * (-k_n \times x_n)$, a konstanta $e$ lze vyjádřit jako $0 \times x$. □

**Příklad.**

- $\langle a, b \rangle_{\mathbb{Z}} = \{ua + vb : u, v \in \mathbb{Z}\} = \langle \mathrm{NSD}(a, b) \rangle_{\mathbb{Z}}$ díky Bézoutově rovnosti.
- $\langle 2, i \rangle_{\mathbb{C}} = \{2u + vi : u, v \in \mathbb{Z}\}$.
- $\langle 2, i \rangle_{\mathbb{C}^*} = \{2^u \cdot i^v : u, v \in \mathbb{Z}\} = \{\pm 2^u, \pm i 2^u : u \in \mathbb{Z}\}$.

Buď $\mathbf{G} = (G, *, ', e)$ a $\mathbf{H} = (H, \cdot, ^{-1}, 1)$ dvě grupy. Zobrazení $\varphi : G \to H$ je *homomorfismus* těchto grup, pokud pro každé $a, b \in G$ platí

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b), \quad \varphi(a') = \varphi(a)^{-1} \quad \text{a} \quad \varphi(e) = 1.$$

Pojmy *monomorfismus* (neboli *vnoření*), *epimorfismus*, *izomorfismus*, *endomorfismus* a *automorfismus* se používají stejně jako pro obecné algebry. Definujeme

- *jádro* homomorfismu $\varphi$ předpisem

$$\mathrm{Ker}(\varphi) = \{a \in G : \varphi(a) = 1\};$$

- *obraz* homomorfismu $\varphi$ předpisem

$$\mathrm{Im}(\varphi) = \{b \in H : b = \varphi(a) \text{ pro nějaké } a \in G\}.$$

Tedy jádro je blok $[e]$ ekvivalence $\ker(\varphi)$, definice obrazu se shoduje s definicí pro obecné algebry.

**Tvrzení 13.4.** *Buď* $\mathbf{G} = (G, *, ', e)$ *a* $\mathbf{H} = (H, \cdot, ^{-1}, 1)$ *grupy a* $\varphi : G \to H$ *zobrazení.*

(1) *Pokud platí pro všechna* $a, b \in G$

$$\varphi(a * b) = \varphi(a) \cdot \varphi(b),$$

*pak je* $\varphi$ *homomorfismus těchto grup.*

(2) *Je-li* $\varphi$ *homomorfismus, pak* $\mathrm{Ker}(\varphi)$ *tvoří podrupu* $\mathbf{G}$ *a* $\mathrm{Im}(\varphi)$ *podgrupu* $\mathbf{H}$.

(3) *Homomorfismus* $\varphi$ *je prostý právě tehdy, když je* $\mathrm{Ker}(\varphi) = \{e\}$.

*Důkaz.* (1) Nejprve dokážeme, že $\varphi(e) = 1$. Protože $\varphi(e) = \varphi(e * e) = \varphi(e) \cdot \varphi(e)$, z jednoznačnosti jednotky v grupě $\mathbf{H}$ plyne $\varphi(e) = 1$. A dále dokážeme, že $\varphi(a') = \varphi(a)^{-1}$ pro každé $a \in G$. Protože $1 = \varphi(e) = \varphi(a * a') = \varphi(a) \cdot \varphi(a')$, z jednoznačnosti inverzů v grupě $\mathbf{H}$ plyne $\varphi(a') = \varphi(a)^{-1}$.

(2) Je-li $\varphi(a) = \varphi(b) = 1$, pak $\varphi(a * b) = \varphi(a) \cdot \varphi(b) = 1 \cdot 1 = 1$ a $\varphi(a') = \varphi(a)^{-1} = 1^{-1} = 1$. Navíc $\varphi(e) = 1$, takže $\mathrm{Ker}(\varphi)$ je uzavřeno na všechny operace grupy $\mathbf{G}$. Pro obraz stačí použít obecné Tvrzení 11.5.

(3) Je-li $\varphi$ prosté, pak se dva různé prvky nemohou zobrazovat na 1, takže $\mathrm{Ker}(\varphi)$ musí obsahovat jen prvek $e$. Naopak, není-li $\varphi$ prosté, tedy $\varphi(a) = \varphi(b)$ pro nějaká $a \neq b$, a tedy $1 = \varphi(a) \cdot \varphi(b)^{-1} = \varphi(a * b')$, takže máme $e \neq a * b' \in \mathrm{Ker}(\varphi)$. □

*Direktní součin* grup definujeme stejně jako pro obecné algebry, tj. nosnou množinou je kartézský součin nosných množin jednotlivých grup a operace provádíme po složkách. Pojem ilustrujeme na algebraické verzi Čínské věty o zbytcích.

**Tvrzení 13.5.** *Buď* $m_1, \ldots, m_n$ *po dvou nesoudělná přirozená čísla, označme* $M = m_1 \cdot \ldots \cdot m_n$. *Pak*

$$\mathbb{Z}_M \simeq \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n}.$$

*Důkaz.* Uvažujme zobrazení

$$\begin{aligned} \varphi : \mathbb{Z}_M &\to \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n} \\ x &\mapsto (x \bmod m_1, \ldots, x \bmod m_n). \end{aligned}$$

Podle Čínské věty o zbytcích 2.13 je toto zobrazení bijektivní. Zbývá dokázat, že to je homomorfismus:

$$\begin{aligned}\varphi(x)+\varphi(y) &= (x \bmod m_1,\dots,x \bmod m_n)+(y \bmod m_1,\dots,y \bmod m_n)\\ &= ((x+y) \bmod m_1,\dots,(x+y) \bmod m_n) = \varphi(x+y \bmod M)\end{aligned}$$

pro libovolná $x, y \in \mathbb{Z}_M$. Tedy podle Tvrzení 13.4 je $\varphi$ homomorfismus. □

**Poznámka.** Pro soudělná $m, n$ grupy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ izomorfní nejsou, např. proto, že první z nich obsahuje prvek řádu $mn$, zatímco druhá má všechny prvky řádu nejvýše $\mathrm{NSN}(m,n)$. (O řádech prvků jako invariantech později.)

13.4. **Reprezentace grup.**

**Definice.** Je-li $*$ binární operace na množině $A$ a $a \in A$, definujeme zobrazení

$$L_a : A \to A, \quad x \mapsto a * x \quad \text{a} \quad R_a : A \to A, \quad x \mapsto x * a.$$

Nazývají se *levá* a *pravá translace* prvku $a$.

Např. uvažujeme-li grupu $\mathbb{R} \times \mathbb{R}$, translace $L_{(a,b)}$ je jednoduše posunutí v rovině o vektor $(a, b)$.

**Tvrzení 13.6.**

(1) *Je-li* $\mathbf{G} = (G, *, ', e)$ *grupa, pak všechny levé i pravé translace jsou permutace na množině* $G$.
(2) *Je-li* $\mathbf{G} = (G, *, e)$ *monoid a jsou-li všechny levé i pravé translace permutace, pak existuje unární operace* $'$ *taková, že* $(G, *, ', e)$ *je grupa.*

*Důkaz.* (1) Prostost ihned plyne z krácení. Řešením rovnice $L_a(x) = b$ je pro libovolné $a, b$ prvek $x = a' * b$, řešením rovnice $R_a(x) = b$ je prvek $x = b * a'$.

(2) Definujme $a' = (L_a)^{-1}(e)$. Pak $a * a' = L_a(a') = L_a(L_a^{-1}(e)) = e$ a zbývá dokázat, že $a' * a = e$. Protože $a * a' = e$, platí $(a' * a) * a' = a' * (a * a') = a' * e = a' = e * a'$, tedy $R_{a'}(a' * a) = R_{a'}(e)$, a protože je $R_{a'}$ prosté zobrazení, dostaneme $a' * a = e$. □

V úvodu kapitoly jsme zmínili, že dvěma základními příklady grup jsou grupy permutací a grupy regulárních matic. To proto, že *každou* grupu lze reprezentovat jako grupu permutací a *každou konečnou* grupu jako grupu matic. Reprezentací v tomto případě rozumíme, že daná grupa je, až na izomorfismus, podgrupou symetrické, resp. lineární grupy.

**Věta 13.7** (Cayleyova reprezentace)**.** *Každá grupa je izomorfní nějaké podgrupě nějaké symetrické grupy.*

*Důkaz.* Buď $\mathbf{G} = (G, *, ', e)$ grupa. Najdeme-li vnoření $\lambda$ grupy $\mathbf{G}$ do grupy $\mathbf{S}_X$ pro nějaké $X$, získáme hledanou podgrupu jako $\mathrm{Im}(\lambda)$. Uvažujme tedy zobrazení

$$\lambda : \mathbf{G} \to \mathbf{S}_G, \quad a \mapsto L_a.$$

Podle Tvrzení 13.6 jsou zobrazení $L_a$ permutace na množině $G$. Zbývá dokázat, že je $\lambda$ prostý homomorfismus. Nejprve prostost: jestliže pro nějaká $a, b \in G$ platí $L_a = L_b$, pak $a = L_a(e) = L_b(e) = b$, tedy $a = b$. Podle Tvrzení 13.4 stačí ověřit, že $\lambda(a * b) = \lambda(a) \circ \lambda(b)$, tj. že zobrazení $L_{a*b}$ je totožné se zobrazením $L_a \circ L_b$. Dosadíme-li $x \in G$, dostaneme

$$L_{a*b}(x) = (a * b) * x = a * (b * x) = L_a(b * x) = L_a(L_b(x)),$$

a tedy skutečně $L_{a*b} = L_a \circ L_b$. □

**Věta 13.8** (Lineární reprezentace)**.** *Každá* konečná *grupa je izomorfní nějaké podgrupě nějaké obecné lineární grupy (nad libovolným tělesem).*

*Důkaz.* Buď $\mathbf{T}$ libovolné těleso, $\mathbf{G}$ daná konečná grupa a označme $n = |G|$. Bez újmy na obecnosti předpokládejme, že nosná množina $G$ sestává z čísel $1, \dots, n$ (přejmenování prvků odpovídá izomorfismu). Protože máme k dispozici Cayleovu reprezentaci $\lambda : \mathbf{G} \to \mathbf{S}_n$, stačí nalézt vnoření $\psi$ grupy $\mathbf{S}_n$ do $\mathbf{GL}_n(\mathbf{T})$. Hledanou podgrupu pak získáme jako $\mathrm{Im}(\psi \circ \lambda)$. Uvažujme

$$\psi : \mathbf{S}_n \to \mathbf{GL}_n(\mathbf{T}), \quad \sigma \mapsto \big(\delta_{i,\sigma(j)}\big)_{i,j=1}^{n},$$

kde $\delta_{u,v} = 1$ pokud $u = v$ a $\delta_{u,v} = 0$ v opačném případě. Tedy $\psi(\sigma)$ je matice, ve které je v každém řádku a každém sloupci právě jedna jednička a jinak samé nuly, přičemž ta jednička na $i$-tém řádku je v $\sigma^{-1}(i)$-tém sloupci. Evidentně jde o prosté zobrazení, zbývá tedy dokázat, že to je homomorfismus, tedy že platí

$$\psi(\pi \circ \sigma) = \psi(\pi) \cdot \psi(\sigma)$$

pro všechny permutace $\pi, \sigma \in S_n$. Pravá strana je rovna

$$\big(\delta_{i,\pi(j)}\big)_1^n \cdot \big(\delta_{i,\sigma(j)}\big)_1^n = \big(\sum_k \delta_{i,\pi(k)} \cdot \delta_{k,\sigma(j)}\big)_1^n.$$

Přitom $\delta_{i,\pi(k)} \cdot \delta_{k,\sigma(j)} = 1$ právě tehdy, když $i = \pi(k)$ a $k = \sigma(j)$, což je právě tehdy, když $i = \pi(\sigma(j))$ a $k = \sigma(j)$. Tedy celá suma je rovna jedné pro $i = \pi(\sigma(j))$ a nule v opačném případě. Tím pádem je to přesně matice $\psi(\pi \circ \sigma)$. □

Poznamenejme, že matice $\psi(\sigma)$ jsou ortogonální, tedy každou konečnou grupu lze vnořit dokonce do grupy $\mathbf{O}_n(\mathbf{T})$.

## 14. Cyklické grupy

**Cíl.** *Budeme se důkladně věnovat grupám, které jsou generované jedním prvkem. Podíváme se na jejich strukturu, k čemuž nám vydatně pomůže jejich klasifikace: každá cyklická grupa je izomorfní buď s grupou $\mathbb{Z}$, nebo s některou grupou $\mathbb{Z}_n$. Dokážeme, že cyklické jsou také všechny grupy $\mathbb{Z}_p^*$, $p$ prvočíslo. Uvedená teorie nachází aplikaci v kryptografii, čemuž je věnována poslední část sekce.*

### 14.1. Řád prvku.

**Definice.** *Řádem grupy* $\mathbf{G}$ se rozumí počet prvků její nosné množiny a značí se $|\mathbf{G}|$. Tedy, formálně vzato, $|\mathbf{G}| = |G|$.

**Definice.** *Řádem prvku* $a$ v grupě $\mathbf{G}$ se rozumí počet prvků grupy $\langle a \rangle_{\mathbf{G}}$ a značí se $\mathrm{ord}(a)$. Je-li tato podgrupa nekonečná, rozumí se $\mathrm{ord}(a) = \infty$.

**Tvrzení 14.1.** *Buď* $\mathbf{G} = (G, *, ', e)$ *grupa a* $a \in G$*. Pak* $\mathrm{ord}(a)$ *je rovno nejmenšímu kladnému* $n$ *takovému, že* $n \times a = e$*, pokud takové* $n$ *existuje, resp.* $\infty$ *v opačném případě.*

*Důkaz.* Podle Tvrzení 13.3 je $\langle a\rangle_{\mathbf{G}} = \{k \times a : k \in \mathbb{Z}\}$. Je-li $n \times a = e$ pro nějaké $n > 0$, pak

$$k \times a = (rn + q) \times a = r \times (n \times a) * (q \times a) = (r \times e) * (q \times a) = q \times a,$$

kde $r = k \operatorname{div} n$ a $q = k \bmod n$. Čili $|\langle a\rangle|$ je rovno nejmenšímu $n > 0$, pro které $n \times a = e$, pokud takové existuje. V opačném případě je $\langle a\rangle$ nekonečná. □

**Příklad.**

- V grupě $\mathbb{Z}_6$ je $\operatorname{ord}(0) = 1$, $\operatorname{ord}(1) = 6$, $\operatorname{ord}(2) = 3$, $\operatorname{ord}(3) = 2$, $\operatorname{ord}(4) = 3$ a $\operatorname{ord}(5) = 6$.
- V grupě $\mathbb{Z}_7^*$ je $\operatorname{ord}(1) = 1$, $\operatorname{ord}(2) = 3$, $\operatorname{ord}(3) = 6$, $\operatorname{ord}(4) = 6$, $\operatorname{ord}(5) = 3$ a $\operatorname{ord}(6) = 2$.
- V grupě $\mathbb{Z}$ mají všechny nenulové prvky řád $\infty$.
- V grupě komplexních jednotek existuje prvek libovolného řádu. (Nápověda: uvažujte imaginární kořeny polynomu $x^n - 1$.)

Všimněte si, že v uvedených příkladech řády všech prvků dělí řád celé grupy. To není náhoda.

**Tvrzení 14.2.** *Buď* $\mathbf{G}$ *konečná grupa a* $a \in G$. *Pak* $\operatorname{ord}(a)$ *dělí* $|G|$.

Toto tvrzení je okamžitým důsledkem obecnější Lagrangeovy věty 17.5, kterou dokážeme později; zatím jej budeme používat bez důkazu.

**Poznámka.** Eulerova věta je speciálním případem Tvrzení 14.2: aplikujeme-li jej na grupu $\mathbf{G} = \mathbb{Z}_n^*$, pro každý prvek $a$ této grupy, tj. pro každé $a$ nesoudělné s $n$, dostaneme, že $\operatorname{ord}(a)$ dělí $|\mathbb{Z}_n^*| = \varphi(n)$. Protože $a^{\operatorname{ord}(a)} = 1$, tím spíše bude $a^{\varphi(n)} = 1$ (v $\mathbb{Z}_n^*$, tj. modulo $n$).

Všimněte si, že počet prvků daného řádu je v grupách $\mathbb{Z}_6$ a $\mathbb{Z}_7^*$ stejný. To není náhoda, neboť $\mathbb{Z}_7^* \simeq \mathbb{Z}_6$. Řády prvků jsou asi nejdůležitějším invariantem pro důkazy neizomorfnosti grup.

**Tvrzení 14.3.** *Buď* $\varphi : \mathbf{G} \to \mathbf{H}$ *izomorfismus grup. Pak*

$$\operatorname{ord}(a) = \operatorname{ord}(\varphi(a))$$

*pro každé* $a \in G$.

*Důkaz.* Protože $k \times \varphi(a) = \varphi(k \times a)$ a $\varphi$ je bijekce, platí $k \times a = e$ právě tehdy, když $\varphi(k \times a) = \varphi(e)$, tj. právě tehdy, když $k \times \varphi(a) = 1$. □

Tedy jsou-li dvě grupy izomorfní, pak mají stejný počet prvků každého řádu. Opačná implikace neplatí, ale konečné protipříklady jsou řídké.

**Příklad.**

- Pro $m, n$ soudělná grupy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ nejsou izomorfní, neboť první z nich obsahuje prvek 1 řádu $mn$, zatímco druhá má všechny prvky řádu nejvýše $\operatorname{NSN}(m, n)$. (Srovnejte s Tvrzením 13.5.)
- Grupy $\mathbb{Q}$ a $\mathbb{Q}^*$ nejsou izomorfní, neboť grupa $\mathbb{Q}^*$ obsahuje prvek $-1$ řádu 2, zatímco grupa $\mathbb{Q}$ žádný prvek řádu 2 neobsahuje.
- Grupy $\mathbb{Q}$ a $\mathbb{Q}^+$ nejsou izomorfní, přestože v obou grupách mají všechny prvky kromě jednotky řád nekonečno. Invariantem je např. vlastnost „$\forall y \exists x\ x * x = y$“. (Zde $\mathbb{Q}^+$ uvažujeme jako podgrupu $\mathbb{Q}^*$.)

14.2. **Klasifikace a vlastnosti.**

**Definice.** Grupa $\mathbf{G}$ se nazývá *cyklická*, pokud je generovaná jedním prvkem. Tedy pokud $\mathbf{G} = \langle a \rangle_{\mathbf{G}}$ pro nějaké $a \in G$.

Podle Tvrzení 13.3 je každý prvek cyklické grupy $\mathbf{G} = (G, *, ', e) = \langle a \rangle$ tvaru $k \times a$ pro nějaké $k \in \mathbb{Z}$. Z této vlastnosti vychází i představa cykličnosti: je-li $\mathrm{ord}(a) = n$, pak $\mathbf{G}$ sestává z prvků $0 \times a = e$, $1 \times a$, $2 \times a$, $\ldots$, $(n-1) \times a$, $n \times a = e = 0 \times a$, $(n+1) \times a = 1 \times a$, atd. — seznam se zacyklil. (Pro nekonečný řád si představte přímku jako cyklus nekonečné délky.)

**Příklad.**

- Grupy $\mathbb{Z} = \langle 1 \rangle$ a $\mathbb{Z}_n = \langle 1 \rangle$ pro libovolné přirozené $n$ jsou cyklické.
- Grupy $\mathbb{C}_n$ sestávající ze všech komplexních kořenů polynomu $x^n - 1$ (jako podgrupy $\mathbb{C}^*$) jsou cyklické, $\mathbb{C}_n = \langle e^{2\pi i/n} \rangle$. Prüferova grupa $\mathbb{C}_{p^\infty}$ cyklická není (není ani konečně generovaná), přestože všechny její vlastní podgrupy cyklické jsou.
- Věta 14.9 říká, že grupy $\mathbb{Z}_p^*$ jsou cyklické pro každé prvočíslo $p$. Např. $\mathbb{Z}_5^* = \langle 2 \rangle$, $\mathbb{Z}_7^* = \langle 3 \rangle$, $\mathbb{Z}_{11}^* = \langle 2 \rangle$.
- Některé $\mathbb{Z}_n^*$, $n$ složené, mohou být cyklické: např. $\mathbb{Z}_6^*$ obsahuje pouze prvky 1, 5, tedy $\mathbb{Z}_6^* = \langle 5 \rangle$. Naopak např. $\mathbb{Z}_8^*$ cyklická není, všechny prvky mají řád $\leq 2$.
- Každá grupa $\mathbf{G}$ prvočíselného řádu $p$ je cyklická. Podle Tvrzení 14.2 mají všechny prvky kromě jednotky řád $p$, tj. generují $\mathbf{G}$.

Cílem řady algebraických teorií je tzv. *klasifikace* objektů, tj. úplný seznam všech příkladů *až na izomorfismus*. Jednu takovou větu předvedeme: dokážeme, že každá cyklická grupa je izomorfní některé z grup $\mathbb{Z}$ nebo $\mathbb{Z}_n$, tj. že tyto jsou *až na izomorfismus všechny příklady* cyklických grup.

**Věta 14.4.** *Buď $\mathbf{G}$ cyklická grupa. Je-li $\mathbf{G}$ nekonečná, pak je izomorfní grupě $\mathbb{Z}$. Je-li $\mathbf{G}$ konečná $n$-prvková, pak je izomorfní grupě $\mathbb{Z}_n$.*

*Důkaz.* Nejprve předpokládejme, že je $\mathbf{G} = (G, *, ', e) = \langle a \rangle$ nekonečná a uvažujme zobrazení

$$\mathbb{Z} \to \mathbf{G}, \qquad k \mapsto k \times a.$$

Toto zobrazení je homomorfismus, neboť $(k+l) \times a = (k \times a) * (l \times a)$. Přitom jádro je triviální, neboť řád $a$ je nekonečný, a tedy $k \times a \neq e$ pro každé $k \neq 0$; podle Tvrzení 13.4 tedy jde o prosté zobrazení. Podle Tvrzení 13.3 je toto zobrazení i na.

Nyní předpokládejme, že je $\mathbf{G} = (G, *, ', e) = \langle a \rangle$ konečná $n$-prvková, tj. $\mathrm{ord}(a) = n$, a uvažujme zobrazení

$$\mathbb{Z}_n \to \mathbf{G}, \qquad k \mapsto k \times a.$$

Toto zobrazení je homomorfismus, neboť $(k + l \bmod n) \times a = (k \times a) * (l \times a)$: je-li $k + l < n$, je to splněno triviálně, v opačném případě máme $(k \times a) * (l \times a) = (k+l) \times a = ((k+l-n) \times a) * (n \times a) = ((k+l-n) \times a) * e = (k + l \bmod n) \times a$. Přitom jádro je triviální, neboť $n$ je nejmenší kladné číslo takové, že $n \times a = e$. Je to tedy prosté zobrazení, a protože $|\mathbb{Z}_n| = |\mathbf{G}| = n$, je to podle Lemmatu 1.2 bijekce. □

**Poznámka.** Všimněte si, že pro libovolnou grupu $\mathbf{G}$ a její prvek $a$ je zobrazení

$$\psi_a : \mathbb{Z} \to \mathbf{G}, \qquad k \mapsto k \times a$$

homomorfismem. Přitom $\mathbf{Im}(\psi_a) = \langle a \rangle_{\mathbf{G}}$ a $\mathbf{Ker}(\psi_a) = n\mathbb{Z}$, kde $n = \mathrm{ord}(a)$ v konečném případě a $n = 0$ v případě $\mathrm{ord}(a) = \infty$.

Ve zbytku odstavce se podíváme, jak vypadají podgrupy cyklických grup, jejich generátory, endomorfismy a automorfismy.

**Věta 14.5.** *Každá podgrupa cyklické grupy je cyklická.*

Důkaz je analogický Větě 6.4, srovnejte!

*Důkaz.* Buď $\mathbf{H}$ podgrupa cyklické grupy $\mathbf{G} = (G, *, ', e) = \langle a \rangle$. Je-li $H = \{e\}$, pak $\mathbf{H} = \langle e \rangle$. V opačném případě označme $k$ nejmenší kladné číslo takové, že $k \times a \in H$. Dokážeme, že $\mathbf{H} = \langle k \times a \rangle$. Zřejmě $\langle k \times a \rangle \subseteq H$, pro spor tedy předpokládejme, že existuje nějaký prvek $l \times a \in H \setminus \langle k \times a \rangle$. Označme $q = l \operatorname{div} k$ a $r = l \bmod k$, tj. $l = kq + r$. Samozřejmě $k > r \neq 0$, protože $l \times a \notin \langle k \times a \rangle$. Ovšem

$$r \times a = (l \times a) * (-kq \times a) = \underbrace{(l \times a)}_{\in H} * (-q \times \underbrace{(k \times a)}_{\in H}) \in H,$$

což je spor s výběrem $k$ jako nejmenšího čísla splňujícího $k \times a \in H$. □

**Příklad.**

- Podgrupy grupy $\mathbb{Z}$ jsou právě $a\mathbb{Z} = \langle a \rangle$, $a \in \mathbb{Z}$. Přitom
$$a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = \pm b.$$
Svaz $\mathbf{Sub}(\mathbb{Z})$ je tedy izomorfní se svazem $(\mathbb{N} \cup \{0\}, |^*)$, kde $a \mid^* b \Leftrightarrow b \mid a$; izomorfismem je zobrazení $a \mapsto a\mathbb{Z}$.
(Všimněte si, že podgrupa grupy $\mathbb{Z}$ je totéž co ideál oboru $\mathbb{Z}$, takže charakterizace podgrup je důsledkem toho, že $\mathbb{Z}$ je obor integrity hlavních ideálů.)
- Podgrupy grupy $\mathbb{Z}_n$ jsou právě $a\mathbb{Z}_n = \langle a \rangle$, $a = 0, \ldots, n-1$. Přitom díky Bézoutově rovnosti je $a\mathbb{Z}_n = \langle \mathrm{NSD}(a, n) \rangle$, tedy
$$a\mathbb{Z}_n = b\mathbb{Z}_n \Leftrightarrow \mathrm{NSD}(a, n) = \mathrm{NSD}(b, n).$$
Svaz $\mathbf{Sub}(\mathbb{Z}_n)$ je tedy izomorfní se svazem $(D_n, |^*)$, kde $D_n$ značí množinu všech dělitelů čísla $n$ a $a \mid^* b \Leftrightarrow b \mid a$; izomorfismem je zobrazení $a \mapsto a\mathbb{Z}$.

**Tvrzení 14.6.** *Prvek $a$ generuje grupu $\mathbb{Z}_n$ právě tehdy, když* $\mathrm{NSD}(a, n) = 1$.

*Důkaz.* Jsou-li $a, n$ nesoudělné, pak díky Bézoutově rovnosti existují $u, v \in \mathbb{Z}$ splňující $ua + vn = 1$, a tedy $1 = ua \bmod n = a + a + \ldots + a \bmod n \in \langle a \rangle$. Čili $\langle a \rangle = \langle 1 \rangle = \mathbb{Z}_n$. V opačném případě označme $d = \mathrm{NSD}(a, n)$. Pak pro každé $u \in \mathbb{N}$ je číslo $ua \bmod n$ dělitelné $d$, takže např. $1 \notin \langle a \rangle$. □

Vidíme, že grupa $\mathbb{Z}_n$ obsahuje právě $\varphi(n)$ prvků řádu $n$. Dodefinujme Eulerovu funkci hodnotou $\varphi(1) = 1$.

**Důsledek 14.7.** *$n$-prvková cyklická grupa obsahuje pro každé $k \mid n$ právě $\varphi(k)$ prvků řádu $k$.*

*Důkaz.* Předně je třeba si uvědomit, že díky Větě 14.4 a Tvrzení 14.3 stačí důkaz provést pro grupu $\mathbb{Z}_n$. Prvek řádu $k$ generuje $k$-prvkovou podgrupu. Taková existuje v $\mathbb{Z}_n$ právě jedna (je to $\frac{n}{k}\mathbb{Z}_n$), přičemž podle předchozího tvrzení má právě $\varphi(k)$ generátorů. □

Tuto vlastnost lze překvapivým způsobem aplikovat na řešení následující úlohy z teorie čísel.

**Úloha.** Dokažte, že $\sum_{k|n} \varphi(k) = n$.

*Řešení.* I bez znalosti algebry lze tuto řadu sečíst užitím vzorce z Tvrzení 2.9, je to však velice pracné. Se znalostí výše uvedených vlastností cyklických grup je řešení snadné: uvažujme grupu $\mathbb{Z}_n$. Ta má $n$ prvků, každý z nich má nějaký řád $k \mid n$, přičemž prvků řádů $k$ je $\varphi(k)$. V sumě je tedy započítán každý prvek právě jednou, takže výsledek je roven počtu prvků grupy $\mathbb{Z}_n$, tj. $n$. □

**Tvrzení 14.8.** *Buď* $\mathbf{G} = (G, *, ', e) = \langle a \rangle$ *cyklická grupa.*

(1) *Endomorfismy* $\mathbf{G}$ *jsou právě všechna zobrazení* $x \mapsto k \times x$, $k \in \mathbb{Z}$.
(2) *Automorfismy* $\mathbf{G}$ *jsou právě všechna zobrazení* $x \mapsto k \times x$ *taková, že* $\mathbf{G} = \langle k \times a \rangle$.

*Důkaz.* (1) Nechť $\varphi$ je endomorfismus a buď $k$ takové, že $\varphi(a) = k \times a$. Pak pro dané $x = l \times a$ dostáváme

$$\varphi(x) = \varphi(l \times a) = l \times \varphi(a) = kl \times a = k \times x.$$

Tato zobrazení jsou zřejmě endomorfismy (ne nutně po dvou různé).

(2) Které z endomorfismů $x \mapsto k \times x$ jsou permutace? Protože $\mathrm{Im}(\varphi) = \langle \varphi(a) \rangle$, musí $k \times a$ generovat grupu $\mathbf{G}$. Je-li $\mathbf{G}$ konečná, zobrazení $\varphi$ je pak prosté podle Lemmatu 1.2. Je-li $\mathbf{G}$ nekonečná, pak zřejmě $k = \pm 1$, což také dává bijektivní zobrazení. □

**Poznámka.** Je-li $|G| = n$, pak $\mathbf{G} = \langle k \times a \rangle \Leftrightarrow \mathrm{NSD}(k, n) = 1$. (Dokažte!)

**Příklad.**

- Endomorfismy grupy $\mathbb{Z}$ jsou právě všechna zobrazení $x \mapsto kx$, $k \in \mathbb{Z}$, automorfismy jsou pouze $x \mapsto \pm x$.
- Endomorfismy grupy $\mathbb{Z}_n$ jsou právě všechna zobrazení $x \mapsto kx$, $k = 0, \ldots, n-1$, automorfismy jsou pouze $x \mapsto kx$, kde $\mathrm{NSD}(k, n) = 1$.

## 14.3. * Grupy $\mathbb{Z}_p^*$ jsou cyklické.

Následující věta má dalekosáhlé důsledky v algebře, teorii čísel a zprostředkovaně i v kryptografii.

