Nauč sa matiku – abstraktná algebra

Valdemar Švábenský

28. augusta 2015

Predslov

Tento učebný text z oblasti abstraktnej algebry vznikol v rámci prípravy na jeden z najťažších a zároveň najzaujímavejších matematických kurzov, aký som mal tú časť absolvovať: *MV008 Algebra I* na Fakulte informatiky Masarykovej univerzity pod vedením doc. RNDr. Libora Poláka, CSc. Text vznikal postupne počas piatich mesiacov ako učebný materiál na skúšku. Neskôr som sa ho rozhodol zverejniť v rámci projektu Nauč sa matiku. Je určený primárne pre študentov vysokých škôl (2. ročník a vyššie). Predpokladajú sa základné znalosti logiky a teórie množín a tiež schopnosti čítať matematickú notáciu a abstraktne matematicky myslieť.

Celý dokument je rozdelený do deviatich kapitol (číslovaných 1 až 9), ktoré sú v istých prípadoch rozdelené do podkapitol (napríklad 1.1, 1.2, 1.3). Posledná kapitola obsahuje aplikácie v teórii jazykov, ktorá je dôležitá hlavne pre informatikov.

Otázky a akákoľvek spätná väzba, či už poďakovanie, vyhrážky, oprava chýb, konštruktívna kritika, návrhy na zlepšenie, alebo pozvanie na pivo sú vítané. Kontakt na mňa je k dispozícii na webe `http://www.naucsamatiku.com`. Držím palce všetkým, ktorí sa rozhodli venovať štúdiu tejto krásnej oblasti matematiky.

Valdemar

Licencia a právo na použitie

Obsah

Poďakovanie

- Ďakujem Matúšovi Nemcovi za pravidelné skenovanie a posielanie poznámok z cvičení.
- Ďakujem Jurajovi Majorovi za korektúru textu.

Kapitola 1: Zobrazenia, operácie, grupy

1.1 Základné pojmy

Číselné množiny:

- $\mathbb{N} = \{1, 2, 3, \ldots\}$ je množina prirodzených čísel,
- $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ je množina nezáporných celých čísel,
- $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ je množina celých čísel,
- $\mathbb{Q} = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}$ je množina racionálnych čísel,
- $\mathbb{R}$ je množina reálnych čísel, t. j. všetkých čísel, ktoré sú hodnotou na číselnej osi,
- $\mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$ je množina iracionálnych čísel,
- $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ je množina komplexných čísel.
- $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$.
- X^+ je množina všetkých kladných prvkov z $X \subseteq \mathbb{R}$,
- X^* je množina všetkých nenulových prvkov z $X \subseteq \mathbb{C}$.

Definícia 1.1. *Karteziánsky súčin* množín: $A \times B = \{(a, b) \mid a \in A \wedge b \in B\}$.

- $A^n = \underbrace{A \times \cdots \times A}_{n\text{-krát}}$.

Definícia 1.2. *Relácia* medzi množinami $A_1, \ldots, A_n$ je podmnožinou $A_1 \times \ldots \times A_n$.

Definícia 1.3. *Zobrazenie* (funkcia) z množiny A do množiny B je relácia f medzi množinami A, B taká, že pre každé $x \in A$ existuje *práve jedno* $y \in B$ také, že $(x, y) \in f$.

- Namiesto $(x, y) \in f$ píšeme obvykle $f(x) = y$.
- Množina A sa nazýva *definičný obor* $D(f)$ a množina B *obor hodnôt* $H(f)$ funkcie.
- Zápis $f\colon A \to B$ hovorí, že f je funkcia s $D(f) = A$ a $H(f) = B$.

Definícia 1.4. Nech $n \in \mathbb{N}_0$. Zobrazenie $f\colon A^n \to A$ je n-árna *operácia* na množine A.

- Ak $n = 0$, tak $A^n = \{\emptyset\}$. Nulárne operácie sú teda výbery prvkov z množiny A.
- Najčastejšie používame binárne operácie: $+, \cdot, \ldots$ Značíme $\cdot(a, b) = a \cdot b = ab$.