**Věta 14.9.** *Grupa* $\mathbb{Z}_p^*$ *je cyklická pro každé prvočíslo* $p$.

Jinými slovy,

$$\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}.$$

Větu dokážeme za pomoci několika lemmat a pojmu exponent grupy. Aby byly výpočty názornější, budeme se v celém odstavci držet multiplikativního značení, tj. předpokládáme, že $\mathbf{G} = (G, \cdot, ^{-1}, 1)$.

**Lemma 14.10.** *Buď* $\mathbf{G}$ *grupa,* $a \in G$, $m, n \in \mathbb{Z}$. *Pak*

$$a^m = a^n = 1 \quad \Rightarrow \quad a^{\mathrm{NSD}(m,n)} = 1.$$

*Důkaz.* Bézoutova rovnost dává $u, v \in \mathbb{Z}$ takové, že $\mathrm{NSD}(m, n) = um + vn$. Pak $a^{\mathrm{NSD}(m,n)} = a^{um} \cdot a^{vn} = (a^m)^u \cdot (a^n)^v = 1^u \cdot 1^v = 1$. □

**Lemma 14.11.** *Buď* $\mathbf{G}$ *abelovská grupa a* $a, b \in G$ *prvky takové, že* $\mathrm{ord}(a), \mathrm{ord}(b)$ *jsou nesoudělné. Pak*

$$\mathrm{ord}(ab) = \mathrm{ord}(a) \cdot \mathrm{ord}(b).$$

*Důkaz.* Označme $m = \mathrm{ord}(a)$ a $n = \mathrm{ord}(b)$. Nejprve si všimněte, že $\mathrm{ord}(ab) \leq mn$:

$$(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = 1^n \cdot 1^m = 1.$$

Nyní uvažujme $k$ takové, že $(a \cdot b)^k = a^k \cdot b^k = 1$. Pak $a^k = b^{-k}$, a tak vidíme, že oba prvky $a^k$ i $b^k$ náleží oboum grupám $\langle a \rangle$ i $\langle b \rangle$. Dokážeme, že průnik

$$\langle a \rangle \cap \langle b \rangle$$

ve skutečnosti obsahuje pouze jednotku. Podle Tvrzení 14.2 pro každý prvek $u \in \langle a \rangle$ platí, že $\mathrm{ord}(u)$ dělí $|\langle a \rangle| = \mathrm{ord}(a) = m$. Analogicky, každý $u \in \langle b \rangle$ splňuje $\mathrm{ord}(u) \mid n$. Vzhledem k tomu, že jsou $m, n$ nesoudělné, pro $u \in \langle a \rangle \cap \langle b \rangle$ platí $\mathrm{ord}(u) = 1$, a tedy $u = 1$. Z toho plyne, že $a^k = b^k = 1$. Tedy $k$ je společným násobkem $m, n$, a jelikož jsou $m, n$ nesoudělné, $mn \mid k$. Tedy $\mathrm{ord}(ab) = mn$. □

**Definice.** *Exponentem* grupy $\mathbf{G}$ rozumíme nejmenší přirozené číslo $m$ takové, že $a^m = 1$ pro všechny prvky $a \in G$, pokud takové $m$ existuje. V opačném případě říkáme, že exponent $\mathbf{G}$ je nekonečný.

Je-li $\mathbf{G}$ konečná, její exponent je konečný, díky Tvrzení 14.2 dělí číslo $|G|$ a navíc je roven nejmenšímu společnému násobku všech řádů, které se vyskytují v grupě $\mathbf{G}$. Např.

- exponent grupy $\mathbb{Z}_4$ je 4,
- exponent grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$ je 2,
- exponent obou šestiprvkových grup $\mathbb{Z}_6$ i $\mathbf{S}_3$ je 6.

Exponent cyklické grupy $\mathbf{G}$ je roven $|G|$. Pro abelovské grupy platí i opačné tvrzení: *abelovská* grupa $\mathbf{G}$ je cyklická právě tehdy když je její eponent roven $|G|$. (Obecně to neplatí, viz grupa $\mathbf{S}_3$ !) Dokážeme o něco obecnější tvrzení:

**Lemma 14.12.** *Buď* $\mathbf{G}$ *abelovská grupa s konečným exponentem* $m$*. Pak existuje prvek* $a \in G$ *řádu* $m$*.*

*Důkaz.* Buď $m = p_1^{k_1} \cdots p_n^{k_n}$ prvočíselný rozklad čísla $m$.

(1) Pro každé $i = 1, \ldots, n$ zvolme $a_i \in G$ tak, aby

$$a_i^{m/p_i} \neq 1.$$

(Protože $m/p_i < m$, musí takové $a_i$ existovat.)

(2) Definujme

$$b_i = a_i^{m/p_i^{k_i}}.$$

Ukážeme, že $\mathrm{ord}(b_i) = p_i^{k_i}$.

(a) $b_i^{p_i^{k_i}} = a_i^m = 1$, tedy $\mathrm{ord}(b_i) \leq p_i^{k_i}$.

(b) Předpokládejme, že $b_i^u = 1$ pro nějaké $0 < u < p_i^{k_i}$. Pak podle Lemmatu 14.10 $b_i^{\mathrm{NSD}(u, p_i^{k_i})} = 1$. Přitom $\mathrm{NSD}(u, p_i^{k_i}) = p_i^v$ pro nějaké $0 \leq v < k_i$, a tedy

$$1 = b_i^{p_i^v} = (a_i^{m/p_i^{k_i}})^{p_i^v} = a_i^{m/p_i^{k_i - v}} \neq 1,$$

protože $m/p_i^{k_i - v} < m/p_i$, spor.

(3) Položme

$$a = b_1 \cdot \ldots \cdot b_n.$$

Podle Lemmatu 14.11 je $\mathrm{ord}(a) = \mathrm{ord}(b_1) \cdot \ldots \cdot \mathrm{ord}(b_n) \overset{(2)}{=} p_1^{k_1} \cdots p_n^{k_n} = m$. □

Předchozí lemma tvoří stěžejní krok v důkazu Věty 14.9.

**Věta 14.13.** *Je-li* $\mathbf{T}$ *konečné těleso, pak je* $\mathbf{T}^*$ *cyklická grupa.*

*Důkaz.* Označme $n = |T|$. Stačí dokázat, že exponent grupy $\mathbf{T}^*$ je $n-1$: pak podle Lemmatu 14.12 existuje prvek řádu $n-1$, neboli generátor grupy $\mathbf{T}^*$.

Pro spor předpokládejme, že je exponent $\mathbf{T}^*$ menší, označme jej $k < n-1$. Pak všechny prvky $a \in T^*$ splňují $a^k = 1$, jinými slovy každý nenulový prvek tělesa $\mathbf{T}$ je kořenem polynomu $x^k - 1$. Avšak podle Věty 9.2 polynom stupně $k$ může mít v daném tělese nejvýše $k$ kořenů, spor. □

Věta 14.9 je speciálním případem právě dokázané věty.

14.4. *** Diskrétní logaritmus.**

Buď $\mathbf{G}$ cyklická grupa a $a$ její generátor, označme $n = |G|$. Tedy pro každé $b \in G$ existuje právě jeden exponent $k \in \{0, \ldots, n-1\}$ takový, že $b = k \times a$. Toto číslo se nazývá *diskrétní logaritmus* prvku $b$ o základu $a$ v grupě $\mathbf{G}$ a značí se $\log_a b$. Čili logaritmus je bijektivní zobrazení $G \to \{0, \ldots, n-1\}$.

Proč „logaritmus“? Je-li grupa $\mathbf{G}$ multiplikativní, pak $k \times a = a^k$, tedy jde o značení analogické tomu, na co jsme zvyklí z reálných čísel. V aditivním zápise pak jde jakoby o dělení.

**Příklad.**

- Uvažujme grupu $\mathbb{Z}$. Má jen dva generátory, a to $a = \pm 1$. Pak $\log_a b$ je rovno tomu (jedinému) $k \in \{0, \ldots, n-1\}$, pro které $ka = b$. Tedy $\log_1 b = b$ a $\log_{-1} b = -b$.
- Uvažujme grupu $\mathbb{Z}_n$ a její generátor $a$. Pak $\log_a b$ je rovno tomu (jedinému) $k \in \{0, \ldots, n-1\}$, pro které

  $$ka \bmod n = b.$$

  Takové $k$ najdeme snadno Eukleidovým algoritmem: protože je $\mathrm{NSD}(a, n) = 1$ (viz Tvrzení 14.6), algoritmus nalezne $u, v \in \mathbb{Z}$ splňující $ua + vn = 1$. Tedy $b = uab + vnb \equiv ub \cdot a \pmod{n}$, čili $\log_a b = ub \bmod n$.
  Např. v $\mathbb{Z}_{11}$ je $\log_7 4 = 10$, protože $7 \cdot 10 \equiv 4 \pmod{11}$.
- Uvažujme grupu $\mathbb{Z}_p^*$, $p$ prvočíslo, a její generátor $a$. Pak $\log_a b$ je rovno tomu (jedinému) $k \in \{0, \ldots, p-2\}$, pro které

  $$a^k \bmod p = b.$$

  Není znám žádný efektivní algoritmus (tj. pracující v čase, který je polynomiální vzhledem k počtu cifer $p$) na výpočet $\log_a b$.
  Např. v $\mathbb{Z}_{11}^*$ je $\log_7 4 = 6$, protože $7^6 \equiv 4 \pmod{11}$.

Existuje řada dalších konstrukcí cyklických grup, např. pomocí eliptických křivek, pomocí kvadratických rozšíření těles atd. Ve všech těchto grupách lze uvažovat diskrétní logaritmus. Pro kryptografii jsou zajímavé ty případy, kdy existuje rychlý algoritmus na výpočet „mocniny“, ale není znám žádný rychlý algoritmus na výpočet logaritmu.

14.5. *** Kryptografické aplikace.**

(Celý tento odstavec je míněn pouze jako nástin myšlenek, které jsou za aplikací abelovských grup v kryptografii. Většina informací je v nějakém smyslu zjednodušená. Přesné formulace by byly zcela mimo účel a rozsah tohoto textu, zájemce odkazujeme na kryptografickou literaturu, např. [Kob94], [Sch96].)

Velmi zjednodušeně řečeno, *jednosměrnou funkcí* rozumíme takovou bijekci $f$, pro kterou existuje rychlý algoritmus na její výpočet, ale není znám žádný rychlý algoritmus, který by počítal inverzní funkci $f^{-1}$. V kryptografii se používají např. následující jednosměrné funkce:

- Je-li $N = pq$ součin dvou (přibližně stejně) velkých různých prvočísel a $k > 1$, uvažujme funkci
$$\{0, \dots, N-1\} \to \{0, \dots, N-1\}, \quad x \mapsto x^k \bmod N.$$
Inverzní funkcí je „$k$-tá odmocnina modulo $N$“.
- Je-li $p$ velké prvočíslo a $a$ generátor grupy $\mathbb{Z}_p^*$, uvažujme funkci
$$\{0, \dots, p-2\} \to \{1, \dots, p-1\}, \quad x \mapsto a^x \bmod p.$$
Inverzní funkcí je diskrétní logaritmus v grupě $\mathbb{Z}_p^*$.
- Analogie předchozí funkce pro grupy odvozené z eliptických křivek a jiné konstrukce.

Zatímco mocninu mod $n$ lze snadno spočítat v čase $O(\log^2 n)$, nejlepší známé algoritmy na výpočet diskrétního logaritmu, resp. odmocniny mod $n$, jsou asymptoticky jen o málo lepší než $O(n)$; jinými slovy, počítat inverzní funkci je exponenciálně pomalejší. Zvolíme-li číslo $n$ řádu $2^{1000}$, pak na běžných počítačích probíhá operace mocnění ve zlomku sekundy, zatímco logaritmus, resp. odmocnina, by se počítaly řádově staletí.

Pro ilustraci ukážeme několik protokolů založených na jednosměrných funkcích. Přímočarým využitím je protokol na hod mincí. Problém diskrétního logaritmu se používá pro výměnu klíče (*Diffie-Hellmanův* protokol), obě uvedené jednosměrné funkce lze využít pro kryptografii s veřejným klíčem (*RSA* a *El Gamalův* protokol). V současné době jde patrně o nejpoužívanější kryptosystémy.

**Hod mincí.** Alice a Bob si chtějí na dálku zahrát hru „panna nebo orel“. Alice bude házet mincí, Bob hádat. Jak to ale udělat, aby Alice Boba nepodvedla? Zvolme nějakou jednosměrnou funkci $f$ na množině $\{1, \dots, n\}$. Pokud Alice hodí orla, zvolí náhodné liché číslo $x$, v opačném případě zvolí sudé číslo. Bobovi pošle hodnotu $f(x)$. Protože je $f$ jednosměrná, Bob neumí spočítat, co padlo, zvolí tedy odpověď náhodně. Nyní Alice zveřejní číslo $x$ a Bob ihned vidí, zda vyhrál nebo ne. Může Alice podvádět? Dejme tomu, že padl orel a to samé si tipnul Bob. Aby Alice Boba podvedla, musela by Bobovi poslat sudé $y$ takové, že $f(y) = f(x)$. Takové ale není, pokud je $f$ bijekce.

**Diffie-Hellman.** Jednou ze základních kryptografických úloh je následující: Alice a Bob se potřebují dohodnout na nějakém společném hesle (odborně *klíči*), přičemž k dispozici mají pouze veřejný kanál (např. odposlouchávaný telefon). Jak to provést?

Nejprve se Alice a Bob dohodnou na nějaké cyklické grupě $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ generované prvkem $a$, ve které je mocnění rychlé, ale výpočet diskrétního logaritmu pomalý (jako třeba $\mathbb{Z}_p^*$ pro velké $p$). (Tato informace nepříteli nijak nepomůže, mohou se tedy domluvit libovolným veřejným kanálem.) Dále si Alice zvolí číslo $m$ a Bob číslo $n$ z intervalu $0, \dots, |G| - 1$, přičemž každý bude svoje číslo držet v

tajnosti. Pak provedou následující operace: Alice spočte $x = a^m$ a pošle $x$ Bobovi, Bob spočte $y = a^n$ a pošle $y$ Alici. Poté Alice spočte $y^m = (a^n)^m = a^{mn}$ a Bob spočte $x^n = (a^m)^n = a^{mn}$. Oba tedy získali stejný prvek $a^{mn}$, a ten prohlásí za hledaný klíč.

Kdyby nepřítel poslouchal jejich komunikaci, co zjistí? Bude znát $\mathbf{G}$, $a$ a hodnoty $x = a^m$ a $y = a^n$; chtěl by spočítat prvek $a^{mn}$. Tomuto problému se říká *Diffie-Hellmanův problém*. V současné době je známo jediné řešení: použitím diskrétního logaritmu získat z hodnot $x, y$ čísla $m, n$, vynásobit je a dopočítat $a^{mn}$. Zvolíme-li vhodnou grupu, nepřítel se touto metodou výsledku nikdy nedopočítá.

**RSA** (Rivest-Shamir-Adleman). Problém je následující: Alice (nebo kdokoliv jiný) chce poslat zprávu Bobovi tak, aby nikdo jiný nepřečetl, co v ní je. Bob publikuje tzv. *veřejný klíč*, pomocí něhož může Alice (nebo kdokoliv jiný) zašifrovat svoji zprávu a poslat ji Bobovi. Pouze Bob ovšem zná *soukromý klíč*, pomocí něhož lze zprávu dešifrovat. Popíšeme, jak generovat klíče a jak šifrovat a dešifrovat zprávu.

Na začátku Bob vygeneruje dvě různá přibližně stejně velká prvočísla $p, q$ a spočte $N = pq$. Dále náhodně zvolí číslo $e$ nesoudělné s $\varphi(N)$ a pomocí Eukleidova algoritmu spočte číslo $d$ splňující

$$de \equiv 1 \pmod{\varphi(N)}.$$

Čísla $N, e$ budou *veřejným klíčem* (ten Bob rozhlásí do světa), čísla $d, p, q$ budou *soukromým klíčem* (ten bude Bob držet v tajnosti).

Nyní kdykoliv chce někdo poslat Bobovi zprávu, provede následující (pro jednoduchost budeme předpokládat, že zprávu tvoří nějaké přirozené číslo $0 < x < N$ nesoudělné s $N$): vypočítá

$$y = x^e \bmod N$$

a výsledek pošle libovolným komunikačním kanálem Bobovi.

I když $y$ zachytí nepřítel, nejsou v současné době známy prostředky, jak získat z čísel $N, e, y$ číslo $x$: je-li $N$ dostatečně velké, neumí se v rozumném čase spočítat ani $e$-tá odmocnina mod $N$, ani prvočísla $p, q$ (pomocí nichž by šlo rychle dopočítat soukromý klíč $d$), a není znám ani jiný způsob, jak RSA prolomit.

Bob, se znalostí soukromého klíče $d$, ovšem dešifruje snadno: protože $ed \equiv 1 \pmod{\varphi(N)}$, podle Eulerovy věty je

$$y^d \equiv \left(x^e\right)^d = x^{ed} \equiv x^1 = x \pmod{N}$$

a Bob tedy získá $x$ výpočtem

$$x = y^d \bmod N.$$

(Znovu zopakujme, že bezpečnost RSA není prokazatelná: spočívá v tom, že přes veškerou mnohaletou snahu *nikdo dosud nenašel* způsob, jak rychle spočítat $x$ bez znalosti soukromého klíče $d$.)

Poznamenejme, že tento protokol využívá tzv. *zadní vrátka* (trapdoor) pro funkci odmocňování mod $N$; v obecnosti se zadními vrátky rozumí dodatečná informace, která činí jednosměrnou funkci obousměrnou. V tomto případě jde o znalost $e$ splňujícího $de \equiv 1 \pmod{\varphi(N)}$, které umožňuje počítat $\sqrt[e]{y}$ jako $y^d$. Útok proti RSA tak lze vést dvěma způsoby: proti jednosměrné funkci (najít rychlý algoritmus na výpočet odmocniny) i proti zadním vrátkům (nalezení rychlého způsobu výpočtu $e$ bez znalosti $p, q$).

**El Gamal.** Tento protokol řeší stejnou úlohu jako RSA, ale je založen na na diskrétním logaritmu (nikoliv odmocňování).

Bob zvolí *vhodnou* cyklickou grupu $\mathbf{G} = (G, \cdot, ^{-1}, 1) = \langle a \rangle$, náhodné číslo $k \in \{0, \dots, |G| - 1\}$ a spočte $b = a^k$. *Veřejným klíčem* bude $\mathbf{G}, a, b$, *soukromým klíčem* bude $k$.

Odesilatel zprávy zvolí náhodné číslo $l \in \{0, \dots, |G| - 1\}$ (které bude držet v tajnosti) a zprávu $x \in G$ zašifruje jako dvojici

$$y = (c_1, c_2),$$

kde $c_1 = a^l$ a $c_2 = x \cdot b^l$. Dešifrování pomocí $k$ je snadné:

$$c_2 \cdot c_1^{-k} = x \cdot b^l \cdot (a^l)^{-k} = x \cdot (a^l)^k \cdot (a^l)^{-k} = x.$$

Je vidět, že kdybychom uměli počítat rychle diskrétní logaritmus, okamžitě získáme soukromý klíč. Neexistence rychlého logaritmování však bohužel není postačující podmínkou na volbu *vhodné* cyklické grupy $\mathbf{G}$: byl např. nalezen způsob, jak El Gamalův protokol prolomit v případě grup $\mathbb{Z}_p^*$. Možná proto se tento algoritmus používá relativně málo, hodí se pro něj např. grupy odvozené z eliptických křivek.

## 15. * Klasifikace konečných abelovských grup

**Cíl.** *Direktní součiny cyklických grup jsou, až na izomorfismus, jediné příklady konečných abelovských grup.*

V této sekci se seznámíme s dalším příkladem tzv. *klasifikační věty*, tj. věty, která popisuje všechny příklady algeber s danou vlastností. Konkrétně půjde o všechny konečné abelovské grupy. (Jeden takový příklad jsme již měli: cyklické grupy jsou, až na izomorfismus, pouze grupy $\mathbb{Z}_n$ a $\mathbb{Z}$.)

Věta říká dokonce více: rozklad dané konečné abelovské grupy na součin cyklických je v jistém smyslu jednoznačný.

**Věta 15.1.** *Buď* $\mathbf{G}$ *alespoň dvouprvková konečná abelovská grupa. Pak existují prvočísla* $p_1, \dots, p_m$ *a přirozená čísla* $k_1, \dots, k_m$ *taková, že*

$$\mathbf{G} \simeq \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_2^{k_2}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

*Čísla* $p_1, \dots, p_m$ *a* $k_1, \dots, k_m$ *jsou jednoznačně určená až na pořadí.*

Než větu dokážeme, předvedeme si příklady.

**Příklad.** Grupy $\mathbb{Z}_5^*$ i $\mathbb{Z}_{12}^*$ jsou čtyřprvkové. Jsou tedy izomorfní buď grupě $\mathbb{Z}_4$, nebo grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$.

- $\mathbb{Z}_5^* \simeq \mathbb{Z}_4$, protože řád prvku 2 v $\mathbb{Z}_5^*$ je 4, tedy $\mathbb{Z}_5^* = \langle 2 \rangle$.
- $\mathbb{Z}_{12}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, protože všechny prvky $\mathbb{Z}_{12}^*$ mají řád 1 nebo 2.

**Příklad.** Grupa $\mathbb{Z}_{21}^*$ je dvanáctiprvková. Je tedy izomorfní buď grupě $\mathbb{Z}_3 \times \mathbb{Z}_4$, nebo grupě $\mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Podle Čínské věty o zbytcích je $\mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_{12}$. Protože grupa $\mathbb{Z}_{21}^*$ neobsahuje žádný prvek řádu 12, platí $\mathbb{Z}_{21}^* \simeq \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

I v této sekci se budeme kvůli názornosti výpočtů držet multiplikativního značení, tj. předpokládáme, že $\mathbf{G} = (G, \cdot, ^{-1}, 1)$.

K důkazu věty se bude hodit pomocné tvrzení, které umožňuje dokázat, že se daná grupa rozkládá jako direktní součin. Označme

$$AB = \{a \cdot b : \ a \in A, \ b \in B\}.$$

Pokud množiny $A, B$ tvoří podgrupu grupy $\mathbf{G}$, pak $AB$ také tvoří podgrupu, neboť pro všechna $a, c \in A$ a $b, d \in B$ platí

$$(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d) \in AB, \quad (a \cdot b)^{-1} = a^{-1} \cdot b^{-1} \in AB, \quad 1 = 1 \cdot 1 \in AB.$$

(Samozřejmě pouze za předpokladu, že je $\mathbf{G}$ abelovská).

**Lemma 15.2.** *Buď $\mathbf{G}$ abelovská grupa, $\mathbf{A}$, $\mathbf{B}$ její podgrupy a předpokládejme, že $A \cap B = \{e\}$ a $AB = G$. Pak*

$$\mathbf{G} \simeq \mathbf{A} \times \mathbf{B}.$$

*Důkaz.* Definujme zobrazení

$$\varphi : \mathbf{A} \times \mathbf{B} \to \mathbf{G}, \qquad (a, b) \mapsto a \cdot b.$$

Protože $AB = G$, zobrazení $\varphi$ je na. Je to homomorfismus, protože

$$\varphi((a, b) \cdot (c, d)) = \varphi((a \cdot c, b \cdot d)) = (a \cdot c) \cdot (b \cdot d) = (a \cdot b) \cdot (c \cdot d) = \varphi((a, b)) \cdot \varphi((c, d)).$$

Nakonec dokážeme prostost. Je-li $a \cdot b = 1$, pak $b = a^{-1}$ a tento prvek leží v obou podgrupách $\mathbf{A}, \mathbf{B}$. Tedy náleží průniku $A \cap B = \{1\}$, čili $a^{-1} = b = 1$. Dostáváme $\mathrm{Ker}(\varphi) = \{(1, 1)\}$ a podle Tvrzení 13.4 je homomorfismus $\varphi$ prostý. □

*Důkaz Věty 15.1.* Nejprve dokážeme existenci direktního rozkladu. Začneme speciálním případem. Je-li grupa $\mathbf{G}$ cyklická, podle Věty 14.4 je $\mathbf{G} \simeq \mathbb{Z}_n$, a označíme-li $n = p_1^{k_1} \cdots p_m^{k_m}$, pak je podle Tvrzení 13.5

$$\mathbf{G} \simeq \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}}.$$

Pro obecné grupy budeme postupovat indukcí podle $|G|$. Je-li $\mathbf{G}$ cyklická, aplikujeme předchozí postup. Není-li cyklická, nalezneme vlastní podgrupy $\mathbf{A}, \mathbf{B}$, které splňují předpoklady Lemmatu 15.2: tyto podgrupy jsou menší, tedy z indukčního předpokladu jdou požadovaným způsobem rozložit a tím získáme rozklad celé grupy $\mathbf{G}$.

Čili předpokládejme, že $\mathbf{G}$ je necyklická konečná abelovská grupa. Podle Lemmatu 14.12 existuje prvek $a \in G$ takový, že jeho řád je roven exponentu grupy $\mathbf{G}$; označme toto číslo $m$. Položme

$$\mathbf{A} = \langle a \rangle$$

a pro spor předpokládejme, že odpovídající podgrupa, která by splňovala podmínky Lemmatu 15.2, neexistuje. V tom případě uvažujme maximální (vzhledem k inkluzi) podgrupu $\mathbf{B}$ splňující $A \cap B = \{1\}$ a definujme

$$C = AB.$$

Podle předpokladu $C \neq G$, zvolme tedy libovolné $d \in G \setminus C$ a označme $r$ nejmenší kladné číslo takové, že

$$d^r \in C.$$

(Takové $r$ existuje, protože přinejmenším $d^m = 1 \in C$.) Nakonec zvolme $b \in B$ a $s \in \mathbb{Z}$ takové, že

$$d^r = a^s \cdot b.$$

(Taková $b, s$ existují, neboť $d^r \in C = AB$ a $A = \langle a \rangle$.)

*Pozorování P1.* Je-li $d^t \in C$, pak $r \mid t$.

Kdyby tomu tak nebylo, označme $u = t \operatorname{div} r$, $v = t \bmod r$ a můžeme psát

$$d^t = d^{ur+v} = (d^r)^u \cdot d^v.$$

Jelikož $d^t \in C$ i $d^r \in C$, měli bychom $d^v \in C$, což je ve sporu s minimalitou $r$.

*Pozorování P2.* $r \mid s$.

Rozepišme

$$1 = d^m = (d^r)^{m/r} = (a^s)^{m/r} \cdot b^{m/r} = a^{ms/r} \cdot b^{m/r}.$$

Protože jak 1, tak $b^{m/r}$ leží v $B$, dostáváme $a^{ms/r} \in B$. Tedy $a^{ms/r} \in A \cap B = \{1\}$, čili $a^{ms/r} = 1$. Přitom $\mathrm{ord}(a) = m$, takže $r \mid s$.

Díky P2 můžeme definovat

$$e = d \cdot a^{-s/r}.$$

*Pozorování P3.* $d^u \in C$ právě tehdy, když $e^u \in C$.

Plyne z toho, že $e^u = d^u \cdot a^{-su/r}$ a z toho, že $a^{-su/r} \in A \subseteq C$.

*Pozorování P4.* $(\tilde{d})^r \in B$

Plyne z toho, že $e^r = d^r \cdot a^{-s} = a^s \cdot b \cdot a^{-s} = b \in B$.

Označme nyní

$$D = \langle e \rangle \qquad \text{a} \qquad \tilde{B} = BD.$$

Zřejmě $B \subset \tilde{B}$, a tak pokud ukážeme, že $A \cap \tilde{B} = \{1\}$, dostaneme spor s tím, že $\mathbf{B}$ byla maximální podgrupa s touto vlastností.

Buď tedy $c \in A \cap \tilde{B}$. Pak existují $u, v \in \mathbb{Z}$ a $\tilde{b} \in B$ takové, že

$$c = a^u \qquad \text{a} \qquad c = \tilde{b} \cdot e^v.$$

Odtud $a^u = b \cdot e^v$ a dostáváme $e^v = a^u \cdot b^{-1} \in AB = C$. Podle P3 také $d^v \in C$, a tedy podle P1 $r \mid v$. Čili podle P4 $e^v \in B$, tedy i $c = b \cdot e^v \in B$ a dostáváme $c \in A \cap B = \{1\}$.

Na závěr dokážeme jednoznačnost koeficientů $p_1, \dots, p_m$ a $k_1, \dots, k_m$. Uvažujme dvě izomorfní grupy

$$\mathbf{G} = \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_m^{k_m}} \simeq \mathbf{H} = \mathbb{Z}_{q_1^{l_1}} \times \cdots \times \mathbb{Z}_{q_r^{l_r}},$$

bez újmy na obecnosti předpokládejme $p_1 \leq \cdots \leq p_m$ a $q_1 \leq \cdots \leq q_r$. Zafixujme prvočíslo $p$, které se vyskytuje v alespoň jednom rozkladu, a označme $a_k$ počet činitelů $\mathbb{Z}_{p^k}$ v grupě $\mathbf{G}$ a $b_k$ počet činitelů $\mathbb{Z}_{p^k}$ v grupě $\mathbf{H}$. Dokážeme, že $a_k = b_k$ pro všechna $k$.

Všimněte si, že všechny prvky řádu $p^u$ jsou tvaru $(0, \dots, 0, x_1, \dots, x_s, 0, \dots, 0)$, kde koeficienty $x_1, \dots, x_s$ jsou na pozicích, které odpovídají grupám $\mathbb{Z}_{p^v}$. Důsledek 14.7 říká, že grupa $\mathbb{Z}_{p^v}$ obsahuje právě $p^{u-1}(p-1)$ prvků řádu $p^u$ pro každé $u \leq v$. Z toho plyne, že grupa $\mathbb{Z}_{p^v}$ obsahuje právě $p^u$ prvků řádu $\leq p^u$. A z toho plyne, že v grupě $\mathbf{G}$ je počet prvků řádu $p^u$ právě

$$\prod_{i<u} \underbrace{p^i \cdots p^i}_{a_i\text{-krát}} \cdot \prod_{i \geq u} \underbrace{p^u \cdots p^u}_{a_i\text{-krát}} = \prod_{i<u} p^{i \cdot a_i} \cdot \prod_{i \geq u} p^{u \cdot a_i} = p^{\sum_{i<u} i \cdot a_i + u \cdot \sum_{i \geq u} a_i}.$$

Analogicky v $\mathbf{H}$ to je

$$p^{\sum_{i<u} i \cdot b_i + u \cdot \sum_{i \geq u} b_i}.$$

Protože $\mathbf{G} \simeq \mathbf{H}$, z Tvrzení 14.3 plyne, že jsou tyto počty totožné, čili že platí

$$\sum_{i<u} i a_i + u \cdot \sum_{i \geq u} a_i = \sum_{i<u} i b_i + u \cdot \sum_{i \geq u} b_i$$

pro všechna $u$. Z těchto rovností se snadno odvodí, že $a_k = b_k$ pro každé $k$:

$$\begin{aligned} u = 1: &\quad \sum_{i\geq 1} a_i = \sum_{i\geq 1} b_i \\ u = 2: &\quad a_1 + 2\cdot\sum_{i\geq 2} a_i = b_1 + 2\cdot\sum_{i\geq 2} b_i \\ u = 3: &\quad a_1 + 2a_2 + 3\cdot\sum_{i\geq 3} a_i = b_1 + 2b_2 + 3\cdot\sum_{i\geq 3} b_i \\ &\dots \end{aligned}$$

Z prvních dvou rovnic vidíme, že $a_1 = b_1$. Třetí rovnice přidá $a_2 = b_2$. Atd. □

## 16. Permutační grupy

**Cíl.** *Grupy permutací na dané množině jsou základním příkladem nekomutativních grup. Speciálně grupy automorfismů různých struktur hrají důležitou roli v celé matematice. V této sekci si ujasníme základní pojmy týkající se permutací (operace, zápis pomocí cyklů, znaménko) a dokážeme základní fakta ohledně řádů, generátorů a konjugace.*

### 16.1. **Permutace, znaménko, generátory.**

*Permutací na množině* $X$ rozumíme bijekci (vzájemně jednoznačné zobrazení) $X \to X$. Pro permutace $\pi, \sigma$ na $X$ definujeme operace $\circ$, $^{-1}$, $id$ předpisy

- $\pi \circ \sigma : x \mapsto \pi(\sigma(x))$,
- $\pi^{-1} : x \mapsto$ ten (jediný) prvek $y$ splňující $\pi(y) = x$,
- $id : x \mapsto x$.

Označíme-li $S_X$ množinu všech permutací na množině $X$, pak $\mathbf{S}_X = (S_X, \circ, ^{-1}, id)$ je tzv. *symetrická grupa* na $X$. Podgrupám této grupy se říká *permutační grupy*. Je-li $X = \{1, \dots, n\}$, značíme $\mathbf{S}_X = \mathbf{S}_n$. Místo $k \times \pi$ používáme značení $\pi^k$.

*Cyklus* v permutaci $\pi$ je posloupnost $x_1, \dots, x_k$ navzájem různých prvků množiny $X$ splňující $\pi(x_1) = x_2$, $\pi(x_2) = x_3$, …, $\pi(x_k) = x_1$. *Rozkladem na cykly* se rozumí zápis

$$(x_{11}\ x_{12}\ \dots\ x_{1k_1})(x_{21}\ x_{22}\ \dots\ x_{2k_2})\cdots(x_{m1}\ x_{m2}\ \dots\ x_{mk_m}),$$

kde $x_{i1}, x_{i2}, \dots, x_{ik_i}$ jsou navzájem různé cykly, $i = 1, \dots, m$. Cykly délky 1 se ze zápisu zpravidla vynechávají. (Je-li $X$ konečná množina, pak rozklad na cykly jistě existuje; pro nekonečné množiny bychom museli povolit „nekonečné cykly“.)

**Tvrzení 16.1.** *Řád permutace $\pi$ v grupě $\mathbf{S}_n$ je roven nejmenšímu společnému násobku délek jejích cyklů.*

*Důkaz.* Cyklus délky $n$ má zřejmě řád $n$ a jsou-li $C_1, \dots, C_m$ disjunktní cykly, pak $(C_1 \circ \dots \circ C_m)^k = C_1^k \circ \dots \circ C_m^k$. Z toho plne, že $(C_1 \circ \dots \circ C_m)^k = id$ právě tehdy, když je $k$ násobkem všech délek cyklů. Čili řád je roven NSN. □

*Transpozicí* rozumíme permutaci tvaru $(x\ y)$.

**Tvrzení 16.2.** *Grupa $\mathbf{S}_n$ je generovaná množinou všech transpozic.*

Jinými slovy, každou permutaci (na konečné množině) lze napsat jako složení transpozic.

*Důkaz.* Libovolný cyklus můžeme rozložit jako

$$(a_1\ a_2\ \dots\ a_k) = (a_1\ a_k) \circ \dots \circ (a_1\ a_3) \circ (a_1\ a_2).$$

Danou permutaci pak můžeme napsat jako složení rozkladů všech jejích cyklů. □

Permutace (na konečné množině) se nazývá *sudá*, pokud se skládá ze sudého počtu transpozic, *lichá* v opačném případě (máme-li dva různé rozklady jedné permutace, mohou mít různé délky, ale určitě stejnou paritu). Definujeme *znaménko permutace*: $\operatorname{sgn}\pi = 1$, je-li $\pi$ sudá, a $\operatorname{sgn}\pi = -1$, je-li $\pi$ lichá. Přímo z definice plyne, že

$$\operatorname{sgn}(\pi \circ \sigma) = \operatorname{sgn}\pi \cdot \operatorname{sgn}\sigma \quad \text{a} \quad \operatorname{sgn}\pi^{-1} = \operatorname{sgn}\pi.$$

(První tvrzení je očividné, druhé plyne ze vztahu $((a_1\ b_1) \circ \dots \circ (a_n\ b_n))^{-1} = (a_n\ b_n) \circ \dots \circ (a_1\ b_1)$.) Z důkazu Tvrzení 16.2 navíc můžeme vyčíst, že

$$\operatorname{sgn}\pi = (-1)^{n-\text{počet cyklů v }\pi}.$$

Díky uvedeným vztahům tvoří sudé permutace podgrupu v $\mathbf{S}_n$, tzv. *alternující grupu* $\mathbf{A}_n$.

**Tvrzení 16.3.** *Grupa $\mathbf{A}_n$ je generovaná množinou všech trojcyklů.*

Jinými slovy, každou sudou permutaci lze napsat jako složení trojcyklů.

*Důkaz.* Danou sudou permutaci nejprve rozložíme na transpozice, a ty seskupíme do dvojic. Pokud jsou dvě sousední transpozice stejné, můžeme je vypustit. Pokud mají společný jeden prvek, pak $(i\ j) \circ (j\ k) = (i\ j\ k)$. A jsou-li disjunktní, pak $(i\ j) \circ (k\ l) = (k\ i\ l) \circ (i\ j\ k)$. Tímto způsobem přepíšeme rozklad na transpozice na složení trojcyklů. □

16.2. **Konjugace.**

**Definice.** Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ grupa a $a, b \in G$. Prvky $a, b$ nazýváme *konjugované* v $\mathbf{G}$, pokud existuje $c \in G$ takové, že $a = c \cdot b \cdot c^{-1}$.

Je vidět, že relace konjugace je ekvivalencí. Můžeme tak hovořit o blocích navzájem konjugovaných prvků.

**Příklad.** Pojem konjugace již znáte z lineární algebry: konjugovaným maticím se tam říká *podobné*. Jordanova věta říká, že matice $A, B$ jsou konjugované v grupě $\mathbf{GL}_n(\mathbb{C})$ právě tehdy, když mají stejný Jordanův kanonický tvar.

**Příklad.** Pojem konjugace je velmi důležitý v permutačních grupách. Uvažujme permutaci

$$\pi = (a_{11}\ a_{12}\ \dots\ a_{1k_1})(a_{21}\ a_{22}\ \dots\ a_{2k_2}) \cdots (a_{m1}\ a_{m2} \dots\ a_{mk_m}),$$

a libovolnou permutaci $\rho$. Pak $\rho \circ \pi \circ \rho^{-1}$ je rovno

$$(\rho(a_{11})\ \rho(a_{12})\ \dots\ \rho(a_{1k_1}))(\rho(a_{21})\ \rho(a_{22})\ \dots\ \rho(a_{2k_2})) \cdots (\rho(a_{m1})\ \rho(a_{m2})\ \dots\ \rho(a_{mk_m})),$$

neboť pro každé $i, j$ platí

$$(\rho \circ \pi \circ \rho^{-1})(\rho(a_{ij})) = \rho(\pi(a_{ij})) = \rho(a_{i(j\oplus 1)}),$$

kde $j \oplus 1 = j + 1$ pro $j < k_j$ a $k_j \oplus 1 = 1$. Konjugace permutace $\pi$ permutací $\rho$ tedy funguje jako „kopírování“, zápis $\pi$ přepíšeme podle pravdidel daných permutací $\rho$.

**Tvrzení 16.4.** *Permutace $\pi, \sigma$ jsou konjugované v grupě $\mathbf{S}_n$ právě tehdy, když mají stejný počet cyklů každé délky (říká se* stejný typ*).*

*Důkaz.* ($\Rightarrow$) Plyne bezprostředně z výpočtu v předchozím příkladu.
($\Leftarrow$) Jsou-li

$$\pi = (a_{11}\ a_{12}\ \dots\ a_{1k_1})(a_{21}\ a_{22}\ \dots\ a_{2k_2})\cdots(a_{m1}\ a_{m2}\dots\ a_{mk_m}),$$
$$\sigma = (b_{11}\ b_{12}\ \dots\ b_{1k_1})(b_{21}\ b_{22}\ \dots\ b_{2k_2})\cdots(b_{m1}\ b_{m2}\dots\ b_{mk_m}),$$

dvě permutace stejného typu, definujeme $\rho(a_{ij}) = b_{ij}$ a použijeme výše uvedený výpočet. □

**Příklad.** Permutace (1 2 3) a (2 3 4) jsou konjugované v grupě $\mathbf{S}_4$, protože obě mají jeden cyklus délky 1 a jeden cyklus délky 3. Tyto permutace ovšem nejsou konjugované v grupě $\mathbf{A}_4$: jak plyne z důkazu Tvrzení 16.4, jediné permutace $\rho$ splňující $(2\ 3\ 4) = \rho \circ (1\ 2\ 3) \circ \rho^{-1}$ jsou (1 4), (1 2 3 4) a (1 3 2 4). Žádná z nich ovšem není sudá.

16.3. *** Grupy automorfismů.**

Důležité příklady permutačních grup jsou tzv. *grupy automorfismů*. Je-li $\mathbf{X} = (X, \dots)$ nějaká struktura (algebra, relační struktura, topologický prostor atd.), její automorfismy vždy tvoří podgrupu grupy $\mathbf{S}_X$; značíme ji $\mathbf{Aut}(\mathbf{X})$.

**Příklad.**

- Pojem automorfismu dané algebry (grupy, oboru integrity atd.) jsme definovali v minulé kapitole. Fakt, že automorfismy tvoří podgrupu, plyne z Tvrzení 11.6.
- Automorfismem grafu $\mathbf{G} = (V, E)$ rozumíme permutaci $\varphi \in S_V$ splňující

  $$\{x, y\} \in E \quad \Leftrightarrow \quad \{\varphi(x), \varphi(y)\} \in E.$$

  Je velmi snadné dokázat, že tato zobrazení tvoří podgrupu grupy $\mathbf{S}_V$.
- Automorfismem uspořádané množiny $\mathbf{X} = (X, \leq)$ rozumíme permutaci $\varphi \in S_X$ splňující

  $$x \leq y \quad \Leftrightarrow \quad \varphi(x) \leq \varphi(y).$$

  Je velmi snadné dokázat, že tato zobrazení tvoří podgrupu grupy $\mathbf{S}_X$.

**Příklad.** Grupa automorfismů úplného grafu na $n$ vrcholech je grupa $\mathbf{S}_n$. Grupa automorfismů $n$-prvkové kružnice je dihedrální grupa $\mathbf{D}_{2n}$. Grupa automorfismů cesty délky $n$ je dvouprvková.

**Příklad.** V předchozí sekci jsme dokázali, že grupa $\mathbf{Aut}(\mathbb{Z})$ je dvouprvková. Je snadné ověřit, že $\mathbf{Aut}(\mathbb{Z}_n) \simeq \mathbb{Z}_n^*$, prvku $a \in \mathbb{Z}_n^*$ odpovídá automorfismus $x \mapsto ax \bmod n$.

S automorfismy grup úzce souvisí konjugace: zobrazení

$$\varphi_a : \mathbf{G} \to \mathbf{G}, \quad x \mapsto a \cdot x \cdot a^{-1}$$

je automorfismus grupy $\mathbf{G}$ pro každé $a \in G$; těmto automorfismům se říká *vnitřní*. Je snadné ověřit, že vnitřní automorfismy tvoří (normální) podgrupu grupy $\mathbf{Aut}(\mathbf{G})$, značíme ji $\mathbf{Inn}(\mathbf{G})$.

**Příklad.**

- V abelovských grupách je zřejmě $\mathrm{Inn}(\mathbf{G}) = \{id\}$.

- V symetrických grupách je $\mathbf{Inn}(\mathbf{S}_n) = \mathbf{Aut}(\mathbf{S}_n) \simeq \mathbf{S}_n$ pro všechna $n \neq 6$. V obecnosti to není vůbec snadné dokázat; předvedeme jednoduchý argument pro $n = 3$.
  Protože je $\mathbf{S}_3 = \langle (1\ 2), (2\ 3) \rangle$, každý její automorfismus je určený hodnotami na těchto dvou transpozicích. Ty se přitom mohou zobrazit jen na transpozice (Tvrzení 14.3), které navíc musí být navzájem různé, takže $\mathbf{Aut}(\mathbf{S}_3)$ je nejvýše šestiprvková grupa. Není těžké nahlédnout, že zobrazení $\mathbf{S}_3 \to \mathbf{Aut}(\mathbf{S}_3)$, $\pi \mapsto \varphi_\pi$ je prostý homomorfismus, a tak $\mathbf{Aut}(\mathbf{S}_3) = \mathbf{Inn}(\mathbf{S}_3) \simeq \mathbf{S}_3$.

**Poznámka.** Každá grupa je izomorfní s grupou $\mathbf{Aut}(\mathbf{G})$ pro nějaký graf $\mathbf{G}$. Každá grupa je izomorfní s grupou $\mathbf{Aut}(\mathbf{X})$ pro nějaký svaz $\mathbf{X}$. Existuje celá teorie o tom, pro které struktury lze reprezentovat každou grupu jako grupu automorfismů.

## 17. Rozklady podle podgrupy

**Cíl.** *Dokážeme Lagrangeovu větu, která říká, že počet prvků podgrupy dělí počet prvků celé grupy. Důkaz se provádí pomocí tzv. rozkladu podle podgrupy. S rozklady pak souvisí pojem normální podgrupy, který je klíčový pro konstrukci faktorgrup.*

### 17.1. Rozklady a Lagrangeova věta.

**Definice.** Buď $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ grupa a $\mathbf{H}$ její podgrupa.

(1) *Levým rozkladem* grupy $\mathbf{G}$ podle podgrupy $\mathbf{H}$ se rozumí množina
$$\{aH : a \in G\},$$
přičemž množinám
$$aH = \{ah : h \in H\}$$
se říká *levé rozkladové třídy.*

(2) *Pravým rozkladem* grupy $\mathbf{G}$ podle podgrupy $\mathbf{H}$ se rozumí množina
$$\{Ha : a \in G\},$$
přičemž množinám
$$Ha = \{ha : h \in H\}$$
se říká *pravé rozkladové třídy.*

Množina $T \subseteq H$ se nazývá

(1) *levou transverzálou*, pokud obsahuje z každé levé rozkladové třídy právě jeden prvek;
(2) *pravou transverzálou*, pokud obsahuje z každé pravé rozkladové třídy právě jeden prvek.

**Příklad.** Buď $\mathbf{G} = \mathbb{Z}$ a $\mathbf{H} = n\mathbb{Z}$. Rozkladové třídy určené prvkem $a \in \mathbb{Z}$ jsou
$$a + H = H + a = \{k \in \mathbb{Z} :\ k \equiv a \pmod{n}\}$$
(používáme symbol + místo $\cdot$, protože grupa $\mathbb{Z}$ má aditivní značení). Je vidět, že dvě rozkladové třídy $a + H$, $b + H$ jsou buď stejné (pokud $a \equiv b \pmod{n}$), nebo disjunktní. Jako transverzálu lze zvolit např.
$$T = \{0, \dots, n-1\},$$
tj. množinu všech možných zbytků po dělení $n$.

**Příklad.** Buď $\mathbf{G} = \mathbf{S}_n$ a $\mathbf{H} = \mathbf{A}_n$. Pak $\pi \circ A_n = A_n \circ \pi = A_n$ pro libovolnou $\pi$ sudou a $\pi \circ A_n = A_n \circ \pi$ sestává ze všech lichých premutací pro libovolnou $\pi$ lichou. Grupa $\mathbf{S}_n$ se tedy rozkládá na dvě rozkladové třídy (levé i pravé vyjdou na stejno), jako transverzálu lze zvolit např. $T = \{id, (1\ 2)\}$.

**Příklad.** Buď $\mathbf{G} = \mathbf{S}_3$ a $\mathbf{H} = \{id, (1\ 2)\}$. Snadno spočteme, že levý i pravý rozklad obsahuje 3 dvouprvkové třídy, avšak

$$(1\ 3) \circ H = \{(1\ 3), (1\ 2\ 3)\}, \quad \text{ale} \quad H \circ (1\ 3) = \{(1\ 3), (1\ 3\ 2)\}.$$

Tedy obecně nemusí platit $aH = Ha$.

Dokážeme několik vlastností levých, resp. pravých rozkladů. Předně, jednotlivé rozkladové třídy jsou disjunktní, tj. je-li $T$ levá transverzála, pak $|T| = |\{aH : a \in G\}|$, resp. je-li $T$ pravá transverzála, pak $|T| = |\{Ha : a \in G\}|$. Další tvrzení říká, za jakých podmínek určují dva prvky stejnou rozkladovou třídu. Dále dokážeme, že jsou všechny (levé i pravé) rozkladové třídy stejně velké a že stejně velký je levý i pravý rozklad. Důsledkem je Lagrangeova věta.

Ve zbytku sekce uvažujme grupu $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ a její podgrupu $\mathbf{H}$.

**Lemma 17.1.** *Pro každé $a, b \in G$ platí*

(1) *buď $aH = bH$, nebo $aH \cap bH = \emptyset$;*
(2) *buď $Ha = Hb$, nebo $Ha \cap Hb = \emptyset$.*

*Důkaz.* (1) Předpokládejme, že existuje $c \in aH \cap bH$; dokážeme, že $aH = bH$. Máme tedy $c = ah_1 = bh_2$ pro nějaká $h_1, h_2 \in H$, a tak pro každé $ah \in aH$ platí

$$ah = ch_1^{-1}h = b\underbrace{h_2h_1^{-1}h}_{\in H} \in bH$$

a podobně pro každé $bh \in bH$ platí

$$bh = ch_2^{-1}h = a\underbrace{h_1h_2^{-1}h}_{\in H} \in aH.$$

Tedy $aH = bH$. (2) se dokáže analogicky. □

**Lemma 17.2.** *Pro každé $a, b \in G$ platí*

(1) *$aH = bH$ právě tehdy, když $a^{-1}b \in H$;*
(2) *$Ha = Hb$ právě tehdy, když $ab^{-1} \in H$.*

*Důkaz.* (1) ($\Rightarrow$) Protože $aH = bH$, máme $b \in aH$, a tedy $b = ah$ pro nějaké $h \in H$. Tudíž $a^{-1}b = h \in H$. ($\Leftarrow$) Jestliže $a^{-1}b \in H$, pak pro každé $ah \in aH$ platí

$$ah = bb^{-1}ah = b\underbrace{(a^{-1}b)^{-1}h}_{\in H} \in bH$$

a podobně pro každé $bh \in bH$ platí

$$bh = a\underbrace{a^{-1}bh}_{\in H} \in aH.$$

Tedy $aH = bH$. (2) se dokáže analogicky. □

**Lemma 17.3.** *Pro každé $a \in G$ platí $|aH| = |Ha| = |H|$.*

*Důkaz.* Vzpomeňme na levé a pravé translace $L_a : G \to G$, $x \mapsto a \cdot x$, resp. $R_a : G \to G$, $x \mapsto x \cdot a$, a uvažujme restrikce $L_a|_H$, resp. $R_a|_H$. Díky krácení jde o prostá zobrazení, obor hodnot $L_a|_H$ je množina $aH$, obor hodnot $R_a|_H$ je množina $Ha$, a tedy $L_a|_H$ je bijekce mezi $H$ a $aH$, a podobně $R_a|_H$ je bijekce mezi $H$ a $Ha$. Čili všechny tyto množiny mají stejný počet prvků. □

**Lemma 17.4.** *Levý i pravý rozklad* $\mathbf{G}$ *podle* $\mathbf{H}$ *mají stejný počet prvků.*

*Důkaz.* Dokážeme, že zobrazení $aH \mapsto Ha^{-1}$ je bijekcí mezi levým a pravým rozkladem. Vlastně není vůbec jasné, zda jsme korektně definovali zobrazení: mohlo by se stát, že tutéž rozkladovou třídu máme označenu dvěma různými způsoby, tj. že $aH = bH$ pro nějaká $a \neq b$, a přitom se jí snažíme přiřadit dvě různé hodnoty $Ha^{-1}, Hb^{-1}$. Ovšem platí

$$aH = bH \;\Leftrightarrow\; a^{-1}b \in H \;\Leftrightarrow\; (a^{-1}b)^{-1} = b^{-1}a \in H \;\Leftrightarrow\; Ha^{-1} = Hb^{-1},$$

a tedy zobrazení je nejen dobře definované, ale také prosté. Evidentně je i na. □

Dokázali jsme, že velikost levého i pravého rozkladu (a tedy levých i pravých transverzál) jsou stejné. Tato hodnota se nazývá *index podgrupy* $\mathbf{H}$ *v grupě* $\mathbf{G}$ a značí se

$$[\mathbf{G} : \mathbf{H}] = |\{aH : a \in G\}| = |\{Ha : a \in G\}|.$$

**Věta 17.5** (Lagrangeova)**.** *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$ *její podgrupa. Pak*

$$|G| = |H| \cdot [\mathbf{G} : \mathbf{H}].$$

*Důkaz.* Zvolme nějakou levou transverzálu $T$; zřejmě $|T| = [\mathbf{G} : \mathbf{H}]$. Protože je nosná množina $G$ disjunktním sjednocením množin $aH$, kde prvky $a$ probíhají množinu $T$ (Lemma 17.1), a protože jsou všechny $aH$ stejně velké (Lemma 17.3), dostáváme $|G| = |T| \cdot |H|$. □

Všechna čtyři lemmata i Lagrangeova věta dávají smysl i pro nekonečné grupy (s použitím kardinálních čísel pro označení velikostí množin). Pro konečné grupy dostáváme následující:

**Důsledek 17.6.** *Buď* $\mathbf{G}$ *konečná grupa a* $\mathbf{H}$ *její podgrupa. Pak* $|H|$ *dělí* $|G|$.

Okamžitým důsledkem je Tvrzení 14.2 — uvažujte $\mathbf{H} = \langle a \rangle$.

## 17.2. **Normální podgrupy.**

**Definice.** Podgrupu $\mathbf{H}$ grupy $\mathbf{G}$ nazýváme *normální*, značíme $\mathbf{H} \trianglelefteq \mathbf{G}$, pokud pro každé $a \in G$ platí $aH = Ha$.

**Příklad.**

- V abelovských grupách je zřejmě každá podgrupa normální.
- Jak je vidět z příkladů uvedených na začátku této sekce, podgrupa $\mathbf{A}_n$ je normální v grupě $\mathbf{S}_n$, ale $\{id, (1\ 2)\}$ netvoří normální podgrupu $\mathbf{S}_3$.

**Tvrzení 17.7.** *Podgrupa* $\mathbf{H}$ *grupy* $\mathbf{G}$ *je normální právě tehdy, když je uzavřena na konjugaci libovolným prvkem grupy* $\mathbf{G}$ *(tj. když pro každé* $h \in H$ *a každé* $a \in G$ *platí* $aha^{-1} \in H$*).*

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

($\Leftarrow$) Buď $ah \in aH$. Pak $k = aha^{-1} \in H$, a tedy $ah = ka \in Ha$. Podobně, je-li $ha \in Ha$, pak $l = a^{-1}ha \in H$, tedy $ha = al \in aH$. Čili $Ha = aH$. □

Důsledkem je, že normální podgrupy grupy $\mathbf{G}$ tvoří svaz, který budeme značit $\mathbf{NSub}(\mathbf{G})$. Infimem je průnik, supremem nejmenší normální podgrupa obsahující sjednocení; důkaz je analogický Tvrzení 11.4. Dokonce platí $\mathbf{H} \vee \mathbf{K} = \mathbf{HK}$, kde $HK = \{hk : h \in H, k \in K\}$. Tato množina zřejmě obsahuje $H$ i $K$ a není těžké ověřit, že tvoří normální podgrupu.

**Příklad.** Užitím Tvrzení 17.7 a 16.4 lze dokázat, že množina

$$\{id, (12)(34), (13)(24), (14)(23)\}$$

tvoří normální podgrupu grupy $\mathbf{S}_4$ (a tedy i grupy $\mathbf{A}_4$): není těžké nahlédnout, že je uzavřena na skládání i invertování a z Tvrzení 16.4 plyne, že je uzavřena i na konjugaci libovolnou permutací. Této podgrupě se říká *Kleinova grupa*.

**Příklad.** Mnohem těžším cvičením na tuto techniku je následující tvrzení:

- Grupy $\mathbf{S}_n$, $n \neq 4$, mají právě tři normální podgrupy: $\{id\}$, $\mathbf{A}_n$ a $\mathbf{S}_n$. Grupa $\mathbf{S}_4$ má čtyři normální podgrupy: navíc ještě Kleinovu.
- Grupy $\mathbf{A}_n$, $n \neq 4$, mají pouze dvě normální podgrupy: obě nevlastní. Grupa $\mathbf{A}_4$ má navíc Kleinovu.

**Tvrzení 17.8.** *Je-li $\varphi : \mathbf{G} \to \mathbf{H}$ homomorfismus grup, pak $\mathbf{Ker}(\varphi) \trianglelefteq \mathbf{G}$.*

*Důkaz.* Podle Tvrzení 13.4 jde o podgrupu a je-li $h \in \mathrm{Ker}(\varphi)$, tj. $\varphi(h) = 1$, a $a \in G$, pak $\varphi(aha^{-1}) = \varphi(a)\varphi(h)\varphi(a)^{-1} = \varphi(a)\varphi(a)^{-1} = 1$, čili $aha^{-1} \in \mathrm{Ker}(\varphi)$. □

Grupy, které nemají vlastní normální podgrupy, se nazývají *jednoduché*. Jedním z největších algebraických výsledků 20. století je klasifikace (tzn. úplný seznam až na izomorfismus) všech konečných jednoduchých grup. Dvě řady příkladů už známe:

- grupy $\mathbb{Z}_p$, $p$ prvočíslo: z Lagrangeovy věty plyne, že nemají vůbec žádné vlastní podgrupy;
- grupy $\mathbf{A}_n$, $n \neq 4$.

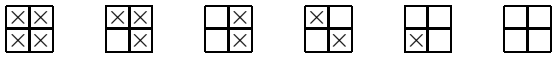
Kromě těchto existuje ještě několik řad maticových grup (např. grupy $\mathbf{PSL}_n(\mathbf{T})$, $\mathbf{T}$ konečné těleso s aspoň 4 prvky, definované jako faktorgrupa $\mathbf{SL}_n(\mathbf{T})/\mathbf{D}$, kde $\mathbf{D}$ značí podgrupu diagonálních matic s determinantem 1) a dále 26 tzv. *sporadických grup*, které nezapadají do ani jedné z uvedených řad.

## 18. * Působení grupy na množině

**Cíl.** *Na každou permutaci lze nahlížet tak, že působí jako hybatel prvků množiny, na které je definovaná. Tento náhled lze zobecnit do působení abstraktní grupy na dané množině. Budeme studovat relaci tranzitivity daného působení a odvodíme Burnsideovu větu, která dává do souvislosti počet orbit a pevné body permutací. Věta má řadu aplikací v kombinatorice i pokročilejší teorii grup.*

Motivací pro tuto kapitolu bude následující kombinatorická úloha.

**Úloha.** Kolika způsoby je možné obarvit políčka čtverce $2 \times 2$ dvěma barvami? Dvě obarvení přitom považujeme za totožná, pokud lze jedno z druhého dostat otočením čtverce.



Úlohu je samozřejmě snadné řešit prostým výčtem všech možných obarvení; až na otočení je to následujících šest:

Pokud bychom ovšem zvětšili čtverec nebo počet barev, výčet by se stal nezvladatelným — uvažujte třeba šachovnici $8 \times 8$ a čtyři barvy! Cílem této sekce je odvodit vzorec (kterému se říká *Burnsideova věta*), který umožňuje relativně snadno počítat *množství nějakých objektů až na dané symetrie* (zde: počet obarvení až na otočení), a to často i v případě, kdy je tento počet obrovský. Teorii budeme průběžně ilustrovat na situaci z uvedené úlohy.

**Definice.** *Působením grupy* $\mathbf{G}$ *na množině* $X$ rozumíme homomorfismus

$$\pi : \mathbf{G} \to \mathbf{S}_X.$$

Hodnotu permutace $\pi(g)$ na prvku $x$ budeme značit krátce $g(x)$.

Protože jde o homomorfismus, jednotka působí jako identita, $g^{-1}$ působí jako inverzní permutace k $\pi(g)$ a platí vztah $(g \cdot h)(x) = g(h(x))$.

**Příklad.** Typickými příklady působení jsou následující tři ukázky.

- Je-li $\mathbf{G}$ podgrupa grupy $\mathbf{S}_X$, můžeme uvažovat přirozené působení na množinu $X$, přičemž $\pi = id$. Speciálně, je-li $\mathbf{X}$ nějaká struktura (např. algebra, graf, uspořádaná množina), pak grupa $\mathbf{Aut}(\mathbf{X})$ působí přirozeně na nosnou množinu $X$ (resp. vrcholy grafu).
- Grupa $\mathbf{GL}_n(\mathbf{T})$ působí na vektorový prostor $\mathbf{T}^n$ jako násobení vektoru maticí; tj. $\pi(A)$ je permutace množiny $T^n$, která vektor $v$ zobrazí na $Av$.
- Grupa $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ působí svoji na nosnou množinu $G$
  - *translacemi*, když za $\pi$ vezmeme Cayleyovu reprezentaci, tj. $g(x) = g \cdot x$;
  - *konjugací*, když za $\pi$ vezmeme homomorfismus, který prvku $g$ přiřadí vnitřní automorfismus daný prvkem $g$; tj. $g(x) = g \cdot x \cdot g^{-1}$.

**Příklad.** V naší motivační úloze působí grupa $\mathbf{G}$ všech otočení čtverce (tj. $\mathbf{G}$ sestává z identity a otočení roviny o 90, 180 a 270 stupňů) na množinu $X$ všech obarvení čverce dvěma barvami (tj. $|X| = 2^4 = 16$), přičemž $\pi(g)$ je permutace, která danému obarvení přiřadí obarvení, které je pootočené o daný úhel.

V celém zbytku sekce budeme uvažovat nějaké pevně dané působení grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ na množinu $X$.

Zavedeme tzv. *relaci tranzitivity* $\sim$ na množině $X$ následujícím způsobem: řekneme, že $x \sim y$, pokud existuje $g \in G$ takové, že $g(x) = y$.

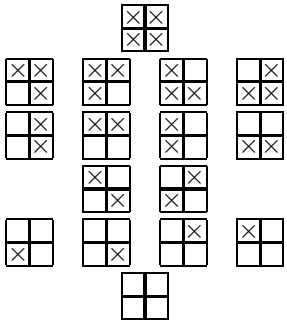
**Pozorování 18.1.** *Relace* $\sim$ *je ekvivalence na* $X$.