1.2 Vlastnosti binárnych operácií

Binárna operácia $\cdot$ na množine A sa nazýva:

- **asociatívna**, ak $\forall\, a, b, c \in A$: $\quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- **komutatívna**, ak $\forall\, a, b \in A$: $\quad a \cdot b = b \cdot a$,
- **idempotentná**, ak $\forall\, a \in A$: $\quad a \cdot a = a$.

Prvok $e \in A$ nazývame:

- **ľavý neutrálny** (jednotkový), ak $\forall\, a \in A$: $\quad e \cdot a = a$,
- **pravý neutrálny** (jednotkový), ak $\forall\, a \in A$: $\quad a \cdot e = a$,
- **neutrálny** (jednotkový), ak je ľavý neutrálny a zároveň pravý neutrálny;
- **ľavý nulový**, ak $\forall\, a \in A$: $\quad e \cdot a = e$,
- **pravý nulový**, ak $\forall\, a \in A$: $\quad a \cdot e = e$,
- **nulový**, ak je ľavý nulový a zároveň pravý nulový;
- **idempotent**, ak $e \cdot e = e$.

Ak $e \in A$ je neutrálnym prvkom, tak prvok $b \in A$ nazývame:

- **ľavá inverzia** prvku $a \in A$, ak $b \cdot a = e$,
- **pravá inverzia** prvku $a \in A$, ak $a \cdot b = e$,
- **inverzia** prvku $a \in A$, ak je jeho ľavou a zároveň pravou inverziou. (Hovoríme, že a je *invertibilný*.)

1.3 Grupové štruktúry

Definícia binárnej operácie vlastne hovorí, že binárna operácia je definovaná pre ľubovoľné dva prvky danej množiny a zaručuje *úplnosť* (= uzavretosť množiny na danú operáciu).

Definícia 1.5. Štyri základné grupové štruktúry sú:

- **Grupoid** (*magma*) je usporiadaná dvojica $(A, \cdot)$.
- **Pologrupa** (*semigroup*) je grupoid, v ktorom je operácia $\cdot$ asociatívna.
- **Monoid** (*monoid*) je pologrupa s neutrálnym prvkom e.
- **Grupa** (*group*) je monoid, v ktorom má každý prvok inverziu.

Grupová štruktúra je *komutatívna*, ak je v nej daná operácia $\cdot$ komutatívna.
Zadanie grupoidu: Cayleyho tabuľkou prvkov / analyticky / prezentáciou (pozri 1.56).
Vyčítanie vlastností z tabuľky: asociativita – ťažko ($O(n^3)$), komutativita – symetria podľa diagonály ($O(n^2)$), idempotencia – z diagonály.

Lemma 1.6. *Nech $(A, \cdot)$ je grupoid, $e \in A$ je ľavý neutrálny (jednotkový) prvok, $f \in A$ je pravý neutrálny (jednotkový) prvok. Potom $e = f$.*

Dôkaz. $f = e \cdot f = e$. □

Dôsledok 1.7. *V grupoide môže byť: a) žiadny neutrálny prvok, b) $k \in \mathbb{N}$ ľavých neutrálnych, 0 pravých neutrálnych, c) $l \in \mathbb{N}$ pravých neutrálnych, 0 ľavých neutrálnych, d) jediný neutrálny prvok.*

Lemma 1.8. *Nech $(S, \cdot)$ je pologrupa s jednotkovým prvkom e. Potom ku každému prvku $x \in S$ existuje najviac jedna inverzia.*

Dôkaz. Nech x má dve rôzne inverzie $y, z \in S$. Potom $xy = yx = e$ a tiež $xz = zx = e$. Ďalej $(yx)z = ez = z$ a tiež z asociativity $(yx)z = y(xz) = ye = y$ ※ . □

Lemma 1.9. *Nech $(M, \cdot, e)$ je monoid, $a \in M$, $b \in M$ je ľavou inverziou k a, $c \in M$ je pravou inverziou k a. Potom $b = c$.*

Dôkaz. $(ba)c = ec = c$, a tiež z asociativity $(ba)c = b(ac) = be = b$. □

Lemma 1.10. *V ľubovoľnej grupe existuje jediný idempotentný prvok.*

Dôkaz. Nech $a \in G$ je idempotentný prvok, t. j. $a = a \cdot a$. Vynásobíme obe strany rovnice inverziou prvku a. Potom $a \cdot a^{-1} = a \cdot a \cdot a^{-1}$, teda $e = ae$, teda $a = e$. □

Príklad 1.11. Tabuľka číselných množín a klasických binárnych operácií:

	$+$	$-$	$\cdot$	$\div$
$\mathbb{N}$	pologrupa	(nič)	monoid	(nič)
$\mathbb{N}_0$	monoid	(nič)	monoid	(nič)
$\mathbb{Z}$	grupa	grupoid	monoid	(nič)
$\mathbb{Q}$	grupa	grupoid	monoid	(nič)
$\mathbb{R}$	grupa	grupoid	monoid	(nič)
$\mathbb{C}$	grupa	grupoid	monoid	(nič)

Príklad 1.12. Príklady grupových štruktúr:

- **Nekomut. grupoid**, ktorý nie je pologrupou: $(\mathbb{R}^3, \times)$, kde $\times$ je vektorový súčin.
- **Komutatívny grupoid**, ktorý nie je pologrupou: $(\mathbb{N}, \oplus)$, kde $a \oplus b = ab + a^2 + b^2$.
- **Nekomutatívna pologrupa**, ktorá nie je monoidom: $(\{\left(\begin{smallmatrix} a & b \\ 0 & 0 \end{smallmatrix}\right) \mid a, b \in \mathbb{R}, a \neq 0\}, \cdot)$.
- **Komutatívna pologrupa**, ktorá nie je monoidom: $(\mathbb{N}, nsd)$.
- **Nekomutatívny monoid**, ktorý nie je grupou: $(\{a, b\}^*, \cdot)$, kde $\cdot$ je zreťazenie slov.

- **Komutatívny monoid**, ktorý nie je grupou: $(\{0,1\}, \wedge)$.
- **Nekomutatívna grupa**: $(\mathbb{S}_3, \circ)$.
- **Komutatívna (Abelovská) grupa**: triviálna grupa $(\{e\}, \cdot)$.

Príklad 1.13. Nasledovné množiny matíc s operáciou sčítania matíc tvoria grupy pre $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ alebo $\mathbb{C}$:

- $Mat_{mn}(R)$ je množina všetkých matíc typu $m \times n$ nad R.
- $GL_n(R)$ je množina všetkých regulárnych matíc rádu n nad R.
- $SL_n(R)$ je množina všetkých matíc rádu n nad R a determinantom rovným 1.
- Posledné dve tvoria grupu s násobením pre $R = \mathbb{Q}$, $\mathbb{R}$ alebo $\mathbb{C}$.

Príklad 1.14. $(\mathbb{N}, nsd)$ je pologrupa, $(\mathbb{N}_0, nsd)$ je monoid, $(\mathbb{Z}, nsd)$ je monoid.

Príklad 1.15. $(\mathbb{N}, nsn)$ je monoid, $(\mathbb{N}_0, nsn)$ je monoid, $(\mathbb{Z}, nsn)$ je monoid.

Definícia 1.16. Nech X je množina. $P(X) = 2^X$ je množina všetkých jej podmnožín.

Príklad 1.17. $(P(X), \cap)$ je kom. monoid, $(P(X), \cup)$ je kom. monoid, $(P(X), \setminus)$ je nekom. grupoid, $(P(X), ^C)$ neuvažujeme (doplnok nie je binárna operácia) a $(P(X), \triangle)$ je kom. grupa. Špeciálnym prípadom je $X = \emptyset$.