*Důkaz.* Reflexivita plyne z toho, že $1(x) = id(x) = x$. Symetrie z toho, že $g(x) = y \Rightarrow g^{-1}(y) = x$. A je-li $x \sim y \sim z$, tedy $g(x) = y$ a $h(y) = z$ pro nějaká $g, h$, pak $(h \cdot g)(x) = h(g(x)) = h(y) = z$, a tedy $x \sim z$. □

Bloky ekvivalence $\sim$ nazýváme *orbity*. Orbitu obsahující prvek $x$ budeme značit

$$[x] = \{y \in X : x \sim y\}.$$

**Příklad.** V naší motivační úloze jsou v relaci $\sim$ taková dvě obarvení, která lze jedno z druhého dostat otočením; tato jsou sdružena do jednotlivých orbit. Množina všech obarvení se tedy rozpadne na šest orbit následujícím způsobem:



Vidíme, že řešením úlohy je *počet orbit* v tomto působení.

Bod $x$ se nazývá *pevným bodem* permutace $\pi$, pokud $\pi(x) = x$. Množinu všech pevných bodů permutace $\pi(g)$ budeme značit

$$X_g = \{x \in X : g(x) = x\}$$

a *stabilizátorem prvku* $x \in X$ nazveme množinu

$$G_x = \{g \in G : g(x) = x\}.$$

**Příklad.** Stabilizátorem obou jednobarevných obarvení je celá grupa $\mathbf{G}$. Stabilizátor obarvení  obsahuje pouze identitu. Stabilizátor obarvení  obsahuje identitu a otočení o 180 stupňů.

**Pozorování 18.2.** *$G_x$ tvoří podgrupu grupy $\mathbf{G}$.*

*Důkaz.* Jednotka náleží $G_x$, neboť $1(x) = id(x) = x$. Je-li $g, h \in G_x$, tj. $g(x) = h(x) = x$, pak $g^{-1}(x) = x$ a $(g \cdot h)(x) = g(h(x)) = g(x) = x$, tedy množina $G_x$ je uzavřená na všechny operace grupy. □

**Lemma 18.3.** *Pro každé $x \in X$ platí $|G| = |G_x| \cdot |[x]|$.*

*Důkaz.* Protože je $\mathbf{G}_x$ podgrupa grupy $\mathbf{G}$, Lagrangeova věta říká, že

$$|G| = |G_x| \cdot [\mathbf{G} : \mathbf{G}_x].$$

Stačí tedy dokázat, že $\big|[x]\big| = [\mathbf{G} : \mathbf{G}_x] = \big|\{gG_x : g \in G\}\big|$. Uvažujme tedy zobrazení

$$\varphi : \{gG_x : g \in G\} \to [x], \qquad gG_x \mapsto g(x),$$

dokážeme, že to je bijekce. Předně je třeba ověřit, že jsme skutečně definovali zobrazení: mohlo by se stát, že tutéž rozkladovou třídu máme označenu dvěma různými způsoby, tj. že $gG_x = hG_x$ pro nějaká $g \neq h$, a přitom se jí snažíme přiřadit dvě různé hodnoty $g(x), h(x)$. Ovšem podle Lemmatu 17.2 platí

$$gG_x = hG_x \;\Leftrightarrow\; h^{-1}g \in G_x \;\Leftrightarrow\; h^{-1}g(x) = x \;\Leftrightarrow\; g(x) = h(x),$$

a tedy $\varphi$ je nejen dobře definované, ale také prosté. Navíc pro každý prvek $y \in [x]$ existuje $g \in G$ splňující $g(x) = y$, tedy $\varphi$ je bijekce. □

Z lemmatu plyne, že velikosti orbit dělí počet prvků grupy $\mathbf{G}$. (Všimněte si, že to je splněno v naší motivační úloze.)

Připomeňme, že $X/\!\sim$ značí množinu všech bloků ekvivalence $\sim$, tj. $|X/\!\sim|$ značí počet orbit daného působení.

**Věta 18.4** (Burnsideova)**.** *Působí-li konečná grupa* $\mathbf{G}$ *na konečnou množinu* $X$*, pak*

$$\big|X/{\sim}\big| = \frac{1}{|G|} \cdot \sum_{g \in G} \big|X_g\big|.$$

*Důkaz.* Označme

$$M = \big\{(g,x) \in G \times X : g(x) = x\big\}.$$

Prvky této množiny můžeme spočítat dvěma způsoby: buď pro každé $g$ počítáme počet $x$ takových, že $(g,x) \in M$, nebo naopak, pro každé $x$ počítáme počet $g$ takových, že $(g,x) \in M$. Dostáváme tak následující rovnost:

$$|M| = \sum_{g \in G} |X_g| = \sum_{x \in X} |G_x|.$$

Použitím této rovnosti dopočítáme uvedený vzorec:

$$\frac{1}{|G|} \cdot \sum_{g \in G} |X_g| \;=\; \frac{1}{|G|} \cdot \sum_{x \in X} |G_x| \overset{18.3}{=} \frac{1}{|G|} \cdot \sum_{x \in X} \frac{|G|}{\big|[x]\big|} \;=\; \sum_{x \in X} \frac{1}{\big|[x]\big|} \;=$$

$$\sum_{O \in (X/\sim)} \sum_{x \in O} \frac{1}{\big|[x]\big|} \;=\; \sum_{O \in (X/\sim)} \sum_{x \in O} \frac{1}{|O|} \;=\; \sum_{O \in (X/\sim)} |O| \cdot \frac{1}{|O|} \;=\; \sum_{O \in (X/\sim)} 1.$$

Výsledek je tedy roven velikosti množiny $X/{\sim}$, tj. počtu orbit. □

Vzorec lze interpretovat tak, že „počet orbit je roven průměrnému počtu pevných bodů permutací z $\mathbf{G}$“. V kombinatorických úlohách bývá obvykle množina $X$ obrovská (např. obarvení velkých objektů mnoha barvami), zatímco grupa symetrií poměrně malá (např. otočení čtverce jsou jen čtyři, nezávisle na jeho velikosti). Vytvoření „všech možných konfigurací“ by již pro čtverec $4 \times 4$ bylo ručně takřka nezvladatelné, ovšem spočítat počet pevných bodů pro jednotlivá otočení lze snadno i v obecném případě.

**Příklad.** Vrátíme-li se k naší motivační úloze, vidíme, že identita zachovává všechna obarvení, tedy $|X_{id}| = |X| = 2^4 = 16$. Otočení o 90 stupňů zobrazuje levý dolní čtverec na levý horní, levý horní na pravý horní, atd., čili abychom dostali stejné obarvení, musí mít všechny čtyři čtverce stejnou barvu. Tedy $|X_{90}| = 2$. Podobně $|X_{270}| = 2$. Otočení o 180 stupňů zaměňuje levý dolní čtverec na pravý horní a levý horní za pravý dolní. Tyto dvě dvojice tedy musí být stejnobarevné, a to lze provést čtyřmi způsoby. Tedy $|X_{180}| = 4$. Podle Burnsideovy věty je počet obarvení až na otočení $\frac{1}{4} \cdot (16 + 2 + 4 + 2) = 6$.

Metodu ilustrujeme na několika dalších úlohách.

**Úloha.** a) Dětská stavebnice obsahuje tři červené, tři zelené a tři modré čtvercové destičky. Kolika způsoby je lze sestavit do velkého čtverce $3 \times 3$? Dvě sestavy považujeme za totožné, pokud jednu z druhé dostaneme otočením. b) Jak se výsledek změní, pokud je možné dílky pevně spojovat? Tedy pokud dvě sestavy považujeme za totožné, dostaneme-li jednu z druhé otočením a převrácením.

*Řešení.* Místo sestav budeme uvažovat barvení jednotlivých políček čtverce. Čili $X$ bude množina všech obarvení čtverce $3 \times 3$ daným počtem barev a $\mathbf{G}$ bude a) grupa všech otočení čtverce, b) grupa všech symetrií čtverce (tj. $\mathbf{G} = \mathbf{D}_8$). Grupa $\mathbf{G}$ působí na $X$ tak, že příslušná permutace otočí/převrátí čtverec i s jeho obarvením. Řešením úlohy je počet orbit tohoto působení (dvě obarvení jsou v jedné orbitě

právě tehdy, když jedno z druhého dostaneme otočením, resp. převrácením). Vyrobíme tabulku, v jejímž prvním sloupci je seznam prvků grupy $\mathbf{G}$, v druhém počet prvků daného typu a ve třetím počet pevných bodů těchto prvků. Pevným bodem se rozumí takové obarvení, které po daném otočení/převrácení vypadá stejně.

| $g$ | # | $\lvert X_g\rvert$ |
|---|---|---|
| $id$ | 1 | 1680 |
| $\circlearrowleft \pm 90°$ | 2 | 0 |
| $\circlearrowleft +180°$ | 1 | 0 |
| osa přes vrcholy | 2 | 36 |
| osa středem hran | 2 | 36 |

Podle Burnsideovy věty je počet obarvení

a) $\frac{1}{4} \cdot (1680 + 2 \cdot 0 + 1 \cdot 0) = 420$,
b) $\frac{1}{8} \cdot (1680 + 2 \cdot 0 + 1 \cdot 0 + 2 \cdot 36 + 2 \cdot 36) = 228$.

□

**Úloha.** Kolik náhrdelníků lze sestavit a) ze tří červených, tří zelených a tří modrých kuliček, b) z šesti žlutých a tří černých kuliček? (Nezáleží na poloze náhrdelníku, je možno jej převracet či otáčet.)

*Řešení.* Místo náhrdelníků budeme uvažovat barvení vrcholů pravidelného devítiúhelníka. Čili $X$, resp. $Y$, budou množiny všech obarvení vrcholů pravidelného devítiúhelníka danými barvami a $\mathbf{G} = \mathbf{D}_{18}$ bude grupa všech symetrií pravidelného devítiúhelníka, která působí na $X$, resp. $Y$, tak, že příslušná permutace otočí/převrátí devítiúhelník i s jeho obarvením. Každé orbitě tohoto působení odpovídá právě jeden náhrdelník (jehož kuličky jsou uspořádány podle toho obarvení). Vyrobíme tabulku podobně jako v předchozí úloze.

| $g$ | # | $\lvert X_g\rvert$ | $\lvert Y_g\rvert$ |
|---|---|---|---|
| $id$ | 1 | 1680 | 84 |
| $\circlearrowleft \pm 1$ | 2 | 0 | 0 |
| $\circlearrowleft \pm 2$ | 2 | 0 | 0 |
| $\circlearrowleft \pm 3$ | 2 | 6 | 3 |
| $\circlearrowleft \pm 4$ | 2 | 0 | 0 |
| osové sym. | 9 | 0 | 4 |

Podle Burnsideovy věty je počet obarvení $\frac{1}{18} \cdot (1680 + 2 \cdot 6) = 94$, resp. $\frac{1}{18} \cdot (84 + 2 \cdot 3 + 9 \cdot 4) = 7$. □

**Úloha.** Kolika způsoby je možné obarvit stěny krychle dvěma barvami? Kolika způsoby lze přiřadit stěnám čísla $1, \ldots, 6$? A kolik existuje hracích kostek, tj. kolika způsoby lze přiřadit čísla $1, \ldots, 6$ tak, že součet protilehlých stěn je sedm? Dvě obarvení/přiřazení považujeme za totožná, pokud lze jedno z druhého dostat otočením krychle.

*Řešení.* Buď $X$ množina všech obarvení stěn krychle dvěma barvami, $Y$ množina všech přiřazení čísel $1, \ldots, 6$ stěnám a $Z$ množina těch přiřazení z $Y$, jejichž protilehlé stěny dávají součet sedm. $\mathbf{G}$ bude grupa všech otočení krychle působící na $X$, $Y$ i $Z$ tak, že příslušná permutace otočí krychli i s jejím obarvením/přiřazením.

Vyrobíme tabulku podobně jako v předchozí úloze.

| $g$ | # | $\lvert X_g\rvert$ | $\lvert Y_g\rvert$ | $\lvert Z_g\rvert$ |
|---|---|---|---|---|
| identita | 1 | $2^6$ | 6! | 48 |
| osa přes středy protilehlých stěn, $\pm 90°$ | 6 | $2^3$ | 0 | 0 |
| osa přes středy protilehlých stěn, $+180°$ | 3 | $2^4$ | 0 | 0 |
| osa přes středy protilehlých hran, $+180°$ | 6 | $2^3$ | 0 | 0 |
| osa přes protilehlé vrcholy, $\pm 120°$ | 8 | $2^2$ | 0 | 0 |

Tedy počty orbit jsou

- $|X/\!\sim| = \frac{1}{24} \cdot (2^6 + 3 \cdot 2^4 + 12 \cdot 2^3 + 8 \cdot 2^2) = 10$,
- $|Y/\!\sim| = \frac{1}{24} \cdot 6! = 30$,
- $|Z/\!\sim| = \frac{1}{24} \cdot 48 = 2$.

Jak známo, hrací kostky jsou dvě, pravotočivá a levotočivá, podle pořadí stěn 1,2,3 při pohledu na příslušný roh kostky. □

Burnsideovu větu lze použít v řadě dalších aplikací, např. pokud chceme zjistit *počet nějakých struktur dané velikosti až na izomorfismus*. Metodu ilustrujeme na grafech s čtyřmi vrcholy. Buď $X$ množina všech grafů s vrcholy $1, 2, 3, 4$. Dva grafy jsou izomorfní, pokud existuje permutace z $\mathbf{S}_4$, která převádí hrany na hrany a mezery na mezery. Uvažujme tedy působení grupy $\mathbf{S}_4$ na $X$ tak, že daná permutace přehází vrcholy i s hranami. Orbity tohoto působení budou obsahovat právě všechny navzájem izomorfní grafy, počet neizomorfních grafů je tedy roven počtu orbit. Řešením je tabulka

| $g$ | # | $\lvert X_g\rvert$ |
|---|---|---|
| $id$ | 1 | $2^6$ |
| (..) | 6 | $2^4$ |
| (..)(..) | 3 | $2^4$ |
| (...) | 8 | $2^2$ |
| (....) | 6 | $2^2$ |

Vidíme, že čtyřprvkových grafů je 11.

Na závěr jedna poučná algebraická aplikace. Působení grupy se nazývá *tranzitivní*, má-li jen jednu orbitu. Podgrupa $\mathbf{G}$ grupy $\mathbf{S}_X$ se nazývá tranzitivní, pokud je tranzitivní její přirozené působení na množinu $X$.

**Příklad.** Grupy $\mathbf{S}_n$, $\mathbf{A}_n$, $\mathbf{D}_{2n}$ jsou tranzitivní. Působení grupy translacemi na svoji nosnou množinu je také tranzitivní. Naopak, působení konjugací tranzitivní není (nejde-li o jednoprvkovou grupu) — jeho orbity jsou právě množiny navzájem konjugovaných prvků. Působení grupy $\mathbf{GL}_n(\mathbf{T})$ na vektorový prostor $\mathbf{T}^n$ tranzitivní není, ale působení téže grupy na množinu $T^n \setminus \{(0, \dots, 0)\}$ už tranzitivní je.

**Věta 18.5** (Jordanova)**.** *Každá alespoň dvouprvková konečná tranzitivní grupa obsahuje alespoň jednu permutaci bez pevného bodu.*

*Důkaz.* Podle Burnsideovy věty je počet orbit roven průměrnému počtu pevných bodů. Z tranzitivity plyne, že počet orbit je 1. Přitom identita má alespoň dva pevné body, tedy *nadprůměrné* množství, musí tedy existovat permutace, která má *podprůměrné* množství pevných bodů. Protože je počet pevných bodů nezáporné celé číslo, jediná podprůměrná hodnota je 0. Tedy existuje permutace bez pevného bodu. □

Působení grupy translacemi i konjugací a Burnsideova věta mají řadu použití v pokročilejší teorii konečných grup. Pomocí působení konjugací lze dokázat např. Sylowovy věty, z nichž snadno plyne např. klasifikace osmiprvkových grup či grup řádu $p^2$ a $2p$.

# Okruhy

## 19. Základní vlastnosti

**Cíl.** *Pojem okruhu vychází ze základních vlastností sčítání a násobení, např. v číselných oborech nebo pro matice. V úvodní sekci pro okruhy adaptujeme pojmy z kapitoly o algebrách (podokruhy, generátory, homomorfismy atd.) a pojem ideálu.*

19.1. **Definice a příklady.**

Obecný pojem komutativního okruhu zavedla Emmy Noetherová ve 20. letech 20. století, aby sjednotila do té doby odděleně se rozvíjející teorie číselných oborů (rozšíření celých a racionálních čísel v oboru komplexních čísel) a oborů polynomů. Třetí významnou rodinu příkladů struktur se sčítáním a násobením tvoří maticové okruhy; ty obecně nejsou komutativní, což vede k formulaci obecného pojmu okruhu. Řada věcí v této kapitole je přímočarým zobecněním analogických faktů ze Sekce 3.

**Definice.** *Okruhem* nazýváme algebru $\mathbf{R} = (R, +, -, \cdot, 0)$ typu $(2, 1, 2, 0)$ splňující následující podmínky:

(1) $(R, +, -, 0)$ je abelovská grupa;
(2) operace $\cdot$ je asociativní;
(3) pro všechna $a, b, c \in R$ platí tzv. *distributivita*

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \text{a} \quad (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

Okruh se nazývá *komutativní*, pokud platí $a \cdot b = b \cdot a$ pro všechna $a, b \in R$.
Říkáme, že okruh má *jednotku*, pokud existuje prvek $1 \in R$ splňující $1 \cdot a = a \cdot 1 = a$ pro všechna $a \in R$.

Tedy *obory integrity* jsou komutativní okruhy s jednotkou splňující $a \cdot b \neq 0$ pro každé $a, b \neq 0$, a *tělesa* jsou komutativní okruhy s jednotkou, kde pro každé $a \neq 0$ existuje $b$ splňující $a \cdot b = 1$.

V okruzích se takřka výhradně používá sada operací $+, -, \cdot, 0$, podobně jako u grup zkracujeme $x - y = x + (-y)$. Často vynecháváme závorky, násobení má vyšší prioritu než sčítání.

**Příklad.** Základní *číselné obory* tvoří okruhy, zejména tedy tělesa $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, obor integrity $\mathbb{Z}$ a okruhy $\mathbb{Z}_n = (\{0, \dots, n-1\}, +_{\bmod n}, -_{\bmod n}, \cdot_{\bmod n}, 0)$ s operacemi modulo $n$. Uvedené příklady jsou komutativní okruhy s jednotkou. Bez jednotky je např. podokruh všech sudých celých čísel.

**Příklad.** Okruh *kvaternionů*

$$\mathbb{H} = (\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}, +, -, \cdot, 0),$$

kde, podobně jako v komplexních číslech, se sčítá po složkách a násobí se podle pravidel uvedených v definici kvaternionové grupy, tj. daný výraz roznásobíme a upravíme podle pravidel

$$i^2 = j^2 = k^2 = -1, \quad ij = -ji = k, \quad ik = -ki = -j, \quad jk = -kj = i.$$

Kvaterniony tvoří nekomutativní okruh s jednotkou, prvky $\pm 1, \pm i, \pm j, \pm k$ tvoří osmiprvkovou kvaternionovou grupu. (Značí se $\mathbb{H}$ podle jejich objevitele Williama Hamiltona.)

**Příklad.** Existuje řada konstrukcí, jak z daného okruhu $\mathbf{R}$ sestrojit další okruhy.

- *Podokruhy* a *direktní součiny*. Mezi důležité příklady patří tzv. *rozšíření* $\mathbf{R}[a_1, \dots, a_n]$, viz níže.
- *Okruhy polynomů* a *formálních mocninných řad n proměnných* nad komutativním okruhem $\mathbf{R}$

$$\mathbf{R}[x_1, \dots, x_n] = (\{ \sum_{k_1,\dots,k_n=0}^{N} a_{k_1,\dots,k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} : \ a_{k_1,\dots,k_n} \in R\}, +, -, \cdot, 0),$$

$$\mathbf{R}[X] = (\{f \in R[x_1, \dots, x_n] : \ n \in \mathbb{N}, x_1, \dots, x_n \in X\}, +, -, \cdot, 0),$$

$$\mathbf{R}[[x_1, \dots, x_n]] = (\{ \sum_{k_1,\dots,k_n=0}^{\infty} a_{k_1,\dots,k_n} x_1^{k_1} \cdot \ldots \cdot x_n^{k_n} : \ a_{k_1,\dots,k_n} \in R\}, +, -, \cdot, 0).$$

  Jde o komutativní okruhy. Jednotku mají právě tehdy, má-li ji $\mathbf{R}$. (Formální definice viz Sekce 3.)
- *Okruh matic* $n \times n$ nad $\mathbf{R}$

$$\mathbf{M}_n(\mathbf{R}) = (\{A : A \text{ je matice } n \times n \text{ nad } \mathbf{R}\}, +, -, \cdot, 0),$$

  kde $+, -, \cdot$ je maticové sčítání, odčítání a násobení a 0 je nulová matice. Okruhy matic jsou zpravidla nekomutativní a má-li $\mathbf{R}$ jednotku, pak je jednotková matice jednotkou v $\mathbf{M}_n(\mathbf{R})$.

**Příklad.** Buď $\mathbf{G}$ abelovská grupa a uvažujme algebru

$$\mathbf{End}(\mathbf{G}) = (\mathrm{End}(\mathbf{G}), +, -, \circ, 0),$$

kde $\mathrm{End}(\mathbf{G})$ značí množinu všech endomorfismů grupy $\mathbf{G}$, sčítání a odčítání endomorfismů je definováno po prvcích, tj. $(f \pm g)(x) = f(x) \pm g(x)$, 0 značí konstantní endomorfismus $x \mapsto 0$ a $\circ$ značí skládání zobrazení. Je snadné ověřit, že se jedná o okruh s jednotkou (obecně nemusí být komutativní).

I pro okruhy na úvod zformulujeme několik jednoduchých faktů.

**Tvrzení 19.1.** *Buď $\mathbf{R}$ okruh, $a, b, c \in R$. Pak*

(1) *pokud $a + c = b + c$, pak $a = b$;*
(2) $a \cdot 0 = 0 \cdot a = 0$;
(3) $-(-a) = a, \quad -(a + b) = -a - b$;
(4) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b), \quad (-a) \cdot (-b) = ab$.

*Důkaz.* Stejně jako Tvrzení 3.1. (Dodatečné vlastnosti oborů integrity se použily jen v bodě (5).) □

Z kapitoly o abelovských grupách adaptujeme „násobení skalárem“, tj. budeme značit

$$n \cdot a = \begin{cases} 0 & n = 0 \\ \underbrace{a + a + \ldots + a}_{n} & n > 0 \\ \underbrace{-a - a - \ldots - a}_{-n} & n < 0 \end{cases}$$

19.2. **Podokruhy.**

Místo podalgeber okruhu $\mathbf{R}$ mluvíme o *podokruzích*. Tedy podmnožina $S \subseteq R$ tvoří podokruh pokruhu $\mathbf{R}$, pokud je uzavřena na všechny operace, tj. pokud $0 \in S$, $-a \in S$, $a + b \in S$ a $a \cdot b \in S$ pro každé $a, b \in S$. Píšeme $\mathbf{S} \leq \mathbf{R}$. Podokruhy $\mathbf{R}$ a $\{0\}$ nazýváme *nevlastní*. Je zřejmé, že podokruhy splňují všechny axiomy okruhů a jsou to tedy také okruhy. Podokruhy komutativních okruhů jsou komutativní, ovšem podokruh nemusí obsahovat jednotku(!).

**Příklad.** Podokruhy okruhu $\mathbb{Z}$ tvoří právě množiny $a\mathbb{Z}$, $a \in \mathbb{Z}$. Protože to musí být podgrupy grupy $(\mathbb{Z}, +, -, 0)$, podle Tvrzení 14.5 jsou $a\mathbb{Z}$ jedinými kandidáty. Není těžké ověřit, že jde o podokruhy. Přitom jednotku obsahuje pouze nevlastní podokruh $\mathbb{Z}$.

Zopakujme, že nejmenší podokruh okruhu $\mathbf{R}$ obsahující danou množinu $X \subseteq R$ se nazývá *podokruh generovaný množinou* $X$ a značí se $\langle X \rangle_{\mathbf{R}}$. Je-li $\mathbf{R}$ okruh, $\mathbf{S}$ jeho podokruh a $a_1, \ldots, a_n \in R$, značíme

$$\mathbf{S}[a_1, \ldots, a_n] = \langle S \cup \{a_1, \ldots, a_n\} \rangle_{\mathbf{R}}$$

a hovoříme o *rozšíření* $\mathbf{S}$ *o prvky* $a_1, \ldots, a_n$. Následující popis prvků takového rozšíření bude velmi důležitý v poslední kapitole o tělesech.

**Tvrzení 19.2.** *Buď* $\mathbf{R}$ *komutativní okruh,* $\mathbf{S}$ *jeho vlastní podokruh a* $a_1, \ldots, a_n \in R$. *Pak*

$$\mathbf{S}[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) : \ f \in S[x_1, \ldots, x_n]\}.$$

*Důkaz.* Označme $M = \{f(a_1, \ldots, a_n) : f \in S[x_1, \ldots, x_n]\}$. Je třeba dokázat, že

(1) množina $M$ obsahuje $S \cup \{a_1, \ldots, a_n\}$,
(2) všechny prvky množiny $M$ lze nagenerovat z prvků množiny $S \cup \{a_1, \ldots, a_n\}$,
(3) množina $M$ je uzavřená na všechny operace okruhu $\mathbf{R}$.

(1) Prvky $S$ dostaneme skrze konstantní polynomy, prvek $a_i$ pomocí polynomu $x_i \in S[x_1, \ldots, x_n]$. (2) Je-li $f = \sum c_{k_1,\ldots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ polynom z $S[x_1, \ldots, x_n]$, pak $f(a_1, \ldots, a_n) = \sum c_{k_1,\ldots,k_n} \cdot a_1^{k_1} \cdot \ldots \cdot a_n^{k_n}$ je prvek podokruhu $\mathbf{S}[a_1, \ldots, a_n]$, neboť jde o součet součinů prvků $c_{k_1,\ldots,k_n} \in S$ a $a_1^{k_1} \cdot \ldots \cdot a_n^{k_n} \in \langle a_1, \ldots, a_n \rangle$. (3) Označme $\bar{a} = (a_1, \ldots, a_n)$. Pak $0 = 0(\bar{a})$ a je-li $f(\bar{a}), g(\bar{a}) \in M$, pak $-f(\bar{a}) = (-f)(\bar{a}) \in M$, $f(\bar{a}) + g(\bar{a}) = (f + g)(\bar{a}) \in M$ a $f(\bar{a}) \cdot g(\bar{a}) = (f \cdot g)(\bar{a}) \in M$. □

**Příklad.**

- Dobře víme, že $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Protože $i^2 = -1 \in \mathbb{Z}$, a tedy $i^k \in \{\pm 1, \pm i\}$ pro všechna $k$, hodnota polynomu $f \in \mathbb{Z}[x]$ v bodě $i$ je rovna nějakému číslu tvaru $a + bi$, $a, b \in \mathbb{Z}$. Tedy

$$\mathbb{Z}[i] = \{f(i) : \ f \in \mathbb{Z}[x]\} = \{f(i) : \ f \in \mathbb{Z}[x], \ \deg f \leq 1\}.$$

- Podobně, protože $(\sqrt[3]{2})^3 \in \mathbb{Z}$, platí

$$\mathbb{Z}[\sqrt[3]{2}] = \{f(\sqrt[3]{2}) :\ f \in \mathbb{Z}[x]\} = \{f(\sqrt[3]{2}) :\ f \in \mathbb{Z}[x],\ \deg f \leq 2\}.$$

- Z podobného důvodu

$$\mathbb{Z}[\sqrt{2},\sqrt{3}] = \{f(\sqrt{2},\sqrt{3}) : f \in \mathbb{Z}[x,y]\} = \{f(\sqrt{2},\sqrt{3}) :\ f = a+bx+cy+dxy \in \mathbb{Z}[x,y]\}.$$

**Poznámka.** Pro komutativní okruhy existuje i relativně dobrý popis prvků obecného podokruhu $\langle X\rangle_{\mathbf{R}}$:

$$\langle X\rangle_{\mathbf{R}} = \{f(a_1,\dots,a_n) :\ n \in \mathbb{N},\ f \in \mathbb{Z}[x_1,\dots,x_n],\ f(0,\dots,0) = 0,\ a_1,\dots,a_n \in X\}.$$

Důkaz se provede podobně jako pro předchozí tvrzení. Hodnotou celočíselného polynomu bez absolutního členu (tj. polynomu splňujícího $f(0,\dots,0) = 0$) na prvku obecného oboru se rozumí výpočet, kde násobení celým číslem interpretujeme jako výše uvedené „násobení skalárem“. Např. je-li $f = 2x^2 + 3x \in \mathbb{Z}[x]$, pak v okruhu $\mathbb{Z}_2$ máme $f(1) = (1^2 + 1^2) + (1 + 1 + 1) = 1$ a v maticovém okruhu $\mathbf{M}_2(\mathbb{R})$ máme $f(\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)) = 2 \cdot \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)^2 + 3 \cdot \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) = 2 \cdot \left(\begin{smallmatrix}2&1\\0&2\end{smallmatrix}\right) + \left(\begin{smallmatrix}3&3\\0&3\end{smallmatrix}\right) = \left(\begin{smallmatrix}7&5\\0&7\end{smallmatrix}\right)$.

19.3. **Ideály.**

**Definice.** Podokruh $\mathbf{I}$ okruhu $\mathbf{R}$ se nazývá *ideál*, pokud navíc splňuje $ra \in I$ a $ar \in I$ pro každé $a \in I$ a každé $r \in R$.

Všimněte si, že $\{0\}$ a $\mathbf{R}$ jsou ideály v libovolném okruhu $\mathbf{R}$; říká se jim *nevlastní*.

Ideály daného okruhu $\mathbf{R}$ tvoří svaz, který se značí $\mathbf{Id}(\mathbf{R})$. Infimem je průnik, supremem nejmenší ideál obsahující sjednocení; důkaz je analogický Tvrzení 11.4. Jak ukazuje následující tvrzení, $\mathbf{I} \vee \mathbf{J} = \mathbf{I} + \mathbf{J}$.

**Tvrzení 19.3.** *Buď $\mathbf{R}$ okruh a $\mathbf{I}_1, \mathbf{I}_2$ jeho ideály. Pak množiny $I_1 \cap I_2$ a $I_1 + I_2 = \{a_1 + a_2 : a_1 \in I_1, a_2 \in I_2\}$ tvoří ideály okruhu $\mathbf{R}$.*

Tyto ideály budeme značit $\mathbf{I}_1 \cap \mathbf{I}_2$ a $\mathbf{I}_1 + \mathbf{I}_2$.