Príklad 1.18. Nech A je neprázdna množina a $X_1, \ldots, X_n \subseteq A$. Uvažujme operácie $\cap, \cup, ^C$. Dva množinové výrazy sú ekvivalentné práve vtedy, keď pri ľubovoľnom dosadení za $X_1, \ldots, X_n$ dostaneme to isté. Počet tried ekvivalencie je 2^{2^n}.

1.4 Skladanie zobrazení

Definícia 1.19. Nech A, B sú množiny. Kladieme:

- $B^A = \{f \mid f\colon A \to B\}$ je množina všetkých zobrazení množiny A do množiny B.
- $T(A) = A^A$ je množina všetkých zobrazení množiny A do seba (tzv. *transformácie*).
- $S(A)$ je množina všetkých bijekcií množiny A do seba (tzv. *permutácie*).

Definícia 1.20. Nech $f\colon A \to B$, $g\colon B \to C$ sú zobrazenia. Potom ich *zloženie* (v tomto poradí) je $(g \circ f)(x) = g(f(x))$, kde $(g \circ f)\colon A \to C$.

Lemma 1.21. *Skladania zobrazení sú asociatívne.*

Dôkaz. Máme množiny A, B, C, D a zobrazenia f, g, h, pričom $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$. Potom $[(h \circ g) \circ f](x) = (h \circ g)(f(x)) = h(g(f(x)))$ aj $[h \circ (g \circ f)](x) = h((g \circ f)(x)) = h(g(f(x)))$. □

Lemma 1.22. *Identita je neutrálnym prvkom pri operácii skladania zobrazení.*

Dôkaz. $\forall x \in A\colon f(f^{-1}(x)) = f^{-1}(f(x)) = x$, t. j. $f \circ f^{-1} = f^{-1} \circ f = id$. □

Dôsledok 1.23. *Množina všetkých binárnych relácií s operáciou skladania* $(P(A \times A), \circ)$ *je monoid. Táto štruktúra je grupou, práve keď* $A \neq \emptyset$.

Poznámka. Pre skladanie relácií platí:

$$S \circ R = \{(a, c) \mid \exists b \in B \colon (a, b) \in R \wedge (b, c) \in S\}, \text{ pričom } S \circ R \subseteq A \times C.$$

Dôsledok 1.24. *Množina všetkých transformácií s operáciou skladania* $(T(A), \circ)$ *je monoid. Táto štruktúra je grupou, práve keď* $|A| \leq 1$.

Dôsledok 1.25. *Množina všetkých prostých transformácií s operáciou skladania* $(T_{inj}(A), \circ)$ *je monoid. Táto štruktúra je grupou, práve keď* A *je konečná.*

Definícia 1.26. Nech $f \colon A \to B$ je funkcia. Potom f je *invertibilná*, ak existuje funkcia $f^{-1} \colon B \to A$, pričom $f(x) = y \iff f^{-1}(y) = x$.

- Ak je f prostá (injektívna), potom je aj invertibilná.
- Ak je f invertibilná, potom f^{-1} je jedinečná.
- Ak sú f, f^{-1} (totálne) funkcie, potom sú obe bijekcie.

1.5 Permutácie

Množina permutácií je množina $S(A) = \{f \mid f \colon A \to A\}$, kde f je bijektívne zobrazenie. Permutácia (teda prvok tejto množiny) je vlastne (invertibilná) funkcia.

Dôsledok 1.27. $(S(A), \circ)$ *je grupa. Táto grupa je komutatívna pre* $|A| \leq 2$.

Definícia 1.28. Obvykle uvažujeme $A = \{1, \ldots, n\}$ a píšeme $S(\{1, \ldots, n\}) = S_n = \mathbb{S}_n$, kde $n \in \mathbb{N}$. Grupa $(S_n, \circ)$ sa nazýva *symetrická grupa* stupňa n.

Veta 1.29. $|S_n| = n!$.

Definícia 1.30. Nech $k \in \mathbb{N}$, $k \geq 2$. Nech $i_1, \ldots, i_k \in \{1, \ldots, n\}$ sú po dvoch rôzne. Permutácia $f \in S_n$ definovaná vzťahom

$$\begin{aligned} f(i_j) &= i_{j+1} \quad \text{pre } j = 1, \ldots, k-1; \\ f(i_j) &= i_1 \quad \text{pre } j = k; \\ f(i) &= i \quad \text{pre } i \notin \{i_1, \ldots, i_k\}; \end{aligned}$$

sa nazýva *cyklus* dĺžky k. Píšeme $f = (i_1, \ldots, i_k)$.

- Cykly $(i_1, \ldots, i_k)$ a $(j_1, \ldots, j_l)$ sú *nezávislé*, ak $\{i_1, \ldots, i_k\} \cap \{j_1, \ldots, j_l\} = \emptyset$.
- *Transpozícia* je cyklus dĺžky 2.

Veta 1.31. *Nezávislé cykly komutujú.*

Veta 1.32. *Ľubovoľná permutácia* $f \in S_n$ *sa dá rozložiť na súčin nezávislých cyklov. Tento rozklad je daný jednoznačne (až na poradie činiteľov).*

Dôkaz. Nech π je permutáciou na S_n. Vezmime nejaké $x \in \{1, \ldots, n\}$. Definujme $\pi^0(x) = x$ (identická permutácia), $\pi^{k+1}(x) = \pi(\pi^k(x))$, kde $k \in \mathbb{N}_0$.

Keďže $\{1, \ldots, n\}$ je konečná množina, aj postupnosť $x, \pi(x), \pi^2(x), \ldots$ je konečná. Preto existuje nejaké „opakovanie“, teda $\exists k < l$: $\pi^k(x) = \pi^l(x)$. Z toho $x = \pi^{l-k}(x)$.

Permutáciu π potom môžeme zapísať ako cyklus $\pi = (x, x_1, x_2, \ldots, x_{l-k})$.

Ak v množine $\{1, \ldots, n\}$ ešte existujú nejaké prvky, ktoré sme nevyužili, vezmeme nejaké y, ktoré sa nevyskytuje v cykle $(x, x_1, x_2, \ldots, x_{l-k})$ a proces zopakujeme. Tým získame cyklus $\sigma = (y, y_1, y_2, \ldots, y_m)$. Cykly π a σ sú zjavne nezávislé.

Proces opakujeme, kým nevyužijeme všetky prvky z množiny $\{1, \ldots, n\}$. □

Poznámka. Súčin nula činiteľov chápeme ako identickú permutáciu *id*.

Veta 1.33. *Ľubovoľná permutácia $f \in S_n$ sa dá rozložiť na súčin transpozícií.*

Dôkaz. $(i_1, \ldots, i_k) = (i_1, i_k) \circ \cdots \circ (i_1, i_3) \circ (i_1, i_2)$. Rozklad nie je jednoznačný. □

- Ak je počet činiteľov v takom rozklade párny, hovoríme o *párnej* permutácii.
- Ak je počet činiteľov v takom rozklade nepárny, hovoríme o *nepárnej* permutácii.

Definícia 1.34. Grupa párnych permutácií je tzv. *alternujúca*. $A_n = \{f \in S_n \mid f \text{ je párna}\}$.

Veta 1.35. $|A_n| = \frac{n!}{2}$.

Definícia 1.36. *Inverzia* permutácie $f \in S_n$ je usporiadaná dvojica (i, j) taká, že $i, j \in \{1, \ldots, n\}$ a platí: $i < j$ a $f(i) > f(j)$.

- Párna permutácia ($sgn(f) = 1$) má párny počet inverzií.
- Nepárna permutácia ($sgn(f) = -1$) má nepárny počet inverzií.

Lemma 1.37. *Súčin k transpozícií je párny, práve keď k je párne* [2, I.2.8].