*Důkaz.* Důkaz pro průnik je stejný jako v případě průniku podalgeber (viz Tvrzení 11.1). Uzavřenost součtu ideálů na operace $+, -, 0$ se dokáže stejně jako pro abelovské grupy (viz úvod Sekce 15) a je-li $a_1 + a_2 \in I_1 + I_2$ a $r \in R$, pak $r(a_1 + a_2) = ra_1 + ra_2 \in I_1 + I_2$ a $(a_1 + a_2)r = a_1r + a_2r \in I_1 + I_2$. □

**Tvrzení 19.4.** *Buď $\mathbf{R}$ komutativní okruh a $a \in R$. Pak*

$$aR = \{ar : r \in R\}$$

*tvoří ideál, a to nejmenší ideál obsahující prvek $a$.*

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

*Důkaz.* Nechť $au, av \in aR$ a $r \in R$. Pak $au + av = a(u + v) \in aR$, $-au = a(-u) \in aR$, $0 = a \cdot 0 \in aR$ a $r \cdot au = au \cdot r = a \cdot ur \in aR$. Přitom jakýkoliv ideál $\mathbf{I}$ obsahující prvek $a$ musí obsahovat i všechny jeho $r$-násobky, takže $aR \subseteq I$, a tedy $aR$ je nejmenší ideál obsahující $a$. □

Z předchozích dvou tvrzení plyne, že nejmenší ideál komutativního okruhu $\mathbf{R}$ obsahující prvky $a_1, \dots, a_n$, tzv. *ideál generovaný* $a_1, \dots, a_n$, je ideál

$$a_1R + \cdots + a_nR.$$

Následující fakt je důležitou přísadou metody konstrukce těles, kterou budeme využívat v závěrečné kapitole.

**Tvrzení 19.5.** *Buď* $\mathbf{R}$ *komutativní okruh s jednotkou. Pak* $\mathbf{R}$ *je těleso právě tehdy, když má pouze nevlastní ideály.*

*Důkaz.* ($\Rightarrow$) Buď $\mathbf{I}$ 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 $1 = a \cdot b$. □

Toto tvrzení neplatí pro nekomutativní okruhy: např. okruhy matic $\mathbf{M}_n(\mathbf{T})$, $\mathbf{T}$ těleso, nemají vlastní ideály (těžší cvičení), přesto nejde o (nekomutativní) tělesa. Problém je, že množiny $aR$ obecně nemusí tvořit ideály.

Mohli bychom však uvažovat tzv. jednostranné ideály: podmnožinu $I \subseteq R$ uzavřenou na $+, -, 0$ nazveme *levý ideál* (resp. *pravý ideál*), pokud navíc $ra \in I$ (resp. $ar \in I$) pro každé $a \in I$ a $r \in R$. Pak $aR$ tvoří zaručeně pravý ideál a $Ra$ levý ideál, v každém okruhu. Předchozí tvrzení pak lze formulovat obecněji následujícím způsobem: *Je-li* $\mathbf{R}$ *okruh s jednotkou, pak* $\mathbf{R}$ *je (nekomutativní) těleso* $\Leftrightarrow$ $\mathbf{R}$ *má pouze nevlastní levé ideály* $\Leftrightarrow$ $\mathbf{R}$ *má pouze nevlastní pravé ideály.* Důkaz je zcela analogický původnímu důkazu. Z toho plyne, že ač maticové okruhy mají pouze nevlastní oboustranné ideály, musí nutně obsahovat vlastní jednostranné ideály: jsou jimi např. ideály matic, jejichž vybraný sloupec, resp. řádek, je nulový.

19.4. **Homomorfismy.**

Buď $\mathbf{R}$, $\mathbf{S}$ dva okruhy. Zobrazení $\varphi : R \to S$ je *homomorfismus* těchto okruhů, pokud pro každé $a, b \in R$ platí

$$\varphi(a+b) = \varphi(a) + \varphi(b), \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b), \quad \varphi(-a) = -\varphi(a) \quad \text{a} \quad \varphi(0) = 0.$$

Pojmy *monomorfismus* (neboli *vnoření*), *epimorfismus*, *izomorfismus*, *endomorfismus* a *automorfismus* se používají stejně jako pro obecné algebry. Definujeme

- *jádro* homomorfismu $\varphi$ předpisem
$$\mathrm{Ker}(\varphi) = \{a \in R : \varphi(a) = 0\};$$
- *obraz* homomorfismu $\varphi$ předpisem
$$\mathrm{Im}(\varphi) = \{b \in S : b = \varphi(a) \text{ pro nějaké } a \in R\}.$$

Tedy jádro je blok $[0]$ ekvivalence $\ker(\varphi)$, definice obrazu se shoduje s definicí pro obecné algebry.

**Tvrzení 19.6.** *Buď* $\mathbf{R}$, $\mathbf{S}$ *okruhy a* $\varphi : R \to S$ *zobrazení.*

(1) *Pokud platí pro všechna* $a, b \in R$
$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad a \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),$$
*pak je* $\varphi$ *homomorfismus těchto okruhů.*

(2) *Je-li* $\varphi$ *homomorfismus, pak* $\mathrm{Ker}(\varphi)$ *tvoří ideál v* $\mathbf{R}$ *a* $\mathrm{Im}(\varphi)$ *tvoří podokruh v* $\mathbf{S}$.

(3) *Homomorfismus* $\varphi$ *je prostý právě tehdy, když je* $\mathrm{Ker}(\varphi) = \{0\}$.

*Důkaz.* (1) Plyne okamžitě z Tvrzení 13.4. (2) Jádro tvoří podgrupu vzhledem k operacím $+, -, 0$ podle Tvrzení 13.4. Je-li $\varphi(a) = 0$ a $r \in R$ libovolné, pak $\varphi(a \cdot r) = \varphi(a) \cdot \varphi(r) = 0 \cdot \varphi(r) = 0$ a $\varphi(r \cdot a) = \varphi(r) \cdot \varphi(a) = \varphi(r) \cdot 0 = 0$, tedy $\mathrm{Ker}(\varphi)$ tvoří ideál. Pro obraz stačí použít obecné Tvrzení 11.5. (3) Viz Tvrzení 13.4. □

**Poznámka.** Připomeňme, že je-li $f = \sum_{i=1}^{n} a_i x^i$ polynom z $R[x]$ a $u \in R$, pak výrazem $f(u)$ rozumíme hodnotu polynomu $f$ na $u$, tj. prvek $f(u) = \sum_{i=1}^{n} a_i u^i \in R$. Formálně vzato, dosazování do polynomu je homomorfismus

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

Nazývá se *dosazovací homomorfismus.*

*Direktní součin* okruhů definujeme stejně jako pro obecné algebry, tj. nosnou množinou je kartézský součin nosných množin jednotlivých okruhů a operace provádíme po složkách. I pro okruhy platí algebraická verze Čínské věty o zbytcích.

**Tvrzení 19.7.** *Buď $m_1, \ldots, m_n$ po dvou nesoudělná přirozená čísla, označme $M = m_1 \cdot \ldots \cdot m_n$. Pak*

$$\mathbb{Z}_M \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_n}.$$

*Důkaz.* Jako pro grupy, viz Tvrzení 13.5. Je vidět, že uvedené zobrazení zachovává i násobení. □

19.5. **Charakteristika okruhu.**

Buď $\mathbf{R}$ okruh s jednotkou. Jeho *charakteristikou* rozumíme nejmenší $n \in \mathbb{N}$ takové, že

$$n \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{n} = 0,$$

pokud takové $n$ existuje, resp. 0 v opačném případě. Je-li $\mathbf{R}$ obor integrity (nebo dokonce těleso), pak je charakteristika zaručeně 0 nebo prvočíslo: kdyby $n = a \cdot b$, pak bychom měli $n \cdot 1 = (a \cdot 1) \cdot (b \cdot 1) = 0$, tedy $a \cdot 1 = 0$ nebo $b \cdot 1 = 0$, což by byl spor s minimalitou.

*Prvookruhem* okruhu $\mathbf{R}$ s jednotkou se rozumí podokruh generovaný prvkem 1. Uvažujme zobrazení

$$\mathbb{Z} \to \mathbf{R}, \qquad n \mapsto n \cdot 1.$$

Zřejmě jde o homomorfismus, jehož obrazem je prvookruh okruhu $\mathbf{R}$. Jeho jádro je ideál $n\mathbb{Z}$, kde $n$ je charakteristika okruhu $\mathbf{R}$. Použijeme-li 1. větu o izomorfismu, kterou dokážeme v příští kapitole, můžeme dedukovat, že prvookruh je izomorfní buď okruhu $\mathbb{Z}$ v případě charakteristiky 0, nebo $\mathbb{Z}/n \simeq \mathbb{Z}_n$ v případě charakteristiky $n$. Zpravidla se prvek $n \cdot 1$ ztotožňuje s číslem $n \in \mathbb{Z}$ a v tom případě můžeme uvažovat, že $\mathbb{Z}$, resp. $\mathbb{Z}_n$, je podokruhem libovolného okruhu s jednotkou.

**Tvrzení 19.8.** *Buď $\mathbf{R}$ okruh s jednotkou prvočíselné charakteristiky $p$. Pak*

$$\varphi_p : \mathbf{R} \to \mathbf{R}, \qquad a \mapsto a^p$$

*je homomorfismus.*

Říká se mu *Frobeniův endomorfismus.*

*Důkaz.* Zřejmě $(a \cdot b)^p = a^p \cdot b^p$ a podle binomické věty

$$(a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p,$$

neboť $p$ dělí $\binom{p}{i}$ pro každé $i \neq 0, p$. □

**Důsledek 19.9.** *Je-li $\mathbf{T}$ konečné těleso charakteristiky $p$, pak je $\varphi_p$ jeho automorfismus.*

*Důkaz.* Protože podle Tvrzení 19.5 tělesa nemají žádné vlastní ideály, musí být jádro $\varphi_p$ triviální, tedy jde o prosté zobrazení a podle Lemmatu 1.2 je to bijekce. □

Frobeniovy automorfismy hrají v teorii konečných těles důležitou roli.

## 20. * Moduly

**Cíl.** *Uvažujme definici vektorového prostoru, ve které těleso nahradíme obecným okruhem; takové struktuře se říká modul. Alternativně, moduly lze považovat za reprezentace okruhů pomocí endomorfismů abelovských grup. V této sekci se seznámíme s několika příklady a základními pojmy teorie modulů.*

**Definice.** *Levým modulem nad okruhem* $\mathbf{R} = (R, +_{\mathbf{R}}, -_{\mathbf{R}}, \cdot_{\mathbf{R}}, 0)$, krátce $\mathbf{R}$*-modulem*, rozumíme algebru $\mathbf{M} = (M, +, -, 0, (r\cdot) : r \in R)$ typu $(2, 1, 0, 1, 1, 1, \dots)$ splňující následující podmínky:

(1) $(M, +, -, 0)$ je abelovská grupa;
(2) pro každé $r, s \in R$ a $m, m_1, m_2 \in M$ platí

$$r\cdot(m_1+m_2) = r\cdot m_1 + r\cdot m_2, \quad (r+_{\mathbf{R}} s)\cdot m = r\cdot m + s\cdot m, \quad (r\cdot_{\mathbf{R}} s)\cdot m = r\cdot(s\cdot m).$$

(Abychom odlišili sčítání a násobení v okruhu od sčítání a skalárního násobení v modulu, pro okruhové operace doplňujeme indexy.)

*Pravé* $\mathbf{R}$*-moduly* se definují analogicky a můžeme dokonce definovat *bimoduly*, kde je k dispozici násobení z obou stran, přičemž se předpokládá $r\cdot(m\cdot s) = (r\cdot m)\cdot s$. (Pro komutativní okruhy samozřejmě není rozdíl mezi levým a pravým modulem.)

Podmínka (2) je ekvivalentní faktu, že zobrazení

$$\varphi : \mathbf{R} \to \mathbf{End}(M, +, -, 0), \qquad r \mapsto (r\cdot)$$

je homomorfismus okruhů (připomeňme, že operace okruhu $\mathbf{End}(M, +, -, 0)$ jsou sčítání po bodech a skládání zobrazení): první rovnost říká, že $(r\cdot)$ je endomorfismus abelovské grupy $(M, +, -, 0)$, druhá říká, že $\varphi$ zachovává sčítání v obou okruzích, a třetí se překládá na zachování násobení. Jinými slovy, moduly jsou reprezentace okruhů pomocí endomorfismů abelovských grup.

**Příklad.**

- Je-li $\mathbf{T}$ těleso, pak $\mathbf{T}$-moduly jsou přesně vektorové prostory nad $\mathbf{T}$.
- Vektorový prostor $\mathbf{T}^n$ lze považovat také za $\mathbf{M}_n(\mathbf{T})$-modul, skalární násobení je jednoduše násobení vektoru maticí (sloupcového zleva, resp. řádkového zprava). Ihned vidíme, že jde o modul, protože matice odpovídají lineárním zobrazením (endomorfismům) na vektorovém prostoru $\mathbf{T}^n$ a násobení matic odpovídá skládání příslušných endomorfismů. Levý a pravý modul jsou v tomto případě odlišné struktury.
- Abelovskou grupu lze považovat za $\mathbb{Z}$-modul, skalární násobení je definováno $n \cdot a = a + \dots + a$, resp. $-a - a - \dots - a$, analogicky jako pro grupy.
- Libovolný okruh $\mathbf{R}$ lze považovat za levý (resp. pravý) $\mathbf{R}$-modul, pokud vezmeme levé (resp. pravé) translace vzhledem k násobení (tj. $r \cdot s = r \cdot_{\mathbf{R}} s$, resp. $s\cdot r = s\cdot_{\mathbf{R}} r$). Uvědomte si, že pro nekomutativní okruh pravé translace nedefinují levý modul a naopak! (Selže poslední rovnost.)

- Buď $\mathbf{R}$ okruh, $X$ množina a uvažujme množinu $R^X$ všech zobrazení $X \to R$. Definujeme-li operace

$$(f+g)(x) = f(x) + g(x), \qquad (r \cdot f)(x) = r \cdot f(x),$$

dostaneme tzv. *volný* $\mathbf{R}$*-modul nad* $X$.

Místo podalgeber modulu $\mathbf{M}$ mluvíme o *podmodulech*. Tedy podmnožina $K \subseteq M$ tvoří podmodul modulu $\mathbf{M}$, pokud je uzavřena na všechny operace, tj. pokud $0 \in K$, $-a \in K$, $a + b \in K$ a $r \cdot a \in K$ pro každé $a, b \in K$ a $r \in R$. Píšeme $\mathbf{K} \leq \mathbf{M}$.

Podobně se adaptuje pojem direktního součinu (v této souvislosti se spíše používá termín *direktní suma*) a *homomorfismu*. Tedy díky Tvrzení 13.4 je zobrazení $\varphi : M \to N$ homomorfismem modulů $\mathbf{M} \to \mathbf{N}$, pokud pro každé $a, b \in M$ a $r \in R$ platí

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{a} \quad \varphi(r \cdot a) = r \cdot \varphi(a)$$

podobně jako pro vektorové prostory (pozor na druhou podmínku!). Analogicky definujeme

- *jádro* homomorfismu $\varphi$ předpisem

$$\mathrm{Ker}(\varphi) = \{a \in M : \varphi(a) = 0\};$$

- *obraz* homomorfismu $\varphi$ předpisem

$$\mathrm{Im}(\varphi) = \{b \in N : b = \varphi(a) \text{ pro nějaké } a \in M\}.$$

Opět je snadné dokázat, že $\mathrm{Ker}(\varphi)$ tvoří podmodul $\mathbf{M}$, $\mathrm{Im}(\varphi)$ tvoří podmodul $\mathbf{N}$ a $\varphi$ je prostý právě tehdy, když je $\mathrm{Ker}(\varphi) = \{0\}$.

**Příklad.**

- Podmoduly vektorových prostorů odpovídají podprostorům, homomorfismy lineárním zobrazením.
- Je celkem zřejmé, že $\mathbf{M}_n(\mathbf{T})$-modul $\mathbf{T}^n$ má pouze nevlastní podmoduly. Při vhodném pohledu je vidět, že endomorfismy tohoto modulu jsou právě centrální endomorfismy vektorového prostoru $\mathbf{T}^n$ (tj. ty, které komutují se všemi ostatními endomorfismy).
- Podmoduly abelovských grup jako $\mathbb{Z}$-modulů odpovídají podgrupám, homomorfismy homomorfismům abelovských grup.
- Podmoduly okruhu $\mathbf{R}$ považovaného za levý (resp. pravý) $\mathbf{R}$-modul odpovídají levým (resp. pravým) ideálům. Pokud jej považujeme za $\mathbf{R}$-bimodul, pak odpovídají *ideálům*.

Na závěr uvedeme ještě jeden pojem, se kterým se čtenář může v budoucnu setkat.

**Definice.** Buď $\mathbf{T}$ těleso. Okruh $\mathbf{R}$ se nazývá $\mathbf{T}$*-algebra*, je-li zároveň vektorovým prostorem nad tělesem $\mathbf{T}$ a platí

$$t \cdot (r \cdot_{\mathbf{R}} s) = r \cdot_{\mathbf{R}} (t \cdot s) = (t \cdot r) \cdot_{\mathbf{R}} s$$

pro každé $t \in T$ a $r, s \in R$.

**Příklad.**

- Je-li $\mathbf{S}$ těleso a $\mathbf{T}$ jeho podtěleso, pak $\mathbf{S}$ je $\mathbf{T}$-algebra.
- Libovolný maticový okruh $\mathbf{R} \leq \mathbf{M}_n(\mathbf{T})$ je $\mathbf{T}$-algebra dimenze $\leq n$.

- Libovolný okruh polynomů $\mathbf{R} \leq \mathbf{T}[X]$ je $\mathbf{T}$-algebra (nekonečné dimenze, pokud $\mathbf{R} \neq \mathbf{T}$).

**Příklad.** Buď $\mathbf{T}$ těleso a $\mathbf{G} = (V, E)$ orientovaný graf, označme $P$ množinu všech orientovaných cest v grafu $\mathbf{G}$. Definujeme tzv. *algebru cest*: bude to vektorový prostor $\mathbf{T}^{V \cup P}$ na množině $T^{V \cup P} = \{\sum_{v \in V} a_v v + \sum_{p \in P} a_p p : a_v, a_p \in T\}$, na kterém dodefinujeme násobení následujícím způsobem: pro dvě cesty $p_1, p_2$, součin $p_1 \cdot p_2$ bude cesta vzniklá jejich složením, pokud na sebe navazují, resp. 0 v opačném případě; pro cestu $p$ a vrchol $v$, součin $v \cdot p$ bude $p$, pokud tato cesta začíná ve vrcholu $v$, resp. 0 v opačném případě, a součin $p \cdot v$ bude $p$, pokud tato cesta končí ve vrcholu $v$, resp. 0 v opačném případě; součin $v_1 \cdot v_2$ dvou vrcholů bude buď $v_1 = v_2$, jsou-li totožné, nebo 0 v opačném případě. Na obecné prvky vektorového prostoru $\mathbf{T}^{V \cup P}$ se pak násobení rozšíří pomocí distributivity.

Tímto způsobem lze reprezentovat řadu dobře známých algeber. Např. $\mathbf{T}$-algebra $\mathbf{T}[x_1, \ldots, x_n]$ je izomorfní algebře cest grafu s $n$ vrcholy a smyčkou u každého vrcholu. $\mathbf{T}$-algebra horních trojúhelníkových matic $n \times n$ je izomorfní algebře cest grafu $\bullet \to \bullet \to \ldots \to \bullet$ s $n$ vrcholy.

**Příklad.** Kvaterniony tvoří nekomutativní $\mathbb{R}$-algebru dimenze 4.

## Faktoralgebry

Koncept faktorobjektu se objevuje v celé strukturní matematice, s větším či menším významem. Zcela zásadní význam má pro algebru.

Myšlenka je následující: vyrobme z jemného objektu hrubší objekt tak, že některé prvky budeme považovat za totožné. 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 strukturu objektu původního (tj. z jednotlivých prvků).

Formálně, buď $A$ množina s nějakou strukturou (algebra, topologický prostor, graf, atd.) a $\sim$ vhodná ekvivalence na $A$. (Tato ekvivalence popisuje, které prvky ztotožníme.) Faktorobjekt bude mít za nosnou množinu $A/\!\sim = \{[a]_\sim : a \in A\}$, tj. množinu všech bloků této ekvivalence. Strukturu pak přetáhneme na bloky tak, že blok $[a]$ bude simulovat roli prvku $a$.

### 21. Faktorgrupy

**Cíl.** *Operace dané grupy můžeme přenést na množinu rozkladových tříd její normální podgrupy; tak dostaneme tzv. faktorgrupu. Ukážeme si, jak rozpoznat strukturu takové faktorgrupy.*

Buď $\mathbf{G} = (G, \cdot, ^{-1}, e)$ grupa a $\mathbf{H}$ její normální podgrupa. Definujeme relaci

$$a \sim b \quad \Leftrightarrow \quad a \cdot b^{-1} \in H.$$

Podle Lemmatu 17.2 je $a \sim b$ právě tehdy, když $Ha = Hb$, a tedy z Lemmatu 17.1 plyne, že relace $\sim$ je ekvivalence. Její bloky jsou rozkladové třídy grupy $\mathbf{G}$ podle podgrupy $\mathbf{H}$, a protože je $\mathbf{H}$ normální, levé i pravé rozkladové třídy jsou totéž, tj.

$$[a] = aH = Ha.$$

Na těchto blocích definujeme operace předpisy

$$[a] \cdot [b] := [a \cdot b] \qquad \text{a} \qquad [a]^{-1} := [a^{-1}].$$

Měli bychom samozřejmě ověřit, že je tato definice korektní, tzn. že výsledek operace nezávisí na tom, kterým prvkem si daný blok označíme. Předpokládejme tedy $[a] = [c]$ a $[b] = [d]$, ověříme, že $[a \cdot b] = [c \cdot d]$ a $[a^{-1}] = [b^{-1}]$. Protože $a \sim c$ a $b \sim d$, tj. $a \cdot c^{-1} \in H$ a $b \cdot d^{-1} \in H$, z uzavřenosti množiny $H$ na násobení i konjugaci libovolným prvkem (Tvrzení 17.7) dostáváme

$$(ab) \cdot (cd)^{-1} = abd^{-1}c^{-1} = ac^{-1}cbd^{-1}c^{-1} = \underbrace{(ac^{-1})}_{\in H} \cdot \underbrace{c(bd^{-1})c^{-1}}_{\in H} \in H$$

a podobně také

$$a^{-1} \cdot (c^{-1})^{-1} = a^{-1}c = a^{-1}ca^{-1}a = a^{-1}\underbrace{(ac^{-1})^{-1}}_{\in H}a \in H,$$

čili $a \cdot b \sim c \cdot d$ a $a^{-1} \sim b^{-1}$, tj. $[a \cdot b] = [c \cdot d]$ a $[a^{-1}] = [b^{-1}]$.

Uvažujme nyní algebru

$$\mathbf{G}/\mathbf{H} = (\{[a] : a \in G\}, \cdot, ^{-1}, [e]).$$

Operace $\cdot$ je očividně asociativní, neboť $[a] \cdot ([b] \cdot [c]) = [a \cdot (b \cdot c)] = [(a \cdot b) \cdot c] = ([a] \cdot [b]) \cdot [c]$, a podobně se ověří i $[a] \cdot [e] = [a \cdot e] = [a] = [e \cdot a] = [e] \cdot [a]$ a $[a] \cdot [a]^{-1} = [a \cdot a^{-1}] = [e] = [a]^{-1} \cdot [a]$. Algebra $\mathbf{G}/\mathbf{H}$ je tedy grupa, tzv. *faktorgrupa grupy* $\mathbf{G}$ *podle podgrupy* $\mathbf{H}$.

**Příklad.** Připomeňme rozklad

- grupy $\mathbb{Z}$ podle normální podgrupy $n\mathbb{Z}$, jehož rozkladové třídy jsou právě množiny $[a] = \{k \in \mathbb{Z} : k \equiv a \pmod n\}$, $a = 0, \dots, n-1$. Faktorgrupa $\mathbb{Z}/n\mathbb{Z}$ tedy má $n$ prvků, přičemž $[a] + [b] = [a + b] = [a + b \bmod n]$ a $-[a] = [-a] = [n - a]$. Vidíme, že operace na prvcích $\mathbb{Z}/n\mathbb{Z}$ jsou jako operace na číslech $0, \dots, n-1$ modulo $n$. Jinými slovy, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.
- grupy $\mathbf{S}_n$ podle normální podgrupy $\mathbf{A}_n$, jenž má dvě rozkladové třídy, a to množinu $S$ sudých permutací a množinu $L$ lichých permutací. Operace na těchto třídách je $S \circ S = L \circ L = S$ a $S \circ L = L \circ S = L$. Jde o dvouprvkovou grupu.

**Věta 21.1** (o homomorfismu)**.** *Je-li* $\varphi : \mathbf{G} \to \mathbf{H}$ *homomorfismus grup a* $\mathbf{N}$ *normální podgrupa grupy* $\mathbf{G}$ *taková, že* $\mathbf{N} \subseteq \mathbf{Ker}(\varphi)$*, pak je zobrazení*

$$\psi : \mathbf{G}/\mathbf{N} \to \mathbf{H}, \qquad [a] \mapsto \varphi(a)$$

*homomorfismus.*

*Důkaz.* Předně je třeba ověřit, že je $\psi$ zobrazení: mohlo by se stát, že tentýž blok máme označen dvěma různými způsoby, tj. že $[a] = [b]$ pro nějaká $a \neq b$, a přitom se těmto blokům snažíme přiřadit dvě různé hodnoty $\varphi(a), \varphi(b)$. Ovšem

$$[a] = [b] \;\Leftrightarrow\; a \cdot b^{-1} \in N \;\Rightarrow\; a \cdot b^{-1} \in \mathrm{Ker}(\varphi) \;\Leftrightarrow\; \varphi(a \cdot b^{-1}) = e \;\Leftrightarrow\; \varphi(a) = \varphi(b).$$

Tedy $\psi$ je dobře definované zobrazení, a protože $\psi([a \cdot b]) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = \psi([a]) \cdot \psi([b])$, je to homomorfismus. □

**Důsledek 21.2** (1. věta o izomorfismu)**.** *Je-li* $\varphi : \mathbf{G} \to \mathbf{H}$ *homomorfismus grup, pak*

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

*Důkaz.* Dosaďte do Věty o homomorfismu $\mathbf{N} = \mathbf{Ker}(\varphi)$. Výsledný homomorfismus je prostý, neboť

$$[a] = [b] \;\Leftrightarrow\; a \cdot b^{-1} \in \mathrm{Ker}(\varphi) \;\Leftrightarrow\; \varphi(a \cdot b^{-1}) = e \;\Leftrightarrow\; \varphi(a) = \varphi(b),$$

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

Často se uvádějí ještě dva důsledky věty o homomorfismu. Protože pro ně nebudeme mít dalšího využití a jejich důkazy nejsou těžké, zato však dosti technické, přenecháváme je čtenáři.

**Důsledek 21.3** (2. věta o izomorfismu)**.** *Buď* $\mathbf{G}$ *grupa a* $\mathbf{H}$*,* $\mathbf{K}$ *její normální podgrupy takové, že* $\mathbf{K} \leq \mathbf{H}$*. Pak* $\mathbf{K} \trianglelefteq \mathbf{H}$*,* $\mathbf{H}/\mathbf{K} \trianglelefteq \mathbf{G}/\mathbf{K}$ *a*

$$(\mathbf{G}/\mathbf{K})/(\mathbf{H}/\mathbf{K}) \simeq \mathbf{G}/\mathbf{H}.$$

**Důsledek 21.4** (3. věta o izomorfismu)**.** *Buď* $\mathbf{G}$ *grupa,* $\mathbf{H}$ *její normální podgrupa a* $\mathbf{K}$ *její libovolná podgrupa. Pak* $HK = \{hk : h \in H, k \in K\}$ *tvoří podgrupu grupy* $\mathbf{G}$*,* $\mathbf{H} \cap \mathbf{K} \trianglelefteq \mathbf{K}$ *a*

$$\mathbf{HK}/\mathbf{H} \simeq \mathbf{K}/(\mathbf{H} \cap \mathbf{K}).$$

1. věta o izomorfismu je dobrý nástroj, pokud chceme vyšetřit, jak vypadá daná faktorgrupa. Chceme-li dokázat, že $\mathbf{G}/\mathbf{N} \simeq \mathbf{H}$, stačí najít homomorfismus $\mathbf{G}$ na $\mathbf{H}$, jehož jádro je $\mathbf{N}$.

**Příklad.**

- Uvažujme $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $x \mapsto x \bmod n$. Jde samozřejmě o homomorfismus na, jehož jádro je $\{x : x \bmod n = 0\} = n\mathbb{Z}$. Tedy podle 1. věty o izomorfismu

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

- Uvažujme $\varphi : \mathbf{S}_n \to \mathbb{Z}^*$, který permutaci přiřadí její znaménko. Známý součinový vzorec říká, že jde o homomorfismus, je očividně na a jeho jádro sestává ze sudých permutací. Tedy podle 1. věty o izomorfismu

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

- Jak vypadá faktorgrupa $\mathbf{GL}_n(\mathbf{T})/\mathbf{SL}_n(\mathbf{T})$? Dvě matice jsou ekvivalentní, tj. $A \sim B$, právě tehdy, když $AB^{-1} \in \mathrm{SL}_n(T)$, tj. právě tehdy, když $\det AB^{-1} = \det A \cdot \frac{1}{\det B} = 1$, tj. právě tehdy, když $\det A = \det B$. Za reprezentanty bloků si tedy můžeme zvolit nenulové prvky tělesa $\mathbf{T}$ a zkusíme dokázat, že příslušná faktorgrupa je izomorfní grupě $\mathbf{T}^*$.
  Uvažujme zobrazení $\varphi : \mathbf{GL}_n(\mathbf{T}) \to \mathbf{T}^*$, $A \mapsto \det A$. Ze součinového vzorce $\det AB = \det A \cdot \det B$ plyne, že jde o homomorfismus. Jeho jádro sestává z matic s determinantem 1, tj. $\mathbf{Ker}(\varphi) = \mathbf{SL}_n(\mathbf{T})$. Tedy podle 1. věty o izomorfismu

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

- Jak vypadá faktorgrupa $\mathbf{S}_4/\mathbf{H}$, kde $\mathbf{H}$ je Kleinova podgrupa? Protože $|S_4| = 24$ a $|H| = 4$, podle Lagrangeovy věty je $|S_4/H| = 6$, tedy tato faktorgrupa je izomorfní buď s grupou $\mathbf{S}_3$, nebo s cyklickou grupou $\mathbb{Z}_6$. Dokážeme, že grupa $\mathbf{S}_4/\mathbf{H}$ není abelovská, tudíž je správně první možnost:

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

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

**Poznámka.** Pomocí 1. věty o izomorfismu lze provést přehlednější důkaz klasifikace cyklických grup (Věta 14.4). Buď $\mathbf{G} = \langle a \rangle$ cyklická grupa a uvažujme zobrazení

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

Jistě $\mathbf{Im}(\varphi) = \mathbf{G}$. Je-li zobrazení prosté, pak $\mathbf{G} \simeq \mathbb{Z}$. V opačném případě je $\mathbf{Ker}(\varphi) = n\mathbb{Z}$, kde $n = \mathrm{ord}(a)$, a podle 1. věty o izomorfismu $\mathbf{G} \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$.