Lemma 1.38. *Pre $f, g \in S_n$ platí: $sgn(f \circ g) = sgn(f) \cdot sgn(g)$* [2, I.2.9].

1.6 Rád grupy

Lemma 1.39. *Nech $(S, \cdot)$ je pologrupa, $a_1, \ldots, a_n \in S$, kde $n \in \mathbb{N}$. Potom výsledok súčinu $a_1 \cdot \ldots \cdot a_n$ (v tomto poradí) nezáleží na zátvorkovaní.*

Dôkaz. Báza: $n = 1, 2, 3$ – triviálne (z asociativity).

IP: nezáleží na zátvorkovaní pre výsledok súčinu $a_1 \cdot \ldots \cdot a_k$, kde $k < n$.

IK: Ak $n \geq 4$ a $k \geq 2$, tak $(a_1 \cdot \ldots \cdot a_k) \cdot (a_{k+1} \cdot \ldots \cdot a_n) = (a_1 \cdot (a_2 \cdot \ldots \cdot a_k)) \cdot (a_{k+1} \cdot \ldots \cdot a_n) = a_1 \cdot ((a_2 \cdot \ldots \cdot a_k) \cdot (a_{k+1} \cdot \ldots \cdot a_n))$. □

Dôsledok 1.40. *V pologrupách nemusíme pri násobení prvkov písať zátvorky.*

Lemma 1.41. *Nech $(S, \cdot)$ je komutatívna pologrupa, $a_1, \ldots, a_n \in S$, kde $n \in \mathbb{N}$. Potom výsledok súčinu $a_1 \cdot \ldots \cdot a_n$ nezáleží na poradí.*

Dôkaz. Báza: $n = 1, 2$ – triviálne (z komutativity).

Ak $n \geq 3$ a nezáleží na zátvorkovaní, môžeme ľubovoľnú permutáciu prvkov $a_1, \ldots, a_n$ po dvoch zátvorkovať a postupne vymieňať, kým sa všetky nedostanú na svoje miesto. □

Definícia 1.42. Nech $(S, \cdot)$ je pologrupa, $a \in S$, $n \in \mathbb{N}$. Potom $a^n = \underbrace{a \cdot \ldots \cdot a}_{n\text{-krát}}$.

Tento súčin je podľa 1.39 definovaný jednoznačne.

Naviac, ak S obsahuje neutrálny prvok e, tak $a^0 = e$.

Lemma 1.43. *Nech $(S, \cdot)$ je pologrupa, $a \in S$. $\forall m, n \in \mathbb{N}$: $a^m \cdot a^n = a^{m+n}$.*

Dôkaz. $\underbrace{a \cdot \ldots \cdot a}_{m\text{-krát}} \cdot \underbrace{a \cdot \ldots \cdot a}_{n\text{-krát}} = \underbrace{a \cdot \ldots \cdot a}_{(m+n)\text{-krát}}$. □

Lemma 1.44. *Nech $(S, \cdot)$ je pologrupa, $a \in S$. $\forall m, n \in \mathbb{N}$: $(a^m)^n = a^{mn}$.*

Dôkaz. $\underbrace{a^m \cdot \ldots \cdot a^m}_{n\text{-krát}} = a^{\overbrace{m+\ldots+m}^{n\text{-krát}}}$. □

Lemma 1.45. *Nech $1 \in S$ je jednotkový prvok v pologrupe. Potom $1^{-1} = 1$; $(a^{-1})^{-1} = a$; $(a_1 \ldots a_n)^{-1} = a_n^{-1} \ldots a_1^{-1}$; kde $a, a_1, \ldots, a_n$ sú ľubovoľné invertibilné prvky z S* [2, I.4.6].

Lemma 1.46. *Ak má prvok a inverziu, tak $\forall n \in \mathbb{N}$: $a^{-n} = \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{n\text{-krát}} = (\underbrace{a \cdot \ldots \cdot a}_{n\text{-krát}})^{-1}$.*

Definícia 1.47. *Rád* prvku a v grupe $(G, \cdot)$ je najmenšie $n \in \mathbb{N}$ také, že $a^n = e$.
Ak také n neexistuje, kladieme rád a rovný 0 (podľa [2, I.4.11] je to ∞).

Príklad 1.48. Rád prvku 0 v grupe $(\mathbb{Z}, +)$ je 1, rád ďalších prvkov je 0.

Lemma 1.49. *Nech rád prvku a v grupe $(G, \cdot)$ je 0. Potom ak $a^k = a^l$, tak $k = l$ $(k, l \in \mathbb{Z})$.*

Dôkaz. BUNV[1] $k \leq l$. Ak $a^k = a^l$, tak $1 = a^{l-k}$. Ak rád a je 0, tak $l - k = 0$, teda $l = k$. □

Lemma 1.50. *Nech rád prvku a v grupe $(G, \cdot)$ je $n \in \mathbb{N}$. Potom $1, a, a^2, \ldots, a^{n-1}$ sú po dvoch rôzne. Navyše, pre $k = qn + r$, kde $r \in \{0, \ldots, n-1\}$ je $a^k = a^r$ (tzn. že $a^n = a^0$, $a^{n+1} = a$, ... a podobne aj pre záporné exponenty).*

Dôkaz. Sú po dvoch rôzne: BUNV $0 \leq k \leq l \leq n - 1$. Ak $a^k = a^l$, tak $1 = a^{l-k}$. Ak $l - k \in \{0, \ldots, n-1\}$, tak $l - k = 0$ (nesmie byť n), teda $l = k$.

Navyše: $a^k = a^{qn+r} = (a^n)^q \cdot a^r = 1^q \cdot a^r = a^r$. □

[1] Bez ujmy na všeobecnosti

1.7 Dihedrálne grupy

Definícia 1.51. Nech $M \subseteq \mathbb{R}^n$ je množina bodov. Zobrazenie $f\colon M \to M$ je *symetria*, ak je bijekciou a zachováva vzdialenosti, t. j. ak vzdialenosť bodov $p, q \in M$ sa rovná vzdialenosti ich obrazov $f(p), f(q) \in M$.

Veta 1.52. *Množina všetkých symetrií s operáciou skladania tvorí grupu.*

Dôkaz. Jedná sa o špeciálny prípad grupy permutácií $(S(A), \circ)$. □

Definícia 1.53. *Dihedrálna grupa* $(\mathbb{D}_n, \circ)$ stupňa n je grupa všetkých symetrií pravidelného n-uholníka. Nemusíme uvažovať všetky body geometrického útvaru – symetria je určená tým, ako zamieňa jeho vrcholy.

Príklad 1.54. Ak r je rotácia o $\frac{2\pi}{n}$, d preklopenie (zrkadlenie) podľa osi y, potom napr. $\mathbb{D}_4 = \{id, r, r^2, r^3, d, rd, r^2d, r^3d\}$.

Lemma 1.55. $\mathbb{D}_n =$ *práve* $\{id, r, r^2, \ldots, r^{n-1}, d, rd, r^2d, \ldots, r^{n-1}d\}$.

Dôkaz. Bijekcia, ktorá zachováva vzdialenosti musí posielať vrchol na vrchol. Platí: $r^n = 1$; $d^2 = 1$; $dr = r^{n-1}d$. V grupe $(\mathbb{D}_n, \circ)$ už nie sú žiadne ďalšie zobrazenia. □

Definícia 1.56. *Prezentácia* $G_p = \langle a, b; a^r = 1, b^s = 1, ab = ba^t \rangle$, kde $r, s, t \in \mathbb{N}$ je najvšeobecnejšia grupa, ktorá je zadaná svojou *generujúcou množinou* ($\{a, b \in G\}$ generuje grupu G) a *reláciami* (za bodkočiarkou), ktoré na nej platia.

Príklad 1.57. Grupa $(\mathbb{D}_n, \circ)$ má prezentáciu $G_p = \langle r, d; r^n = 1, d^2 = 1, dr = r^{n-1}d \rangle$.