## 22. Faktorokruhy

**Cíl.** *Operace daného okruhu můžeme přenést na množinu rozkladových tříd jeho ideálu; tak dostaneme tzv. faktorokruh. Ukážeme si, jak rozpoznat strukturu takového faktorokruhu. Jako aplikaci získáme důležitou metodu konstrukce těles jako faktorokruhů podle maximálního ideálu. Na závěr si ukážeme, jak se dá zobecnění Čínská věta o zbytcích z celých čísel na libovolné komutativní okruhy.*

22.1. **Konstrukce faktorokruhu.**
Buď $\mathbf{R}$ okruh a $\mathbf{I}$ jeho ideál. Definujeme relaci

$$a \sim b \quad \Leftrightarrow \quad a - b \in I.$$

Protože je $(R, +, -, 0)$ abelovská grupa a $(I, +, -, 0)$ její (normální) podgrupa, relace $\sim$ je ekvivalence a její bloky jsou rozkladové třídy této podgrupy, tj.

$$[a] = a + I.$$

Na těchto blocích definujeme operace předpisy

$$[a] + [b] := [a + b], \qquad -[a] := [-a] \qquad \text{a} \qquad [a] \cdot [b] := [a \cdot b].$$

Díky sekci o faktorgrupách již víme, že operace $+, -$ jsou definovány korektně, zbývá ověřit korektnost pro násobení. Předpokládejme tedy $[a] = [c]$ a $[b] = [d]$, dokážeme, že $[a \cdot b] = [c \cdot d]$. Protože $a \sim c$ a $b \sim d$, tj. $a - c \in I$ a $b - d \in I$, máme také $(a - c) \cdot b \in I$ a $c \cdot (b - d) \in I$, a tedy $(a - c) \cdot b + c \cdot (b - d) = a \cdot b - c \cdot d \in I$. Čili $a \cdot b \sim c \cdot d$ a $[a \cdot b] = [c \cdot d]$.

Uvažujme nyní algebru

$$\mathbf{R}/\mathbf{I} = (\{[a] : a \in R\}, +, -, \cdot, [0]).$$

Podobně jako pro faktorgrupy je snadné ověřit, že jde o okruh, tzv. *faktorokruh okruhu* $\mathbf{R}$ *podle ideálu* $\mathbf{I}$.

**Věta 22.1** (o homomorfismu)**.** *Je-li* $\varphi : \mathbf{R} \to \mathbf{S}$ *homomorfismus okruhů a* $\mathbf{I}$ *ideál okruhu* $\mathbf{R}$ *takový, že* $\mathbf{I} \subseteq \mathbf{Ker}(\varphi)$*, pak je zobrazení*

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

*homomorfismus.*

*Důkaz.* Stejně jako pro grupy. (Viz též obecný případ 23.1.) □

**Důsledek 22.2** (1. věta o izomorfismu)**.** *Je-li* $\varphi : \mathbf{R} \to \mathbf{S}$ *homomorfismus okruhů, pak*

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

**Důsledek 22.3** (2. věta o izomorfismu)**.** *Buď* $\mathbf{R}$ *okruh a* $\mathbf{I}$*,* $\mathbf{J}$ *jeho ideály takové, že* $\mathbf{J} \leq \mathbf{I}$*. Pak* $\mathbf{J}$ *je ideál v* $\mathbf{I}$*,* $\mathbf{I}/\mathbf{J}$ *je ideál v* $\mathbf{R}/\mathbf{J}$ *a*

$$(\mathbf{R}/\mathbf{J})/(\mathbf{I}/\mathbf{J}) \simeq \mathbf{R}/\mathbf{I}.$$

**Důsledek 22.4** (3. věta o izomorfismu)**.** *Buď* $\mathbf{R}$ *okruh,* $\mathbf{I}$ *jeho ideál a* $\mathbf{S}$ *jeho podokruh. Pak* $S + I = \{s + i : s \in S, i \in I\}$ *tvoří podokruh okruhu* $\mathbf{R}$ *a*

$$(\mathbf{S} + \mathbf{I})/\mathbf{I} \simeq \mathbf{S}/(\mathbf{S} \cap \mathbf{I}).$$

**Příklad.** Jak vypadá faktorokruh $\mathbb{Z}[x]/\mathbf{I}$, kde $I = \{f \in \mathbb{Z}[x] : 3 \mid f(0)\}$? Dva polynomy jsou ekvivalentní, tj. $f \sim g$, právě tehdy, když $f - g \in I$, tj. právě tehdy, když $3 \mid f(0) - g(0)$, tj. právě tehdy, když $f(0) \equiv g(0) \pmod 3$. Existují tedy přesně tři rozkladové třídy a podle 1. věty o izomorfismu je

$$\mathbb{Z}[x]/\mathbf{I} \simeq \mathbb{Z}_3,$$

jak dokazuje homomorfismus $\varphi : \mathbb{Z}[x] \to \mathbb{Z}_3$, $f \mapsto f(0) \bmod 3$.

Zvláště důležitý je případ, kdy $\mathbf{R}$ je komutativní okruh a $\mathbf{I}$ jeho *hlavní* ideál. Je-li $I = mR$, zapisujeme faktorokruh zkráceně $\mathbf{R}/m$. Jak takový faktorokruh vypadá? Dva prvky jsou ekvivalentní, tj. $a \sim b$, právě tehdy, když $a - b \in mR$, tj. právě tehdy, když $m \mid a - b$, tj. právě tehdy, když $a \equiv b \pmod m$. Je-li v okruhu $\mathbf{R}$ definováno dělení se zbytkem, prvky $\mathbf{R}/m$ můžeme reprezentovat pomocí zbytků po dělení $m$ a operace v $\mathbf{R}/m$ fungují 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.** Podobně jako pro grupy, prvky faktorokruhu $\mathbb{Z}/n$ můžeme reprezentovat jako zbytky po dělení číslem $n$, tj. jako čísla $0, \ldots, n-1$, přičemž operace provádíme modulo $n$. Dosadíme-li do 1. věty o izomorfismu homomorfismus $\varphi : \mathbb{Z} \to \mathbb{Z}_n$, $x \mapsto x \bmod n$, jehož jádro je ideál $n\mathbb{Z}$, dostaneme

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

(Vzpomeňte na aplikaci tohoto pozorování při charakterizaci prvookruhů.)

**Příklad.** Nejdůležitější pro nás budou faktorkruhy oborů polynomů.

- Prvky faktorokruhu $\mathbb{Z}[x]/x-1$ můžeme reprezentovat jako zbytky po dělení polynomem $x - 1$, tj. jako konstatní polynomy, přičemž operace provádíme modulo polynom $x - 1$. Dosadíme-li do 1. věty o izomorfismu homomorfismus $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$, $f \mapsto f(1)$, jehož jádro je

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

  dostaneme

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

- Prvky faktorokruhu $\mathbb{Z}[x]/x^2 - 1$ můžeme reprezentovat jako zbytky po dělení polynomem $x^2 - 1$, tj. jako polynomy stupně $\leq 1$, přičemž operace provádíme modulo polynom $x^2 - 1$. Dosadíme-li do 1. věty o izomorfismu homomorfismus $\varphi : \mathbb{Z}[x] \to \mathbb{Z} \times \mathbb{Z}$, $f \mapsto (f(1), f(-1))$, jehož jádro je

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

  dostaneme

  $$\mathbb{Z}[x]/x^2 - 1 \simeq \mathbb{Z} \times \mathbb{Z}.$$

- Prvky faktorokruhu $\mathbb{Z}[x]/x^2+1$ můžeme reprezentovat analogicky, ovšem dostaneme zcela odlišný okruh. Dosadíme-li do 1. věty o izomorfismu homomorfismus $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[i]$, $f \mapsto f(i)$, jehož jádro je

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

  dostaneme

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

**Poznámka.** Analogicky jako pro grupy a okruhy lze definovat faktormodul daného $\mathbf{R}$-modulu podle podmodulu. Konkrétně, je-li $\mathbf{M}$ modul a $\mathbf{K}$ jeho podmodul, definujeme relaci

$$a \sim b \quad \Leftrightarrow \quad a - b \in K.$$

Dokažte sami, že jde o ekvivalenci, že jsou modulové operace na třídách ekvivalence dobře definovány a dokažte věty o homomorfismu a izomorfismu.

22.2. **Maximální ideály a konstrukce těles.**

Ideál $\mathbf{I}$ okruhu $\mathbf{R}$ nazveme *maximální*, pokud je $\mathbf{I}$ maximální v uspořádané množině vlastních ideálů, tj. pokud neexistuje ideál $\mathbf{J}$ splňující $I \subset J \subset R$. Konstrukce těles založená na následující větě nachází velkého použití v závěrečné kapitole i v pokročilejší teorii těles.

**Věta 22.5.** *Je-li $\mathbf{R}$ komutativní okruh s jednotkou a $\mathbf{I}$ jeho maximální ideál, pak je faktorokruh $\mathbf{R}/\mathbf{I}$ těleso.*

*Důkaz.* Podle Tvrzení 19.5 stačí dokázat, že okruh $\mathbf{R}/\mathbf{I}$ neobsahuje žádné vlastní ideály. Pro spor tedy uvažujme vlastní ideál $\mathbf{K}$ v $\mathbf{R}/\mathbf{I}$ a definujme

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

Ukážeme, že $J$ tvoří ideál okruhu $\mathbf{R}$. 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 $\mathbf{I}$. □

**Poznámka.** Tuto větu lze vyslovit v mnohem obecnější formě: svaz ideálů okruhu $\mathbf{R}/\mathbf{I}$ je izomorfní s intervalem $[\mathbf{I}, \mathbf{R}]$ ve svazu ideálů okruhu $\mathbf{R}$ (izomorfismem je zobrazení $K \mapsto \{a \in R : [a] \in K\}$). Tato vlastnost je snadným důsledkem obecnější Věty 23.3 v kombinaci s Tvrzením 23.5 a plyne z ní také opačná implikace ve Větě 22.5: není-li $\mathbf{I}$ maximální, pak $\mathbf{R}/\mathbf{I}$ není těleso.

**Poznámka.** Podobnou charakterizaci lze dokázat i pro obory integrity: faktorokruh $\mathbf{R}/\mathbf{I}$ je obor integrity právě tehdy, když je $\mathbf{I}$ tzv. *prvoideál*, tj. pokud platí následující podmínka: kdykoliv $a \cdot b \in I$, pak $a \in I$ nebo $b \in I$. Hlavní ideál $mR$ je prvoideál právě tehdy, když je $m$ prvočinitel.

Typické použití Věty 22.5 je v situaci, kdy je $\mathbf{R}$ obor integrity hlavních ideálů (např. $\mathbb{Z}$ nebo $\mathbf{T}[x]$) a $\mathbf{I} = a\mathbf{R}$ hlavní ideál generovaný ireducibilním prvkem $a$. Takový ideál je maximální: připomeňme, že $a \mid b$ právě tehdy, když $bR \subseteq aR$,

z čehož plyne, že ideál $a\mathbf{R}$ je maximální (nejde zvětšit) právě tehdy, když je $a$ minimální (nejde zmenšit) vzhledem k dělitelnosti, tj. ireducibilní. (V obecných oborech je však tato úvaha chybná, protože mezi $aR$ a $R$ by mohl 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 podobné příklady jako v předchozím odstavci. Rozdíl je v tom, že $\mathbb{Q}[x]$ je (narozdíl od $\mathbb{Z}[x]$) obor integrity 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.
- 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.** Polynom $x-1$ je sice ireducibilní v oboru $\mathbb{Z}[x]$, ale faktorokruh

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

těleso není: to proto, že existuje (nehlavní) ideál $\mathbf{I}$ takový, že $(x-1)\mathbb{Z}[x] \subset I \subset \mathbb{Z}[x]$, např. $I = \{f \in \mathbb{Z}[x] : 2 \mid f(1)\}$.

Pomocí faktorizace oborů $\mathbb{Z}_p[x]$ podle hlavních ideálů generovaných ireducibilními polynomy se konstruují konečná tělesa. Je-li $f$ ireducibilní polynom stupně $k$, pak $|\mathbb{Z}_p[x]/f| = p^k$, protože prvky tohoto faktorokruhu lze reprezentovat pomocí polynomů stupně $< k$. Vezmeme-li na nich operace modulo $f$, dostaneme $p^k$-prvkové těleso.

V poslední kapitole dokážeme, že konečné těleso velikosti $n$ existuje právě tehdy, když $n = p^k$ pro nějaké prvočíslo $p$ a přirozené číslo $k$, a navíc jsou-li $\mathbf{T}$, $\mathbf{S}$ dvě konečná tělesa stejné velikosti, pak $\mathbf{T} \simeq \mathbf{S}$. To jediné těleso velikosti $p^k$ se obvykle značí $\mathbb{F}_{p^k}$. Přitom $\mathbb{F}_p = \mathbb{Z}_p$ a např. $\mathbb{F}_4 = \mathbb{Z}_2[x]/x^2+x+1$. (Uvědomte si, že $\mathbb{F}_4 \not\simeq \mathbb{Z}_4$!)

### 22.3. * Zobecněná Čínská věta o zbytcích.

Tvrzení 13.5 a 19.7 popisují algebraickým jazykem Čínskou větu o zbytcích pro celá čísla: jsou-li $m_1, \ldots, m_n$ po dvou nesoudělná přirozená čísla a $M = m_1 \cdot \ldots \cdot m_n$, pak

$$\mathbb{Z}_M \simeq \mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_n},$$

protože zobrazení

$$x \mapsto (x \bmod m_1, \ldots, x \bmod m_n)$$

zachovává sčítání i násobení. Při reprezentaci $\mathbb{Z}_n \simeq \mathbb{Z}/n$ tak dostáváme

$$\mathbb{Z}/M \simeq \mathbb{Z}/m_1 \times \ldots \times \mathbb{Z}/m_n,$$

přičemž předpoklady věty se překládají do řeči ideálů jako $m_i\mathbb{Z} + m_j\mathbb{Z} = \mathbb{Z}$ pro každé $i \neq j$ (Bézoutova věta) a $M\mathbb{Z} = \bigcap m_i\mathbb{Z}$. Toto tvrzení lze radikálně zobecnit.

**Věta 22.6** (Zobecněná Čínská věta o zbytcích)**.** *Buď $\mathbf{R}$ okruh s jednotkou, $\mathbf{M}_1, \ldots, \mathbf{M}_n$ jeho ideály splňující $\mathbf{M}_i + \mathbf{M}_j = \mathbf{R}$ pro každé $i \neq j$ a označme*

$$\mathbf{M} = \bigcap_{i=1}^{n} \mathbf{M}_i.$$

*Pak*

$$\mathbf{R}/\mathbf{M} \simeq \mathbf{R}/\mathbf{M}_1 \times \ldots \times \mathbf{R}/\mathbf{M}_n.$$

Připomeňme, že jsou-li $\mathbf{I}, \mathbf{J}$ ideály okruhu $\mathbf{R}$, pak podle Tvrzení 19.3 tvoří množiny $I \cap J$ i $I + J = \{a + b : a \in I, b \in J\}$ také ideál. Pro důkaz věty potřebujeme následující pomocné lemma.

**Lemma 22.7.** *Buď* $\mathbf{R}$ *okruh s jednotkou,* $\mathbf{N}, \mathbf{M}_1, \ldots, \mathbf{M}_n$ *jeho ideály splňující* $\mathbf{N} + \mathbf{M}_i = \mathbf{R}$ *pro všechna* $i$ *a označme*

$$\mathbf{M} = \bigcap_{i=1}^{n} \mathbf{M}_i.$$

*Pak* $\mathbf{M} + \mathbf{N} = \mathbf{R}$.

*Důkaz.* Evidentně stačí dokázat, že $1 \in M + N$: v tom případě $1 = a + b$ pro nějaká $a \in M$, $b \in N$ a libovolné $r \in R$ lze napsat jako $r = r \cdot 1 = ra + rb \in M + N$.

Víme, že pro všechna $i$ platí $\mathbf{N} + \mathbf{M}_i = \mathbf{R}$, tedy existují $c_i \in N$ a $d_i \in M_i$ splňující $1 = c_i + d_i$. Pak

$$\begin{aligned} 1 = 1 \cdot 1 \cdot \ldots \cdot 1 = (c_1 + d_1) \cdot (c_2 + d_2) \cdot \ldots \cdot (c_n + d_n) = \\ = d_1 d_2 \cdots d_n + c_1 d_2 \cdots d_n + d_1 c_2 \cdots d_n + c_1 c_2 \cdots d_n + \ldots + c_1 c_2 \cdots c_n. \end{aligned}$$

Prvek $d_1 d_2 \cdots d_n$ náleží $M$, neboť pro každé $i$ máme $d_i \in M_i$, tedy i $d_1 d_2 \cdots d_n \in M_i$, a proto $d_1 d_2 \cdots d_n \in \bigcap_{i=1}^{n} M_i = M$. Všechny ostatní sčítance jsou prvkem $N$, neboť v každém z nich je nějaké $c_k \in N$ a podle definice ideálu tam je i libovolný jeho násobek. Tedy i jejich součet je v $N$, a tak jsme našli rozklad $1 \in M + N$. □

Zobecněná Čínská věta o zbytcích je víceméně očividným důsledkem následujícího tvrzení.

**Lemma 22.8.** *Za předpokladů Věty 22.6, zobrazení*

$$\begin{aligned} \varphi : \mathbf{R} &\to \mathbf{R}/\mathbf{M}_1 \times \ldots \times \mathbf{R}/\mathbf{M}_n \\ x &\mapsto ([x]_{\mathbf{M}_1}, \ldots, [x]_{\mathbf{M}_n}) \end{aligned}$$

*je epimorfismus (tj. homomorfismus* na*).*

*Důkaz.* Z definice faktorokruhu plyne, že to je homomorfismus. Zvolme $u_1, \ldots, u_n \in R$, zkonstruujeme $x \in R$ splňující

$$\varphi(x) = ([u_1]_{\mathbf{M}_1}, \ldots, [u_n]_{\mathbf{M}_n}).$$

Označme $\mathbf{N}_i = \bigcap_{j \neq i} \mathbf{M}_j$. Podle Lemmatu 22.7 platí $\mathbf{M}_i + \mathbf{N}_i = \mathbf{R}$, tedy $1 \in M_i + N_i$, a tak můžeme zvolit $a_i \in M_i$, $b_i \in N_i$ splňující

$$1 = a_i + b_i.$$

Položme

$$x = b_1 u_1 + \ldots + b_n u_n.$$

Dokážeme, že pro všechna $i$ platí $[x]_{\mathbf{M}_i} = [u_i]_{\mathbf{M}_i}$, neboli že $x - u_i \in M_i$. Rozepíšeme

$$x - u_i = \sum_{j=1}^{n} b_j u_j - u_i = \sum_{j \neq i} b_j u_j + (b_i - 1) u_i = \sum_{j \neq i} b_j u_j - a_i u_i.$$

Protože $b_j \in M_i$ pro všechna $j \neq i$, máme také $b_j u_j \in M_i$ pro všechna $j \neq i$, a tedy celá suma $\sum_{j \neq i} b_j u_j \in M_i$. Zároveň $a_i \in M_i$, tedy i $a_i u_i \in M_i$, a rozdíl obou prvků je také v $M_i$. □

*Důkaz Věty 22.6.* Jádro zobrazení $\varphi$ z předchozího lemmatu je

$$\begin{aligned}\mathrm{Ker}(\varphi) &= \{x \in R : \varphi(x) = ([0], \dots, [0])\} = \{x \in R : x \in M_1, \dots, x \in M_n\} \\ &= \{x \in R : x \in \bigcap_{i=1}^{n} M_i\} = \bigcap_{i=1}^{n} M_i = M.\end{aligned}$$

1. věta o izomorfismu tak říká, že $\mathbf{R}/\mathbf{M} \simeq \mathbf{Im}(\varphi) = \mathbf{R}/\mathbf{M}_1 \times \ldots \times \mathbf{R}/\mathbf{M}_n$. □

**Důsledek 22.9.** *Buď* $\mathbf{R}$ *obor integrity hlavních ideálů,* $m_1, \dots, m_n$ *jeho po dvou nesoudělné prvky a označme* $M = m_1 \cdot \ldots \cdot m_n$*. Pak*

$$\mathbf{R}/M \simeq \mathbf{R}/m_1 \times \ldots \times \mathbf{R}/m_n.$$

*Důkaz.* Ve Větě 22.6 dosaďte za $\mathbf{M}_i$ hlavní ideál $m_i\mathbf{R}$. Je třeba ověřit, že (1) $m_iR + m_jR = R$ pro všechna $i \neq j$ a (2) $\bigcap_{i=1}^{n} m_iR = MR$.

(1) Protože je $\mathbf{R}$ obor hlavních ideálů, z Bézoutovy rovnosti existují $u, v \in R$ splňující $1 = \mathrm{NSD}(m_i, m_j) = um_i + vm_j \in m_iR + m_jR$. Tedy $m_iR + m_jR = R$.

(2) Jinými slovy, chceme dokázat, že prvek $a$ je dělitelný všemi $m_i$ právě tehdy, když je dělitelný prvkem $M$. (Připomeňme, že $a$ je prvek $mR$ právě tehdy, když $m \mid a$.) To ovšem plyne okamžitě z nesoudělnosti prvků $m_i$. □

Důsledek 22.9 nachází uplatnění v počítačové algebře: analýzou jeho důkazu lze získat např. rychlý algoritmus na řešení Čínské věty o zbytcích.

**Příklad.** Pro $\mathbf{R} = \mathbb{Z}$ dostáváme Čínskou větu o zbytcích ve formě Tvrzení 19.7.

**Příklad.** Pro $\mathbf{R} = \mathbf{T}[x]$ a $m_i = x - a_i \in T[x]$ dostáváme Větu o interpolaci 9.6. (Zde je třeba si uvědomit, že okruh $\mathbf{T}[x]/m_1 \cdots m_n$ je reprezentován polynomy nad $\mathbf{T}$ stupně $< n$, dále že $\mathbf{T}[x]/m_i \simeq \mathbf{T}$, a také že $f \bmod (x - a_i) = f(a_i)$.)

**Příklad.** Buď $\mathbf{R}$ komutativní okruh s jednotkou, ve kterém existují maximální ideály $\mathbf{I}_1, \dots, \mathbf{I}_n$ takové, že $\bigcap I_j = \{0\}$. Pak, díky Větám 22.6 a 22.5, je $\mathbf{R}$ izomorfní součinu $n$ těles.

## 23. * Faktoralgebry

**Cíl.** *Operace dané algebry můžeme přenést na množinu bloků nějaké její kongruence; tak dostaneme tzv. faktoralgebru. Jde o zobecnění pojmů faktorgrupy a faktorokruhu.*

### 23.1. Konstrukce faktoralgebry.

Buď $\mathbf{A} = (A, F)$ algebra (opět uvažujme pouze algebry s operacemi arity nejvýše dva). Ekvivalence $\sim$ na nosné množině $A$ se nazývá *kongruence* algebry $\mathbf{A}$, pokud

- pro každou binární operaci $*$ algebry $\mathbf{A}$

$$a \sim c,\ b \sim d \quad \text{implikuje} \quad a * b \sim c * d;$$

- pro každou unární operaci $'$ algebry $\mathbf{A}$

$$a \sim b \quad \text{implikuje} \quad a' \sim b'.$$

Na blocích ekvivalence $\sim$ definujeme operace předpisy

- $[a] * [b] := [a * b]$ pro každou binární operaci $*$ algebry $\mathbf{A}$;
- $[a]' := [a']$ pro každou unární operaci $'$ algebry $\mathbf{A}$;
- $C := [c]$ pro každou konstantu $c$ algebry $\mathbf{A}$.

Podmínky z definice kongruence říkají přesně to, že jsou tyto operace korektně definované. Uvažujme nyní algebru

$$\mathbf{A}/\sim = (\{[a] : a \in A\}, G)$$

stejného typu jako $\mathbf{A}$ s výše uvedenými operacemi. Nazývá se *faktoralgebra algebry* $\mathbf{A}$ *podle kongruence* $\sim$.

**Příklad.** Na algebře $(\mathbb{Z}, +)$ uvažujme kongruenci $\equiv \pmod n$. To, že jde o kongruenci, jsme dokázali v úvodu skript jako Tvrzení 2.7. Bloky této kongruence jsou zbytkové třídy po dělení $n$ a reprezentujeme-li je pomocí čísel $0, \dots, n-1$, operace faktoralgebry funguje jako sčítání modulo $n$. Tedy $\mathbb{Z}/\sim \simeq (\{0, \dots, n-1\}, +_{\bmod n})$.

Každá algebra $\mathbf{A}$ má alespoň dvě kongruence, říká se jim *nevlastní*: je to nejmenší kongruence $id = \{(a, a) : a \in A\}$ a největší kongruence $A \times A = \{(a, b) : a, b \in A\}$. Kongruence dané algebry tvoří úplný svaz, značíme jej $\mathbf{Con}(\mathbf{A})$. Uspořádáním se rozumí $\subseteq$, průsekem je průnik a spojením kongruencí $\alpha_i$, $i \in I$, je nejmenší ekvivalence obsahující $\bigcup_{i\in I} \alpha_i$ (což zpravidla není sjednocení!).

Je-li $\varphi : \mathbf{A} \to \mathbf{B}$ homomorfismus, pak *jádro*, tj. ekvivalence

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

je kongruence algebry $\mathbf{A}$ (ověření tohoto faktu je snadné).

**Věta 23.1** (o homomorfismu)**.** *Je-li $\varphi : \mathbf{A} \to \mathbf{B}$ homomorfismus algeber a $\sim$ kongruence algebry $\mathbf{A}$ taková, že $a \sim b$ implikuje $\varphi(a) = \varphi(b)$, pak je zobrazení*

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

*homomorfismus.*

*Důkaz.* Předně, $\psi$ je zobrazení, protože $[a] = [b]$ právě tehdy, když $a \sim b$, což implikuje $\varphi(a) = \varphi(b)$. Přitom pro libovolnou binární operaci $*$ na $\mathbf{A}$ a odpovídající operaci $\circ$ na $\mathbf{B}$ máme

$$\psi([a * b]) = \varphi(a * b) = \varphi(a) \circ \varphi(b) = \psi([a]) \circ \psi([b]),$$

pro libovolnou unární operaci $'$ na $\mathbf{A}$ a odpovídající operaci $''$ na $\mathbf{B}$ máme

$$\psi([a']) = \varphi(a') = \varphi(a)'' = \psi([a])''$$

a pro libovolnou konstantu $c$ na $\mathbf{A}$ a odpovídající konstantu $d$ na $\mathbf{B}$ máme $\psi([c]) = \varphi(c) = d$, tedy $\psi$ je homomorfismus. □

**Důsledek 23.2** (1. věta o izomorfismu)**.** *Je-li $\varphi : \mathbf{A} \to \mathbf{B}$ homomorfismus algeber, pak*

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

*Důkaz.* Dosaďte do Věty o homomorfismu za $\sim$ kongruenci $\ker(\varphi)$. Výsledný homomorfismus 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. □

Intervalem $[a, b]$ ve svazu $(X, \leq)$ rozumíme podsvaz $(\{x \in X : a \leq x \leq b\}, \leq)$.

**Věta 23.3.** *Je-li $\mathbf{A}$ algebra a $\sim$ její kongruence, svaz $\mathbf{Con}(\mathbf{A}/\sim)$ je izomorfní intervalu $[\sim, A^2]$ ve svazu $\mathbf{Con}(\mathbf{A})$.*

*Důkaz.* Definujeme dvě zobrazení

$$\varphi : [\sim, A^2] \to \mathrm{Con}(\mathbf{A}/\sim), \qquad \varphi(\approx) = \{([a]_\sim, [b]_\sim) : a \approx b\},$$
$$\psi : \mathrm{Con}(\mathbf{A}/\sim) \to [\sim, A^2], \qquad \psi(\approx) = \{(a, b) : [a]_\sim \approx [b]_\sim\}.$$

Není těžké ověřit, že $\varphi(\approx)$ je skutečně kongruence algebry $\mathbf{A}/\sim$ a že $\psi(\approx)$ je kongruence algebry $\mathbf{A}$ obsahující $\sim$. Dále je vidět, že $\varphi(\psi(\approx)) = \approx$ a $\psi(\varphi(\approx)) = \approx$, tedy $\varphi, \psi$ jsou navzájem inverzní zobrazení, čili bijekce. Přitom obě zobrazení zřejmě zachovávají uspořádání (čím větší $\approx$, tím větší $\varphi(\approx)$, resp. $\psi(\approx)$), jsou to tedy izomorfismy těchto svazů. □

23.2. **Kongruence grup a okruhů.**

Všimněte si, že ekvivalence $\sim$ definovaná v úvodu sekce o faktorgrupách i faktorokruzích je kongruencí příslušné grupy, resp. okruhu. Platí i v jistém smyslu opačné tvrzení: každá kongruence dané grupy, resp. okruhu, vzniká touto konstrukcí z nějaké normální podgrupy, resp. ideálu. Tato tvrzení nyní dokážeme.

**Tvrzení 23.4.** *Je-li $\sim$ kongruence grupy $\mathbf{G} = (G, \cdot, ^{-1}, 1)$, pak $[1]_\sim$ tvoří normální podgrupu grupy $\mathbf{G}$ a $a \sim b$ právě tehdy, když $a \cdot b^{-1} \in [1]_\sim$.*

*Důkaz.* Blok $[1]_\sim$ zřejmě obsahuje jednotku a dále, je-li $a, b \in [1]_\sim$, tj. $a \sim 1$ a $b \sim 1$, pak z definice kongruence plyne $a^{-1} \sim 1^{-1} = 1$, $a \cdot b \sim 1 \cdot 1 = 1$ a navíc pro libovolné $c \in G$ platí $c \cdot a \cdot c^{-1} \sim c \cdot 1 \cdot c^{-1} = c \cdot c^{-1} = 1$. Tedy blok $[1]_\sim$ je uzavřen na všechny operace i konjugaci. Nakonec vidíme, že $a \cdot b^{-1} \sim 1 \;\Leftrightarrow\; a \cdot b^{-1} \cdot b \sim 1 \cdot b \;\Leftrightarrow\; a \sim b$. □

Jinými slovy, svazy $\mathbf{Con}(\mathbf{G})$ a $\mathbf{NSub}(\mathbf{G})$ jsou izomorfní, izomorfismus zobrazuje kongruenci $\sim$ na podgrupu $[1]_\sim$.

**Tvrzení 23.5.** *Je-li $\sim$ kongruence okruhu $\mathbf{R}$, pak $[0]_\sim$ tvoří ideál okruhu $\mathbf{R}$ a $a \sim b$ právě tehdy, když $a - b \in [0]_\sim$.*

*Důkaz.* Podle Tvrzení 23.4 již víme, že $[0]_\sim$ tvoří podgrupu grupy $(R, +, -, 0)$. Je-li $r \in R$ a $a \in [0]_\sim$, pak $a \cdot r \sim 0 \cdot r = 0$ a $r \cdot a \sim r \cdot 0 = 0$, čili $[0]_\sim$ je ideál. Analogicky $a - b \sim 0 \;\Leftrightarrow\; a - b + b \sim 0 + b \;\Leftrightarrow\; a \sim b$. □

Jinými slovy, svazy $\mathbf{Con}(\mathbf{R})$ a $\mathbf{Id}(\mathbf{R})$ jsou izomorfní, izomorfismus zobrazuje kongruenci $\sim$ na ideál $[0]_\sim$.

23.3. **Faktoralgebry v obecném jazyce.**

Ekvivalence $\sim$ na nosné množině $A$ se nazývá *kongruence* algebry $\mathbf{A} = (A, F)$, pokud pro každé $\omega \in \Omega$ a $a_1 \sim b_1, \ldots, a_{\tau(\omega)} \sim b_{\tau(\omega)}$ platí

$$F_\omega(a_1, \ldots, a_{\tau(\omega)}) \sim F_\omega(b_1, \ldots, b_{\tau(\omega)}).$$

Na blocích ekvivalence $\sim$ definujeme operace předpisy

$$G_\omega([a_1], \ldots, [a_{\tau(\omega)}]) = [F_\omega(a_1, \ldots, a_{\tau(\omega)})]$$

pro každé $\omega \in \Omega$ a $a_1, \ldots, a_{\tau(\omega)} \in A$. Podmínky z definice kongruence přesně říkají, že jsou tyto operace korektně definované. Uvažujme nyní algebru

$$\mathbf{A}/\sim = (\{[a] : a \in A\}, G)$$

stejného typu jako $\mathbf{A}$ s výše uvedenými operacemi. Nazývá se *faktoralgebra algebry $\mathbf{A}$ podle kongruence $\sim$*.

**Věta 23.6** (o homomorfismu)**.** *Je-li* $\varphi : \mathbf{A} \to \mathbf{B}$ *homomorfismus algeber a* $\sim$ *kongruence algebry* $\mathbf{A}$ *taková, že* $a \sim b$ *implikuje* $\varphi(a) = \varphi(b)$*, pak je zobrazení*

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

*homomorfismus.*

**Důsledek 23.7** (1. věta o izomorfismu)**.** *Je-li* $\varphi : \mathbf{A} \to \mathbf{B}$ *homomorfismus algeber, pak*

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

**Věta 23.8.** *Je-li* $\mathbf{A}$ *algebra a* $\sim$ *její kongruence, svaz* $\mathbf{Con}(\mathbf{A}/\!\sim)$ *je izomorfní intervalu* $[\sim, A^2]$ *ve svazu* $\mathbf{Con}(\mathbf{A})$*.*

Důkazy lze provést analogicky jako pro Věty 23.1–23.3.

# Tělesa

Připomeňme, že *tělesem* rozumíme komutativní okruh s jednotkou, jehož každý nenulový prvek je invertibilní. (Někteří autoři definují tělesa tak, že nemusejí být nutně komutativní; je-li to nutné, pak výslovně uvádějí „komutativní těleso“.) Nejdůležitějšími příklady jsou

- těleso *komplexních čísel* $\mathbb{C}$ a jeho podtělesa ($\mathbb{Q}$, $\mathbb{R}$ a další, viz následující sekce);
- a dále *konečná tělesa* ($\mathbb{Z}_p$ a další, viz Sekce 27).

Z předchozích kapitol připomeňme

- konstrukci *podílového tělesa* daného oboru integrity (Tvrzení 8.1);
- a konstrukci těles jako faktorokruhů podle maximálních ideálů (Věta 22.5).

Připomeňme, že *charakteristikou* tělesa rozumíme nejmenší $n \in \mathbb{N}$ takové, že $n \cdot 1 = 0$, pokud takové $n$ existuje, resp. 0 v opačném případě. Charakteristika tělesa je zaručeně 0 nebo prvočíslo. Např. charakteristika $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ je 0, charakteristika konečného $p^k$-prvkového tělesa je $p$, charakteristika $\mathbf{T}[x]/f$ je stejná jako charakteristika $\mathbf{T}$.

Nejmenší podtěleso (musí obsahovat prvek 1) se nazývá *prvotěleso*. V Sekci 19.5 jsme dokázali, že prvookruh je izomorfní buď $\mathbb{Z}$ (v charakteristice 0) nebo některému $\mathbb{Z}_n$ (v charakteristice $n$). Každé těleso tedy obsahuje podtěleso izomorfní buď $\mathbb{Q}$ (tj. podílovému tělesu prvookruhu $\mathbb{Z}$) nebo některému $\mathbb{Z}_p$.

*Rozšířením tělesa* $\mathbf{T}$ rozumíme libovolné nadtěleso $\mathbf{S} \geq \mathbf{T}$. Na teorii těles tedy lze pohlížet jako na studium rozšíření tělesa $\mathbb{Q}$, s aplikacemi např. na studium kořenů celočíselných polynomů, nebo jako na studium rozšíření těles $\mathbb{Z}_p$, pod něž spadá např. teorie konečných těles. Do základů obou teorií nahlédneme v této kapitole.

## 24. Rozšíření konečného stupně

**Cíl.** *Budeme studovat rozšíření těles o algebraické prvky. Ukážeme, jak dimenze (stupeň) rozšíření souvisí s kořeny polynomů a na závěr charakterizujeme všechna rozšíření konečného stupně: jsou to právě rozšíření o konečné množství algebraických prvků.*

Připomeňme, že je-li $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a_1, \ldots, a_n \in S$, pak $\mathbf{T}[a_1, \ldots, a_n]$ značí nejmenší *podokruh* $\mathbf{S}$ obsahující $\mathbf{T}$ i $a_1, \ldots, a_n$. Zavedeme značení $\mathbf{T}(a_1, \ldots, a_n)$ pro nejmenší *podtěleso* $\mathbf{S}$ obsahující $\mathbf{T}$ i $a_1, \ldots, a_n$. V některých případech jde o tentýž okruh, někdy ne — např. $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$, ale $\mathbb{Q}(\pi) \neq \mathbb{Q}[\pi]$ (viz Tvrzení 24.2 a příklady pod ním).

Klíčem k pochopení této sekce je myšlenka, že nadtěleso $\mathbf{S} \geq \mathbf{T}$ lze považovat za vektorový prostor nad tělesem $\mathbf{T}$: sčítání a odčítání přebereme beze změny a místo násobení jako operace $S \times S \to S$ uvažujeme pouze restrikci $T \times S \to S$, tj. násobíme prvky $\mathbf{S}$ (vektory) pouze prvky $\mathbf{T}$ (skaláry). Tento vektorový prostor budeme značit $\mathbf{S_T} = (S, +, -, 0, a\cdot : a \in T)$, jeho dimenze se nazývá *stupeň rozšíření* $\mathbf{T} \leq \mathbf{S}$ a značí se $[\mathbf{S} : \mathbf{T}] = \dim \mathbf{S_T}$.

**Příklad.**

- $[\mathbb{C} : \mathbb{R}] = 2$. Prvek $a+bi \in \mathbb{C}$ lze považovat za dvojdimenzionální vektor nad $\mathbb{R}$, sčítání i násobení reálným číslem probíhá po složkách. Báze prostoru $\mathbb{C}_\mathbb{R}$ je např. $1, i$.
- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Prvek $a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}]$ lze považovat za třídimenzionální vektor nad $\mathbb{Q}$ ze stejného důvodu. Báze prostoru $\mathbb{Q}(\sqrt[3]{2})_\mathbb{Q}$ je např. $1, \sqrt[3]{2}, \sqrt[3]{4}$.
- $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$, báze prostoru $\mathbb{Q}(\sqrt{2}, \sqrt{3})_\mathbb{Q}$ je např. $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$.
- Rozšíření mohou mít i nekonečný stupeň: např. $[\mathbb{Q}(\pi) : \mathbb{Q}] = \aleph_0$ a $[\mathbb{R} : \mathbb{Q}] = 2^{\aleph_0}$.

Je-li stupeň $[\mathbf{S} : \mathbf{T}]$ konečný, říkáme, že jde o rozšíření *konečného stupně*.

**Definice.** Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a \in S$. Řekneme, že prvek $a$ je *algebraický* nad $\mathbf{T}$, pokud existuje polynom z $\mathbf{T}[x]$, jehož je $a$ kořenem. V opačném případě se prvek $a$ nazývá *transcendentní* nad $\mathbf{T}$. Je-li každý prvek tělesa $\mathbf{S}$ algebraický nad $\mathbf{T}$, hovoříme o *algebraickém rozšíření*.

**Tvrzení 24.1.** *Rozšíření konečného stupně jsou algebraická.*

*Důkaz.* Označme $n = [\mathbf{S} : \mathbf{T}]$ a uvažujme libovolný prvek $a \in S$; dokážeme, že je algebraický nad $\mathbf{T}$. Prvky $1, a, a^2, \ldots, a^{n-1}, a^n$ jsou lineárně závislé, protože jich je více než je dimenze vektorového prostoru $\mathbf{S}_\mathbf{T}$. Tedy existují koeficienty $b_i \in T$, aspoň jeden z nich nenulový, kterými lze lineárně nakombinovat nulu, tj. $\sum_{i=0}^{n} b_i a^i = 0$. Prvek $a$ je tedy kořenem nenulového polynomu $\sum_{i=0}^{n} b_i x^i \in T[x]$. □

Opačná implikace neplatí: příkladem je algebraický uzávěr tělesa $\mathbb{Q}$ (viz Tvrzení 26.3), který má nekonečný stupeň nad $\mathbb{Q}$. Pokud ovšem rozšiřujeme těleso $\mathbf{T}$ o jediný algebraický prvek, stupeň konečný je (viz Tvrzení 24.3). Dokážeme to pomocí tzv. minimálních polynomů.

**Definice.** Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a \in S$ algebraický prvek nad $\mathbf{T}$. *Minimálním polynomem* prvku $a$ nad $\mathbf{T}$ rozumíme monický polynom $m_{a,\mathbf{T}} \in T[x]$ splňující

(1) $m_{a,\mathbf{T}}(a) = 0$;
(2) kdykoliv monický polynom $f \in T[x]$ splňuje $f(a) = 0$, pak $m_{a,\mathbf{T}} \mid f$.

Existuje takový polynom pro každý algebraický prvek? Ano, neboť množina

$$I = \{f \in T[x] : f(a) = 0\}$$

tvoří ideál v oboru $\mathbf{T}[x]$; protože je v tomto oboru každý ideál hlavní (Věta 6.4), $\mathbf{I}$ má (monický) generátor $m$ (tj. $I = mT[x]$) a vidíme,že $m$ je hledaný polynom $m_{a,\mathbf{T}}$.

Polynom $m_{a,\mathbf{T}}$ je v $\mathbf{T}[x]$ ireducibilní: kdyby se rozkládal na součin $f \cdot g$, pak by prvek $a$ byl kořenem $f$ nebo $g$ (nebo obou), což by bylo ve sporu s minimalitou. Naopak, je-li $a$ kořen monického ireducibilního polynomu $f \in T[x]$, pak $f = m_{a,\mathbf{T}}$: to proto, že $m_{a,\mathbf{T}}$ musí dělit $f$, jenže ten nemá vlastní dělitele.

**Příklad.** Z výše uvedeného důvodu je vidět, že např.

$$m_{1,\mathbb{Q}} = x - 1, \quad m_{i,\mathbb{Q}} = x^2 + 1, \quad m_{\sqrt[3]{2},\mathbb{Q}} = x^3 - 2, \quad m_{\sqrt{2}+\sqrt{3},\mathbb{Q}} = x^4 - 10x^2 + 1.$$

**Tvrzení 24.2.** *Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a \in S$ algebraický prvek nad $\mathbf{T}$. Pak*

$$\mathbf{T}(a) = \mathbf{T}[a].$$

*Důkaz.* Podle Tvrzení 19.2 tvoří $T[a] = \{f(a) : f \in T[x]\}$ podokruh tělesa $\mathbf{S}$. Dokážeme, že to je podtěleso, tj. že v něm existují inverzní prvky ke všem nenulovým prvkům. Mějme nějaký prvek $0 \neq f(a) \in T[a]$; hledáme polynom $g \in T[x]$ takový, že $f(a)g(a) = 1$. Protože $f(a) \neq 0$, polynom $m_{a,\mathbf{T}}$ nedělí $f$. Z ireducibility $m_{a,\mathbf{T}}$ plyne $\mathrm{NSD}(m_{a,\mathbf{T}}, f) = 1$, a tak podle Bézoutovy rovnosti existují polynomy $u, g \in T[x]$ takové, že $1 = um_{a,\mathbf{T}} + gf$. Dosazením prvku $a$ dostáváme $1 = u(a)m_{a,\mathbf{T}}(a) + g(a)f(a) = u(a) \cdot 0 + g(a)f(a) = f(a)g(a)$. □

**Poznámka.** Předchozí tvrzení lze dokázat i takto: homomorfismus $\varphi : \mathbf{T}[x] \to \mathbf{T}[a]$, $f \mapsto f(a)$, je zřejmě na, za jádro má ideál $m_{a,\mathbf{T}}T[x]$, a tak podle 1. věty o izomorfismu $\mathbf{T}[x]/m_{a,\mathbf{T}} \simeq \mathbf{T}[a]$. Protože je $m_{a,\mathbf{T}}$ ireducibilní, podle Věty 22.5 je $\mathbf{T}[a]$ těleso, tedy $\mathbf{T}[a] = \mathbf{T}(a)$.

**Příklad.** Číslo $\pi$ je transcendentní nad $\mathbb{Q}$. Díky tomu má homomorfismus

$$\mathbb{Q}[x] \to \mathbb{Q}[\pi], \qquad f \mapsto f(\pi)$$

triviální jádro a z Tvrzení 19.2 plyne, že to je izomorfismus. Ovšem $\mathbb{Q}[x]$ není těleso, takže ani $\mathbb{Q}[\pi]$ není těleso a z toho důvodu $\mathbb{Q}[\pi] \neq \mathbb{Q}(\pi)$. (Všimněte si, že např. $\frac{1}{\pi} \in \mathbb{Q}(\pi) \setminus \mathbb{Q}[\pi]$.) Ve skutečnosti je $\mathbb{Q}(\pi)$ podílové těleso oboru $\mathbb{Q}[\pi]$.

**Tvrzení 24.3.** *Buď $\mathbf{T} \leq \mathbf{S}$ rozšíření těles a $a \in S$ algebraický prvek nad $\mathbf{T}$. Pak*

$$[\mathbf{T}(a) : \mathbf{T}] = \deg m_{a,\mathbf{T}}.$$

*Důkaz.* Označme $n = \deg m_{a,\mathbf{T}}$. Dokážeme, že prvky $1, a, a^2, \ldots, a^{n-1}$ tvoří bázi vektorového prostoru $\mathbf{T}(a)_{\mathbf{T}}$, a tedy že jeho dimenze je $n$.

Kdyby byly prvky $1, a, a^2, \ldots, a^{n-1}$ lineárně závislé, pak by platilo $\sum_{i=0}^{n-1} b_i a^i = 0$ pro nějaká $b_i \in T$, z nichž je aspoň jedno nenulové. Takže by prvek $a$ byl kořenem (nenulového) polynomu $\sum_{i=0}^{n-1} b_i x^i \in T[x]$ s menším stupněm než $m_{a,\mathbf{T}}$, což je spor s minimalitou $m_{a,\mathbf{T}}$.

Nyní dokážeme, že prvky $1, a, \ldots, a^{n-1}$ generují vektorový prostor $\mathbf{T}(a)_{\mathbf{T}}$. Mějme prvek $f(a)$ tělesa $\mathbf{T}(a) = \mathbf{T}[a]$, vyjádříme jej jako lineární kombinaci. Buď $q, r \in T[x]$ takové, že $f = q \cdot m_{a,\mathbf{T}} + r$ a $\deg r < \deg m_{a,\mathbf{T}} = n$. Pak

$$f(a) = q(a) \cdot m_{a,\mathbf{T}}(a) + r(a) = q(a) \cdot 0 + r(a) = r(a),$$

a protože je stupeň $r$ menší než $n$, máme $f(a) = r(a) = \sum_{i=0}^{n-1} b_i a^i$, kde $b_i \in T$ jsou koeficienty polynomu $r$. □

**Příklad.**

- $[\mathbb{C} : \mathbb{R}] = \deg(x^2 + 1) = 2$.
- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg(x^3 - 2) = 3$.
  Obecněji, $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = \deg(x^n - p) = n$ pro libovolné $n$ a prvočíslo $p$, protože uvedený polynom je podle Eisensteinova kritéria ireducibilní. (Co když $p$ není prvočíslo?)
- $[\mathbb{Q}(e^{2\pi i/3}) : \mathbb{Q}] = 2$. Číslo $e^{2\pi i/3}$ je kořen polynomu $x^3 - 1$, ten však není ireducibilní, rozkládá se jako $(x - 1)(x^2 + x + 1)$.
  Obecněji, $[\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}] = p - 1$ pro libovolné prvočíslo $p$.

**Tvrzení 24.4.** *Buď $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$ rozšíření těles. Pak*

$$[\mathbf{U} : \mathbf{T}] = [\mathbf{U} : \mathbf{S}] \cdot [\mathbf{S} : \mathbf{T}].$$

Abychom zjednodušili zápis, důkaz tvrzení provedeme pouze pro případ, kdy jde o rozšíření konečného stupně. V nekonečném případě lze postupovat analogicky a čtenář zběhlý v práci s nekonečnědimenzionálními prostory si jej snadno sám upraví (v dalším textu nebudeme tento případ potřebovat).

*Důkaz.* Označme $m = [\mathbf{U} : \mathbf{S}]$, $n = [\mathbf{S} : \mathbf{T}]$ a zvolme bázi $a_1, \dots, a_n$ vektorového prostoru $\mathbf{S_T}$ a bázi $b_1, \dots, b_m$ vektorového prostoru $\mathbf{U_S}$. Dokážeme, že prvky

$$a_1b_1, \dots, a_1b_m,\ a_2b_1, \dots, a_2b_m,\ \dots,\ a_nb_1, \dots, a_nb_m$$

tvoří bázi vektorového prostoru $\mathbf{U_T}$.

Nejprve dokážeme, že tyto prvky generují $\mathbf{U_T}$. Je-li $u \in U$, pak $u = \sum_i s_i b_i$ pro nějaká $s_i \in S$. Každé $s_i$ lze napsat jako $s_i = \sum_j t_{ij} a_j$ pro nějaká $t_{ij} \in T$ a dosazením druhé rovnosti do první dostáváme

$$u = \sum_i \big(\sum_j t_{ij} a_j\big) b_i = \sum_{i,j} t_{ij} \cdot a_j b_i.$$

Tedy $u$ je lineární kombinací uvedených prvků s koeficienty z tělesa $\mathbf{T}$.

Nyní dokážeme lineární nezávislost. Předpokládejme, že $\sum_{i,j} t_{ij} \cdot a_i b_j = 0$ pro nějaká $t_{ij} \in T$. Rozepíšeme

$$0 = \sum_{i,j} t_{ij} a_i b_j = \sum_j \underbrace{\big(\sum_i t_{ij} a_i\big)}_{\in S} b_j.$$

Lineární nezávislost prvků $b_1, \dots, b_m$ nad tělesem $\mathbf{S}$ nám dává $\sum_i t_{ij} a_i = 0$ pro každé $j$ a z lineární nezávislosti $a_1, \dots, a_n$ nad tělesem $\mathbf{T}$ dostáváme $t_{ij} = 0$ pro všechna $i, j$. □

**Příklad.** Pomocí výpočtu dimenze předvedeme, že

$$\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3}).$$

Podle Tvrzení 24.3 je $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = \deg(x^4 - 10x^2 + 1) = 4$. Podle Tvrzení 24.4 a 24.3 je $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2 - 3) \cdot \deg(x^2 - 2) = 4$. Protože mají oba prostory stejnou dimenzi, a přitom je zřejmě $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \leq \mathbb{Q}(\sqrt{2}, \sqrt{3})$, musí být tyto prostory stejné.

**Věta 24.5.** *Rozšíření $\mathbf{T} \leq \mathbf{S}$ má konečný stupeň právě tehdy, když $\mathbf{S} = \mathbf{T}(a_1, \dots, a_n)$ pro nějaké prvky $a_1, \dots, a_n \in S$ algebraické nad $\mathbf{T}$.*

*Důkaz.* ($\Leftarrow$) Uvažujme postupná rozšíření

$$\mathbf{T} \leq \mathbf{T}(a_1) \leq \mathbf{T}(a_1, a_2) \leq \ldots \leq \mathbf{T}(a_1, \dots, a_n).$$

Podle Tvrzení 24.4 je $[\mathbf{T}(a_1, \dots, a_n) : \mathbf{T}]$ rovno

$$[\mathbf{T}(a_1) : \mathbf{T}] \cdot [\mathbf{T}(a_1, a_2) : \mathbf{T}(a_1)] \cdot \ldots \cdot [\mathbf{T}(a_1, \dots, a_n) : \mathbf{T}(a_1, \dots, a_{n-1})].$$

Všechny stupně v součinu jsou konečné díky Tvrzení 24.3, tedy i $[\mathbf{T}(a_1, \dots, a_n) : \mathbf{T}]$ je konečný.

($\Rightarrow$) Budeme postupovat indukcí podle $k = [\mathbf{S} : \mathbf{T}]$. Pro $k = 1$ je $\mathbf{S} = \mathbf{T}$ a věta platí. Dále předpokládejme platnost tvrzení pro všechna rozšíření dimenze méně než $k$. Zvolme prvek $a \in S \setminus T$ a uvažujme rozšíření $\mathbf{T} < \mathbf{T}(a) \leq \mathbf{S}$. Podle Tvrzení 24.4 platí

$$\underbrace{[\mathbf{S} : \mathbf{T}]}_{k} = \underbrace{[\mathbf{S} : \mathbf{T}(a)]}_{<k} \cdot \underbrace{[\mathbf{T}(a) : \mathbf{T}]}_{>1}.$$

Z indukčního předpokladu dostáváme, že

$$\mathbf{S} = (\mathbf{T}(a))(b_1, \ldots, b_n) = \mathbf{T}(a, b_1, \ldots, b_n)$$

pro nějaké prvky $b_1, \ldots, b_n$. Protože jde o rozšíření konečného stupně, všechny prvky $a, b_1, \ldots, b_n$ jsou podle Tvrzení 24.1 algebraické nad $\mathbf{T}$. □

Na závěr uvedeme jednu drobnou aplikaci této věty. Rozšířením stupně 2 se říká *kvadratická*. Dokážeme, že je-li $\mathbf{T} < \mathbf{S} \leq \mathbb{C}$ a $[\mathbf{S} : \mathbf{T}] = 2$, pak

$$\mathbf{S} = \mathbf{T}(\sqrt{s}) \text{ pro nějaké } s \in T.$$

Podle Věty 24.5 je $\mathbf{S} = \mathbf{T}(a)$ a podle Tvrzení 24.3 je $a$ kořenem nějakého polynomu z $\mathbf{T}[x]$ stupně 2. Známý vzorec na výpočet kořenů kvadratického polynomu říká, že $a = u + v\sqrt{s}$ pro nějaká $u, v, s \in T$, a tak $\mathbf{S} = \mathbf{T}(u + v\sqrt{s}) = \mathbf{T}(\sqrt{s})$. (Tvrzení platí obecně pro libovolné kvadratické rozšíření charakteristiky $\neq 2$, místo komplexních čísel stačí uvažovat libovolné nadtěleso, kde existují odmocniny, jako např. algebraický uzávěr.)

**Shrnutí.** Zapamatujte si následující vlastnosti rozšíření $\mathbf{T} \leq \mathbf{S}$:

(1) Je-li $a \in S$ algebraický nad $\mathbf{T}$, pak

$$\mathbf{T}(a) = \mathbf{T}[a] = \{f(a) : f \in T[x]\} \quad \text{a} \quad [\mathbf{T}(a) : \mathbf{T}] = \deg m_{a,\mathbf{T}}.$$

(2) Je-li $[\mathbf{S} : \mathbf{T}] < \infty$, pak každý prvek $\mathbf{S}$ je algebraický nad $\mathbf{T}$ a

$$\mathbf{S} = \mathbf{T}(a_1, \ldots, a_n).$$

(3) Je-li $\mathbf{T} \leq \mathbf{S} \leq \mathbf{U}$, pak $[\mathbf{U} : \mathbf{T}] = [\mathbf{U} : \mathbf{S}] \cdot [\mathbf{S} : \mathbf{T}]$.

## 25. * Konstrukce pravítkem a kružítkem

**Cíl.** *Geometrickým konstrukcím pravítkem a kružítkem odpovídají tělesa konstruovatelných čísel. Pomocí poznatků z předchozí sekce lze dokázat, že některá čísla konstruovatelná nejsou, což umožňuje dokázat neřešitelnost některých konstrukčních úloh.*

Mezi klasické starořecké úlohy patřily konstrukce pomocí pravítka a kružítka. Postupem času vykrystalizovaly čtyři slavné úlohy, které se přes všechnu snahu nedařilo vyřešit:

- *Rektifikace kružnice*: k dané kružnici sestrojit úsečku, která je stejně dlouhá jako obvod této kružnice.
- *Kvadratura kruhu*: k danému kruhu sestrojit úsečku takovou, že čtverec s touto hranou má stejnou plochu jako daný kruh.
- *Zdvojení krychle*: k dané úsečce $u$ sestrojit úsečku $v$ takovou, že krychle s hranou dlouhou jako $v$ má dvakrát větší objem, než krychle s hranou dlouhou jako $u$.
- *Trisekce úhlu*: k danému úhlu sestrojit třetinový úhel.

V moderní řeči bychom první tři úlohy přeložili jako „je-li dána jednotková úsečka, zkonstruujte úsečku délky $2\pi$, resp. $\sqrt{\pi}$, resp. $\sqrt[3]{2}$.“ Přes 2000 let trvaly snahy tyto úlohy vyřešit. Až rozvoj algebry v 19. století umožnil dokázat, že to není možné. Pro zdvojení krychle a trisekci úhlu nalezl důkaz Pierre Wantzel roku 1837; stejná metoda řeší i rektifikaci kružnice a kvadraturu kruhu, k dokončení však bylo třeba počkat dalších téměř 50 let na Lindemannův důkaz transcendence čísla $\pi$. Wantzelovu metodu zde předvedeme.

Předně musíme upřesnit, co vlastně rozumíme konstrukcí pomocí pravítka a kružítka. Na začátku je daná jistá konečná množina $\mathcal{M}_0$ bodů v rovině. Z ní můžeme zkonstruovat nový bod jako průsečík přímek nebo kružnic určených již zkonstruovanými body; a tento postup lze několikrát opakovat. Formálně, konstrukce pomocí pravítka a kružítka je posloupnost $\mathcal{M}_0 \subseteq \mathcal{M}_1 \subseteq \ldots \subseteq \mathcal{M}_n$ konečných množin bodů v rovině taková, že $\mathcal{M}_{i+1} = \mathcal{M}_i \cup \{X\}$, kde $X$ vznikne jako

(1) průsečík přímky $AB$ a přímky $CD$;
(2) průsečík přímky $AB$ a kružnice se středem $C$ a poloměrem $|DE|$;
(3) průsečík kružnice se středem $A$ a poloměrem $|BC|$ a kružnice se středem $D$ a poloměrem $|EF|$

pro nějaké body $A, B, C, D, E, F \in \mathcal{M}_i$.

Princip Wantzelovy metody je převedení konstrukcí pravítkem a kružítkem do jazyka algebry. Zvolme v rovině souřadnice a uvažujme nejmenší těleso $\mathbf{T}_i$, které obsahuje $x$-ové i $y$-ové souřadnice všech bodů z $\mathcal{M}_i$. Dostáváme tak řetězec rozšíření těles $\mathbf{T}_0 \leq \mathbf{T}_1 \leq \mathbf{T}_2 \leq \ldots \leq \mathbf{T}_n$.

**Příklad** (Půlení úhlu)**.** Podívejme se, jak se formalizuje úloha k danému úhlu sestrojit poloviční úhel. Mějme dán úhel třemi body $A, B, C$ (kde $A$ je vrchol). Sestrojíme body

$$D = k(A, |AB|) \cap AC \quad \text{a} \quad E = k(B, |BD|) \cap k(D, |BD|),$$

výsledkem bude úhel daný body $A, B, E$. Tedy

$$\mathcal{M}_0 = \{A, B, C\}, \quad \mathcal{M}_1 = \mathcal{M}_0 \cup \{D\}, \quad \mathcal{M}_2 = \mathcal{M}_1 \cup \{E\}.$$

Zvolme souřadnice tak, že $A = (0, 0)$, $B = (1, 0)$ a $C = (a, b)$. Není těžké spočítat, že $D = (\frac{a}{a^2+b^2}, \frac{b}{a^2+b^2})$ a $E = (\frac{a+a^2+b^2-b\sqrt{3}}{2(a^2+b^2)}, \frac{b+(a^2+a-b^2)\sqrt{3}}{2(a^2+b^2)})$, tedy

$$\mathbf{T}_0 = \mathbb{Q}(a, b), \quad \mathbf{T}_1 = \mathbf{T}_0, \quad \mathbf{T}_2 = \mathbf{T}_0(\sqrt{3}).$$

Stěžejním krokem Wantzelovy meotdy je následující tvrzení.

**Tvrzení 25.1.** $[\mathbf{T}_n : \mathbf{T}_0]$ *je mocnina čísla 2.*

*Důkaz.* Podle Tvrzení 24.4 je

$$[\mathbf{T}_n : \mathbf{T}_0] = [\mathbf{T}_n : \mathbf{T}_{n-1}] \cdot \ldots \cdot [\mathbf{T}_2 : \mathbf{T}_1] \cdot [\mathbf{T}_1 : \mathbf{T}_0].$$

Ukážeme, že

$$[\mathbf{T}_{i+1} : \mathbf{T}_i] \in \{1, 2\}.$$

Probereme postupně všechny tři možnosti, jak se konstruuje nový bod.

(1) Jde-li o průsečík dvou přímek, získáme souřadnice nového bodu řešením soustavy dvou lineárních rovnic o dvou neznámých nad tělesem $\mathbf{T}_i$. Řešení soustavy je opět prvek tělesa $\mathbf{T}_i$, takže máme $\mathbf{T}_{i+1} = \mathbf{T}_i$ a

$$[\mathbf{T}_{i+1} : \mathbf{T}_i] = 1.$$

(2) Jde-li o průsečík přímky a kružnice, získáme souřadnice nového bodu řešením soustavy jedné lineární a jedné kvadratické rovnice o dvou neznámých nad tělesem $\mathbf{T}_i$. Vyjádříme-li z lineární rovnice $y$ a dosadíme jej do kvadratické, dostaneme kvadratickou rovnici pro $x$, jejímž řešením je číslo tvaru $a + b\sqrt{s}$, $a, b, s \in T_i$; podobný tvar bude mít i $y$. Tedy $\mathbf{T}_{i+1} = \mathbf{T}_i(\sqrt{s})$, z čehož plyne, že

$$[\mathbf{T}_{i+1} : \mathbf{T}_i] \in \{1, 2\}$$

v závislosti na tom, zda je $\sqrt{s} \in T_i$ nebo ne.

(3) Jde-li o průsečík dvou kružnic, získáme souřadnice nového bodu řešením soustavy dvou kvadratických rovnic o dvou neznámých nad tělesem $\mathbf{T}_i$. Odečteme-li obě rovnice od sebe, zbavíme se kvadratických členů (všechny mají koeficient 1) a získáme tak ekvivaletní soustavu sestávající z jedné lineární a jedné kvadratické rovnice. Stejným argumentem jako v (2) dostaneme

$$[\mathbf{T}_{i+1} : \mathbf{T}_i] \in \{1, 2\}.$$

(Proveďte popsané výpočty podrobně s obecnými rovnicemi přímky a kružnice v rovině!) □

Důsledkem Tvrzení 25.1 je neřešitelnost uvedených úloh pravítkem a kružítkem.

*Rektifikace kružnice* a *kvadratura kruhu.* Zvolme souřadnice tak, že krajní body zadané úsečky (udávající střed a poloměr kružnice) jsou $(0, 0)$ a $(1, 0)$; čili $\mathbf{T}_0 = \mathbb{Q}$. Cílem úlohy je sestrojit úsečku délky $2\pi$, resp. $\sqrt{\pi}$, a bez újmy na obecnosti můžeme předpokládat, že výsledná úsečka má krajní body $(0, 0)$ a $(2\pi, 0)$, resp. $(\sqrt{\pi}, 0)$. V tom případě ale $\pi$, resp. $\sqrt{\pi}$, náleží tělesu $\mathbf{T}_n$ a to je spor, neboť rozšíření $\mathbf{T}_0 \leq \mathbf{T}_n$ je konečného stupně, tedy podle Tvrzení 24.1 algebraické, zatímco $\pi$ i $\sqrt{\pi}$ jsou transcendentní čísla.

(Obecněji bychom mohli říci, že z jednotkové úsečky nelze sestrojit úsečka žádné transcendentní délky.)

*Zdvojení krychle.* Podobně, zvolme souřadnice tak, že krajní body zadané úsečky jsou $(0, 0)$ a $(1, 0)$; čili $\mathbf{T}_0 = \mathbb{Q}$. Cílem úlohy je sestrojit úsečku délky $\sqrt[3]{2}$ a bez újmy na obecnosti můžeme předpokládat, že výsledná úsečka má krajní body $(0, 0)$ a $(\sqrt[3]{2}, 0)$. V tom případě ale $\sqrt[3]{2}$ náleží tělesu $\mathbf{T}_n$, z čehož plyne, že 3 dělí $[\mathbf{T}_n : \mathbf{T}_0]$ — uvažujeme-li rozšíření $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2}) \leq \mathbf{T}_n$, Tvrzení 24.4 říká, že

$$[\mathbf{T}_n : \mathbf{T}_0] = [\mathbf{T}_n : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \cdot [\mathbf{T}_n : \mathbb{Q}(\sqrt[3]{2})].$$

Spor s Tvrzením 25.1.

(Obecněji bychom mohli říci, že z jednotkové úsečky nelze sestrojit úsečka žádné délky $a$ takové, že polynom $m_{a,\mathbb{Q}}$ má stupeň, který není mocnina dvojky.)

*Trisekce úhlu.* Stačí najít jedno konkrétní zadání, které není řešitelné pravítkem a kružítkem. Uvažujme tedy úhel $60°$ zadaný body $(0, 0)$, $(1, 0)$ a $(\frac{1}{2}, \frac{\sqrt{3}}{2})$, tj. $\mathbf{T}_0 = \mathbb{Q}(\sqrt{3})$. Dokážeme, že není možné sestrojit bod

$$(\cos 20°, \sin 20°).$$

(Kdybychom zkonstruovali přímku se směrnicí $20°$ pomocí jiného bodu, dostaneme tento jako její průsečík s jednotkovou kružnicí.) Dokážeme-li, že

$$[\mathbb{Q}(\sqrt{3}, \cos 20°) : \mathbb{Q}(\sqrt{3})] = 3,$$

můžeme použít stejný argument jako pro zdvojení krychle. K tomuto cíli stačí podle Tvrzení 24.3 nalézt minimální polynom čísla $\cos 20°$ nad tělesem $\mathbb{Q}(\sqrt{3})$, tj. nějaký ireducibilní polynom, jehož je číslo $\cos 20°$ kořenem. Použijeme-li vzorec

$$\cos 3\alpha = 4(\cos \alpha)^3 - 3 \cos \alpha$$

(viz nějaká sbírka goniometrických vzorců), dostáváme $\cos 20°$ jako kořen polynomu $4x^3 - 3x - \frac{1}{2} \in \mathbb{Q}(\sqrt{3})[x]$. Tento polynom je v $\mathbb{Q}(\sqrt{3})[x]$ ireducibilní, neboť nemá v $\mathbb{Q}(\sqrt{3})$ kořen (jak snadno zjistíme dosazením $x = a + b\sqrt{3}$). Tedy

$$m_{\cos 20°, \mathbb{Q}(\sqrt{3})} = x^3 - \frac{3}{4}x - \frac{1}{8}$$

a dostáváme $[\mathbb{Q}(\sqrt{3}, \cos 20°) : \mathbb{Q}(\sqrt{3})] = \deg m_{\cos 20°, \mathbb{Q}(\sqrt{3})} = 3$.

## 26. Kořenová a rozkladová nadtělesa, algebraický uzávěr

**Cíl.** *Dokážeme existenci a jednoznačnost (až na izomorfismus) nejmenšího rozšíření daného tělesa na těleso, ve kterém (1) daný polynom má kořen; (2) daný polynom se rozkládá na lineární činitele; (3) každý polynom se rozkládá na lineární činitele.*

### 26.1. **Kořenová a rozkladová nadtělesa.**

Cílem tohoto odstavce je dokázat, že pro každý polynom $f \in T[x]$ existuje nejmenší rozšíření $\mathbf{S} \geq \mathbf{T}$, kde se $f$ rozkládá na lineární činitele (tj. polynomy stupně 1). Intuitivně je věc jasná: je-li $\mathbf{T} \leq \mathbb{C}$, pak stačí vzít $\mathbf{S} = \mathbf{T}(a_1, \ldots, a_n)$, kde $a_1, \ldots, a_n$ jsou komplexní kořeny polynomu $f$. Problémy jsou dva: jednak jsme nedokázali, že se $f$ nad komplexními čísly skutečně rozkládá (mimochodem, důkaz tohoto faktu, nazývaného Základní věta algebry, není vůbec snadný), ale, a to zejména, ne každé těleso je podtělesem $\mathbb{C}$.

Klíčovým krokem je důkaz Věty 26.1(1), kde se najde rozšíření, ve kterém existuje aspoň *nějaký* kořen. Dále stačí postupovat indukcí.

**Definice.** Řekneme, že $\mathbf{S} \geq \mathbf{T}$ je *kořenové nadtěleso* polynomu $f \in T[x]$, pokud má polynom $f$ v tělese $\mathbf{S}$ kořen $a$ a navíc $\mathbf{S} = \mathbf{T}(a)$.

**Věta 26.1.** *Buď $\mathbf{T}$ těleso a $f \in T[x]$ stupně $\geq 1$. Pak*

(1) *existuje kořenové nadtěleso polynomu $f$;*
(2) *je-li polynom $f$ ireducibilní v $\mathbf{T}[x]$, pak jsou každá dvě kořenová nadtělesa polynomu $f$ $\mathbf{T}$-izomorfní.*

Pod pojmem $\mathbf{T}$-*izomorfismus* se rozumí takový izomorfismus $\mathbf{U} \to \mathbf{V}$, jehož restrikce na množinu $T$ je identita.

*Důkaz.* (1) Buď $g$ nějaký ireducibilní dělitel polynomu $f$ a položme $I = gT[x]$. Toto je maximální ideál v oboru $\mathbf{T}[x]$, a tedy faktorokruh $\mathbf{S} = \mathbf{T}[x]/\mathbf{I}$ je podle Věty 22.5 těleso. Uvažujme homomorfismus

$$\psi : \mathbf{T} \to \mathbf{S}, \qquad a \mapsto [a].$$

Ten je prostý, protože prvky tělesa $\mathbf{T}$ (jakožto konstantní polynomy) nejsou v ideálu $\mathbf{I}$. Můžeme tedy ztotožnit těleso $\mathbf{T}$ s $\mathbf{Im}(\psi)$ (formálně vzato, jsou izomorfní) a budeme uvažovat, že $\mathbf{T} \leq \mathbf{S}$. Dosadíme-li do polynomu $g = \sum_{i=0}^{n} a_i x^i$ prvek $b = [x]$, dostaneme

$$g(b) = \sum_{i=0}^{n} a_i [x]^i = [\sum_{i=0}^{n} a_i x^i] = [g] = [0].$$

Prvek $b$ je tedy kořenem polynomu $g$, čili také polynomu $f$, v tělese $\mathbf{S}$. Přitom $\mathbf{S} = \mathbf{T}(b)$, protože už okruh $\mathbf{T}[x]$ je generován množinou $T \cup \{x\}$.

(2) Uvažujme dvě kořenová nadtělesa $\mathbf{T} \leq \mathbf{T}(a)$ a $\mathbf{T} \leq \mathbf{T}(b)$. Podle Tvrzení 24.2 a 19.2 je $T(a) = \{g(a) : g \in T[x]\}$ a $T(b) = \{g(b) : g \in T[x]\}$. Uvažujme tedy zobrazení

$$\varphi : T(a) \to T(b), \qquad g(a) \mapsto g(b).$$

Přesněji řečeno, je třeba dokázat, že to je skutečně zobrazení. Je důležité si uvědomit, že $f = m_{a,\mathbf{T}} = m_{b,\mathbf{T}}$ (protože je $f$ ireducibilní polynom splňující $f(a) = f(b) = 0$), a proto, podle definice minimálního polynomu,

$$g(a) = h(a) \;\Leftrightarrow\; (g-h)(a) = 0 \;\Leftrightarrow\; f \mid g-h \;\Leftrightarrow\; (g-h)(b) = 0 \;\Leftrightarrow\; g(b) = h(b).$$

Čili $\varphi$ je skutečně zobrazení, navíc prosté. Protože očividně zachovává všechny operace, je to izomorfismus $\mathbf{T}(a) \to \mathbf{T}(b)$. □

**Příklad.**

- Kořenové nadtěleso polynomu $x^2+1$ nad $\mathbb{Q}$ je těleso $\mathbb{Q}(i)$.
- Kořenové nadtěleso polynomu $x^2-1$ nad $\mathbb{Q}$ je těleso $\mathbb{Q}$.
- Kořenové nadtěleso polynomu $x^4-1$ nad $\mathbb{Q}$ je těleso $\mathbb{Q}$ i těleso $\mathbb{Q}(i)$ — to je možné, protože nejde o ireducibilní polynom.
- Obecně, kořenové nadtěleso polynomu $x^n-1$ nad $\mathbb{Q}$ je každé $\mathbb{Q}(e^{2k\pi i/n})$, $k = 0, \dots, n-1$.
- Kořenová nadtělesa polynomu $x^3-2$ nad $\mathbb{Q}$ jsou tělesa $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt[3]{2}\cdot e^{2\pi i/3})$ i $\mathbb{Q}(\sqrt[3]{2}\cdot e^{4\pi i/3})$. Podle předešlé věty jsou tato tělesa $\mathbb{Q}$-izomorfní.

**Definice.** Řekneme, že $\mathbf{S} \geq \mathbf{T}$ je *rozkladové nadtěleso* polynomu $f \in \mathbf{T}[x]$, pokud se polynom $f$ rozkládá v $\mathbf{S}[x]$ na lineární činitele, a navíc, kdykoliv $\mathbf{T} \leq \mathbf{U} < \mathbf{S}$, pak se polynom $f$ v $\mathbf{U}[x]$ na lineární činitele nerozkládá.

**Věta 26.2.** *Buď $\mathbf{T}$ těleso a $f \in T[x]$ stupně $\geq 1$. Pak*

(1) *existuje rozkladové nadtěleso polynomu $f$;*
(2) *každá dvě rozkladová nadtělesa polynomu $f$ jsou $\mathbf{T}$-izomorfní.*

*Důkaz.* (1) Budeme postupovat indukcí podle stupně polynomu $f$. Je-li $\deg f = 1$, pak je $\mathbf{S} = \mathbf{T}$. V opačném případě uvažujme kořenové nadtěleso $\mathbf{T}(a) \geq \mathbf{T}$ polynomu $f$ a polynom $g \in T(a)[x]$ takový že $f = g \cdot (x-a)$. Stupeň polynomu $g$ je menší, tedy z indukčního předpokladu existuje jeho rozkladové nadtěleso $\mathbf{S}$ nad $\mathbf{T}(a)$. Protože se $g$ rozkládá v $\mathbf{S}[x]$ na lineární činitele, rozkládá se tam i $f = g \cdot (x-a)$. Navíc těleso $\mathbf{S}$ je nejmenší takové: kdyby se polynom $f$ rozkládal v nějakém menším tělese, pak by se v něm rozkládal i polynom $g$, spor.

(2) Dokážeme indukcí o trochu obecnější tvrzení:

> *Buď $\mathbf{T}_1$ a $\mathbf{T}_2$ nadtělesa $\mathbf{T}$, $\varphi : \mathbf{T}_1 \to \mathbf{T}_2$ $\mathbf{T}$-izomorfismus, $f = \sum a_i x^i$ polynom z $\mathbf{T}_1[x]$, $\varphi(f) = \sum \varphi(a_i)x^i$ polynom z $\mathbf{T}_2[x]$ a označme $\mathbf{S}_1$ rozkladové nadtěleso $f$ nad $\mathbf{T}_1$ a $\mathbf{S}_2$ rozkladové nadtěleso $\varphi(f)$ nad $\mathbf{T}_2$. Pak $\mathbf{S}_1$ a $\mathbf{S}_2$ jsou $\mathbf{T}$-izomorfní.*

Dokazované tvrzení plyne dosazením $\mathbf{T}_1 = \mathbf{T}_2 = \mathbf{T}$ a $\varphi = id$.

Budeme opět postupovat indukcí podle stupně polynomu $f$. Je-li $\deg f = 1$, pak je $\mathbf{S}_1 = \mathbf{T}_1$ a $\mathbf{S}_2 = \mathbf{T}_2$ jediná volba. V opačném případě uvažujme ireducibilní dělitel $g$ polynomu $f$ a jeho kořen $a$ v $\mathbf{S}_1$. Pak $\varphi(g)$ je ireducibilní dělitel polynomu $\varphi(f)$ a $\varphi(a) \in S_2$ je jeho kořen, a tak podobně jako ve Větě 26.1(2) dostáváme, že $\mathbf{T}_1(a)$ a $\mathbf{T}_2(\varphi(a))$ jsou $\mathbf{T}$-izomorfní; označme $\psi$ tento $\mathbf{T}$-izomorfismus. Nyní použijeme indukční předpoklad: označíme-li $h \in T_1(a)[x]$ polynom splňující $f = (x-a)\cdot h$, tedy také $\psi(f) = (x - \psi(a)) \cdot \psi(h)$, pak rozkladové nadtěleso $\mathbf{S}_1$ polynomu $h$ nad $\mathbf{T}_1(a)$ a rozkladové nadtěleso $\mathbf{S}_2$ polynomu $\psi(h)$ nad $\mathbf{T}_2(\varphi(a))$ jsou $\mathbf{T}$-izomorfní, protože $\deg h < \deg f$. □

**Příklad.**

- Rozkladové nadtěleso polynomu $x^2+1$ nad $\mathbb{Q}$ je těleso $\mathbb{Q}(i)$.
- Rozkladové nadtěleso polynomu $x^2-1$ nad $\mathbb{Q}$ je těleso $\mathbb{Q}$.
- Rozkladové nadtěleso polynomu $x^4-1$ nad $\mathbb{Q}$ je těleso $\mathbb{Q}(i)$.
- Obecně, rozkladové nadtěleso polynomu $x^n-1$ nad $\mathbb{Q}$ je těleso $\mathbb{Q}(e^{2\pi i/n})$, tedy rozšíření stupně $n-1$.
- Rozkladové nadtěleso polynomu $x^3-2$ nad $\mathbb{Q}$ je těleso $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.
- Obecně, rozkladové nadtěleso polynomu $x^n-2$ nad $\mathbb{Q}$ je těleso $\mathbb{Q}(\sqrt[n]{2}, e^{2\pi i/n})$, tedy rozšíření stupně $n$.

## 26.2. **Algebraický uzávěr.**

**Definice.** Těleso $\mathbf{T}$ se nazývá *algebraicky uzavřené*, jestliže má každý polynom z $\mathbf{T}[x]$ stupně $\geq 1$ v tělese $\mathbf{T}$ kořen.

V algebraicky uzavřeném tělese se každý polynom rozkládá na lineární činitele, což můžeme snadno dokázat indukcí podle $\deg f$: pro polynomy stupně 1 je tvrzení triviální; pro vyšší stupně využijeme existenci nějakého kořene $a$, vydělíme $f$ polynomem $x-a$, čímž získáme polynom menšího stupně a ten rozložíme pomocí indukčního předpokladu.

**Příklad.** Těleso $\mathbb{C}$ je algebraicky uzavřené. Tomuto tvrzení se říká *Základní věta algebry* a její důkaz lze nejsnadněji provést pomocí komplexní analýzy. Ač se její platnost dlouho tušila, poprvé byla se všemi detaily dokázána Gaussem až kolem roku 1800.

**Poznámka.** Žádné konečné těleso nemůže být algebraicky uzavřené. Označíme-li $a_1, \ldots, a_n$ jeho prvky, pak polynom $(x-a_1)\cdot\ldots\cdot(x-a_n)+1$ nemá v tomto tělese kořen.

**Definice.** Řekneme, že $\mathbf{S} \geq \mathbf{T}$ je *algebraický uzávěr* tělesa $\mathbf{T}$, pokud je $\mathbf{S}$ algebraicky uzavřené těleso a zároveň je algebraickým rozšířením tělesa $\mathbf{T}$.

**Příklad.**

- Algebraický uzávěr tělesa $\mathbb{R}$ je těleso $\mathbb{C}$; je to rozšíření stupně 2, tedy algebraické.
- Algebraický uzávěr tělesa $\mathbb{Q}$ není těleso $\mathbb{C}$, neboť nejde o algebraické rozšíření. Algebraický uzávěr $\mathbb{Q}$ popisuje následující tvrzení.

**Tvrzení 26.3.** *Buď $\mathbf{S}$ rozšíření tělesa $\mathbf{T}$. Pak*

(1) *množina*

$$U = \{a \in S : \ a \text{ je algebraický prvek nad } \mathbf{T}\}$$

*tvoří podtěleso tělesa $\mathbf{S}$;*

(2) *je-li těleso $\mathbf{S}$ je algebraicky uzavřené, pak $\mathbf{U}$ je algebraický uzávěr tělesa $\mathbf{T}$.*

*Důkaz.* (1) Nechť $a, b \in U$ a uvažujme těleso $\mathbf{T}(a,b)$. Protože jsou $a, b$ algebraické prvky nad $\mathbf{T}$, jde o rozšíření konečného stupně (Věta 24.5), a tudíž o rozšíření algebraické (Tvrzení 24.1). Čili $T(a,b) \subseteq U$ a speciálně tedy $U$ obsahuje prvky $a+b$, $a\cdot b$, $-a$ i $a^{-1}$ (pro $a \neq 0$). Takže $U$ tvoří podtěleso.

(2) Evidentně je $\mathbf{U}$ algebraické rozšíření tělesa $\mathbf{T}$. Je algebraicky uzavřené? Uvažujme libovolný polynom

$$f = \sum_{i=0}^{n} a_i x^i \in U[x].$$

Tento polynom má jistě kořen $b \in S$, protože je těleso $\mathbf{S}$ algebraicky uzavřené. Přitom prvek $b$ je algebraický nad tělesem $\mathbf{T}(a_0, \ldots, a_n)$, protože ve skutečnosti $f \in T(a_0, \ldots, a_n)[x]$. Z Tvrzení 24.3 tak plyne, že je stupeň $[\mathbf{T}(a_0, \ldots, a_n, b) : \mathbf{T}(a_0, \ldots, a_n)]$ konečný. Přitom stupeň $[\mathbf{T}(a_0, \ldots, a_n) : \mathbf{T}]$ je také konečný, neboť $a_0, \ldots, a_n$ jsou algebraické nad $\mathbf{T}$, a tak podle Tvrzení 24.4 je stupeň

$$[\mathbf{T}(a_0, \ldots, a_n, b) : \mathbf{T}] = [\mathbf{T}(a_0, \ldots, a_n, b) : \mathbf{T}(a_0, \ldots, a_n)] \cdot [\mathbf{T}(a_0, \ldots, a_n) : \mathbf{T}]$$

také konečný. Tedy podle Tvrzení 24.1 je prvek $b$ algebraický nad $\mathbf{T}$, a tak kořen $b$ polynomu $f$ leží v $\mathbf{U}$. □

Z tohoto tvrzení plyne, že algebraický uzávěr nekonečného tělesa má stejnou velikost jako dané těleso. Argument je analogický důkazu, že algebraických čísel nad $\mathbb{Q}$ je jen spočetně mnoho, který jsme viděli v první kapitole.

**Věta 26.4.** *Ke každému tělesu $\mathbf{T}$ existuje algebraický uzávěr. Každé dva algebraické uzávěry tělesa $\mathbf{T}$ jsou $\mathbf{T}$-izomorfní.*

K důkazu této věty je nezbytné tzv. Zornovo lemma, ekvivalentní formulace axiomu výběru. Čtenář, který toto základní tvrzení teorie množin nezná, musí kroky, kde se Zornovo lemma používá, brát jako fakt. Důkaz jednoznačnosti navíc pouze naznačíme, neboť v něm je užití Zornova lemmatu stěžejní a i předchozí teorii kořenových nadtěles bychom museli dělat podrobněji, abychom byli schopni zapsat důkaz pořádně.

**Lemma 26.5.** *Ke každému tělesu $\mathbf{T}$ existuje rozšíření $\mathbf{S} \geq \mathbf{T}$ takové, že každý polynom z $\mathbf{T}[x]$ má v $\mathbf{S}$ kořen.*

*Důkaz.* Důkaz je analogický konstrukci kořenového nadtělesa daného polynomu; budeme konstruovat něco jako „kořenové nadtěleso pro všechny polynomy zároveň".

Buď tedy $X$ množina proměnných taková, že každému polynomu z $\mathbf{T}[x]$ odpovídá jedna proměnná; formálně, položme

$$X = \{x_f : f \in T[x]\}.$$

Uvažujme nyní okruh $\mathbf{T}[X]$ (polynomy s proměnnými z $X$). Podle Zornova lemmatu existuje maximální ideál $\mathbf{I}$ obsahující všechny polynomy $f(x_f)$, $f \in T[x]$ (za proměnnou $x$ v polynomu $f$ substituujeme proměnnou $x_f$). Faktorokruh $\mathbf{S} = \mathbf{T}[X]/\mathbf{I}$ je podle Věty 22.5 těleso a podobně jako v důkazu Věty 26.1 se dokáže, že do něj lze vnořit těleso $\mathbf{T}$ (vnoření $t \mapsto [t]$) a že každý polynom $f \in T[x]$ má v $\mathbf{S}$ kořen, konkrétně $[x_f]$. □

*Důkaz Věty 26.4.* Uvažujme řetězec nadtěles $\mathbf{T} = \mathbf{S}_0 \leq \mathbf{S}_1 \leq \mathbf{S}_2 \leq \ldots$, kde $\mathbf{S}_{i+1}$ vznikne z $\mathbf{S}_i$ konstrukcí z předchozího lemmatu. Položme $\mathbf{S} := \bigcup_{i=0}^{\infty} \mathbf{S}_i$. Toto je také těleso. Přitom je algebraicky uzavřené, neboť každý polynom $f \in S[x]$ má jen konečně mnoho koeficientů, tedy $f \in S_i[x]$ pro nějaké (dostatečně velké) $i$, a tedy $f$ má kořen v $\mathbf{S}_{i+1}$, čili také v $\mathbf{S}$. Algebraický uzávěr získáme aplikací Tvrzení 26.3.

Důkaz jednoznačnosti se dělá tak, že se vezme uspořádaná množina $M$ všech částečných $\mathbf{T}$-izomorfismů mezi danými dvěma algebraickými uzávěry; o ní se dokáže, že splňuje předpoklady Zornova lemmatu, a tedy v ní existuje maximální prvek; pak se dokáže, že každý částečný izomorfismus, který není úplný, lze rozšířit; z čehož plyne, že maximální prvek množiny $M$ je $\mathbf{T}$-izomorfismus těch dvou těles. Detaily uvádět nebudeme, čtenář může nahlédnout do nějaké obsažnější učebnice, jako např. [Pro90]. □

## 27. * Konečná tělesa

**Cíl.** *V této sekci popíšeme všechna konečná tělesa.*

Ukážeme, že pro každou mocninu prvočísla $p^k$ existuje, až na izomorfismus, právě jedno těleso velikosti $p^k$. Struktura důkazu je následující: nejprve si uvědomíme, že jiné velikosti než mocniny prvočísla nejsou možné, protože jde o vektorové prostory nad $\mathbb{Z}_p$. Pak ukážeme, že každé konečné těleso velikosti $p^k$ je rozkladovým nadtělesem polynomu $x^{p^k} - x$ nad $\mathbb{Z}_p$, čímž jejich existence i jednoznačnost poplynou z Věty 26.2.

**Lemma 27.1.** *Je-li* $\mathbf{T}$ *konečné těleso, pak* $|T| = p^k$ *pro nějaké prvočíslo* $p$ *a přirozené číslo* $k$*.*

*Důkaz.* Označme $p$ charakteristiku tělesa $\mathbf{T}$. Pak $\mathbb{Z}_p$ je jeho prvotělesem, čili $\mathbf{T}$ je rozšířením tělesa $\mathbb{Z}_p$ konečného stupně, čili $\mathbf{T}_{\mathbb{Z}_p}$ je konečnědimenzionální vektorový prostor nad $\mathbb{Z}_p$, a tak musí být izomorfní vektorovému prostoru $(\mathbb{Z}_p)^k$ pro nějaké $k$. □

**Lemma 27.2.** *Rozkladové nadtěleso polynomu* $x^{p^k} - x$ *nad* $\mathbb{Z}_p$ *má* $p^k$ *prvků.*

*Důkaz.* Uvažujme nějaké rozkladové nadtěleso $\mathbf{T}$ polynomu $f = x^{p^k} - x$. Ukážeme, že jeho kořeny jsou v $\mathbf{T}$ uzavřeny na všechny operace tělesa. Tvrzení 19.8 o Frobeniově endomorfismu říká, že $(a + b)^p = a^p + b^p$ pro všechna $a, b$ a $k$-násobnou aplikací tohoto vzorce dostaneme, že $(a+b)^{p^k} = a^{p^k} + b^{p^k}$. Tedy, jsou-li $a, b$ kořeny polynomu $f$, tj. $a^{p^k} = a$ a $b^{p^k} = b$, pak $(a \pm b)^{p^k} = a^{p^k} \pm b^{p^k} = a \pm b$ je také kořen $f$ a stejně tak $(a \cdot b)^{p^k} = a^{p^k} \cdot b^{p^k} = a \cdot b$ a $(a^{-1})^{p^k} = (a^{p^k})^{-1} = a^{-1}$. Z minimality rozkladového nadtělesa plyne, že $\mathbf{T}$ sestává právě z kořenů $f$ a tedy že má $\leq \deg f = p^k$ prvků.

K dokončení zbývá dokázat, že polynom $f$ nemá vícenásobné kořeny (tj. že počet prvků je přesně $p^k$). Kdyby byl prvek $a$ vícenásobným kořenem $f$, pak by podle Věty 10.2 polynom $x - a$ dělil jak $f$, tak $f'$. Ovšem $\mathrm{NSD}(f, f') = 1$, jak čtenář snadno ověří Eukleidovým algoritmem. □

**Lemma 27.3.** *Je-li* $\mathbf{T}$ *konečné těleso a* $|T| = p^k$*, pak je* $\mathbf{T}$ *rozkladovým nadtělesem polynomu* $x^{p^k} - x$ *nad* $\mathbb{Z}_p$*.*

*Důkaz.* Uvažujme grupu $\mathbf{T}^*$: ta má $p^k - 1$ prvků, tedy podle Lagrangeovy věty $a^{p^k-1} = 1$ pro každé $a \in T^*$, a tak $a^{p^k} = a$ pro každé $a \in T$ (včetně nuly). Jinými slovy, každý prvek tělesa $\mathbf{T}$ je kořenem uvedeného polynomu, ten se tedy v $\mathbf{T}$ rozkládá na lineární činitele a $\mathbf{T}$ je jeho rozkladovým nadtělesem. □

**Důsledek 27.4.**

(1) *Konečné těleso velikosti* $n$ *existuje právě tehdy, když* $n = p^k$ *pro nějaké prvočíslo* $p$ *a přirozené číslo* $k$*.*
(2) *Konečná tělesa stejné velikosti jsou izomorfní.*

*Důkaz.* (1) ($\Rightarrow$) plyne z Lemmatu 27.1, ($\Leftarrow$) plyne z Lemmatu 27.2 a (2) plyne z Lemmatu 27.3 a Věty 26.2 (2). □

Konečné těleso velikosti $p^k$ se značí $\mathbb{F}_{p^k}$ (někteří autoři používají též značení $\mathbf{GF}(p^k)$, jako *Galois field*). Buď $a$ generátor cyklické grupy $\mathbb{F}^*_{p^k}$ (viz Věta 14.13). Pak $\mathbb{F}_{p^k} = \mathbb{Z}_p(a)$ a jde o kořenové nadtěleso minimálního polynomu $m_{a,\mathbb{Z}_p}$. Pohledem do důkazu Věty 26.1 o konstrukci kořenových nadtěles zjistíme, že

$$\mathbb{F}_{p^k} = \mathbb{Z}_p(a) \simeq \mathbb{Z}_p[x]/m_{\mathbb{Z}_p,a}.$$

Získali jsme tak velmi užitečnou reprezentaci tělesa $\mathbb{F}_{p^k}$ jako faktorokruhu $\mathbb{Z}_p[x]$ podle ireducibilního polynomu stupně $k$. Z Věty 27.4 tak mimochodem plyne, že pro každé $k$ takový polynom v $\mathbb{Z}_p[x]$ existuje.

**Příklad.**

- $\mathbb{F}_p = \mathbb{Z}_p$.
- $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2+x+1)$, $\mathbb{F}_8 = \mathbb{Z}_2[x]/(x^3+x+1)$, $\mathbb{F}_9 = \mathbb{Z}_3[x]/(x^2+1)$.
- $\mathbb{F}_{p^k}$ není ani $\mathbb{Z}_{p^k}$, ani $(\mathbb{Z}_p)^k$, protože to vůbec nejsou tělesa!

**Poznámka.** Podle Lemmatu 27.3 je $\mathbb{F}_{p^k}$ rozkladové nadtěleso polynomu $f = x^{p^k} - x$ nad $\mathbb{Z}_p$. Z důkazu Lemmatu 27.2 vidíme, že toto těleso sestává právě z kořenů polynomu $f$. Dostáváme tak následující vztah v oboru $\mathbb{F}_{p^k}[x]$:

$$x^{p^k} - x = \prod_{a \in \mathbb{F}_{p^k}} (x - a).$$

Konečná tělesa nacházejí řadu uplatnění, např. v teorii kódů. Pro hlubší studium lze doporučit text [Bar].

Obsah