1.8 Cvičenia

1. Dokážte, že množina $GL_2(\mathbb{R})$ s operáciou $*$ tvorí grupu, ak $*$ je definovaná ako
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} a+b & a-b \\ c+d & c-d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}.$$

2. Dokážte, že množina $\mathbb{R}^*$ s operáciou $\triangle$ tvorí grupu, ak $\triangle$ je definovaná ako
$$a \triangle b = \begin{cases} a \cdot b & \text{ak } a > 0; \\ \frac{a}{b} & \text{ak } a < 0. \end{cases}$$

3. Dokážte, že množina $\mathbb{Z}_2 \times \mathbb{Z}$ s operáciou @ definovanou
$$([a]_2, k) @ ([b]_2, l) = ([a+b]_2, k + (-1)^a \cdot l),$$
kde $a, b, k, l \in \mathbb{Z}$ tvorí grupu.

4. Máme nasledovné permutácie z množiny $\mathbb{S}_8$: $\sigma = (1, 3, 6, 2, 4, 8, 7, 5)$ a $\pi = (1, 3) \circ (2, 4, 6, 8, 7)$. Určte: $\sigma \circ \pi$, σ^{2014}, π^{2014}, π^{-1}, paritu permutácií.

5. Nájdite všetky permutácie $x \in \mathbb{S}_8$ také, že:
   a) $x^2 = (1, 2) \circ (3, 4) \circ (5, 6)$;
   b) $x^2 = (1, 2, 3) \circ (4, 5, 6)$.

6. Ukážte, ze každú permutáciu z $\mathbb{S}_n$ môžeme získať kompozíciou $(1, 2, 3, \ldots, n)$ a $(1, 2)$.

1.9 Návody k riešeniu cvičení

1.
   - Ukážeme, že $*$ je operácia, t. j. že výsledná matica patrí do $GL_2(\mathbb{R})$.
   - Ukážeme, že $*$ je asociatívna.
   - Nájdeme neutrálny prvok: z jednotkovej matice $a+b=1$, $a-b=0$, $c+d=0$, $c-d=1$; dostávame $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$.
   - Nájdeme inverzný prvok: $\dfrac{\begin{pmatrix} c-d-a+b & c-d+a-b \\ -c-d+a+b & -c-d-a-b \end{pmatrix}}{4(bc-ad)}$.

2.
   - Ukážeme, že $\triangle$ je operácia.
   - Ukážeme, že $\triangle$ je asociatívna.
   - Nájdeme neutrálny prvok: 1.
   - Nájdeme inverzný prvok: $\frac{1}{a}$, ak $a > 0$ a a ak $a < 0$.

3.
   - Ukážeme, že @ je operácia: $[a+b]_2$ závisí len na $[a]_2$, $[b]_2$. Ak $[a]_2 = [c]_2$, $[b]_2 = [d]_2$, tak $2 \mid a-c$, $2 \mid b-d$ potom $2 \mid (a+b)-(c+d)$, teda $[a+b]_2 = [c+d]_2$. Ďalej $(-1)^a$ závisí len na $[a]_2$.
   - Ukážeme, že @ je asociatívna.
   - Nájdeme neutrálny prvok: $([0]_2, 0)$.
   - Nájdeme inverzný prvok: $([a]_2, k)^{-1} = ([a]_2, (-1)^{a+1} \cdot k)$.

4.
   - $\sigma \circ \pi = (1,6,7,4,2,8,5)$
   - $\sigma^{2014} = \sigma^{2014 \bmod 8} = \sigma^6 = (\sigma^2)^{-1} = (1,7,4,6) \circ (2,3,5,8)$
   - $\pi^{2014} = (2,4,6,8,7)^4 = (2,4,6,8,7)^{-1} = (2,7,8,6,4)$
   - $\pi^{-1} = (3,1) \circ (7,8,6,4,2)$
   - Parita: obe sú nepárne

5. a) Také x neexistuje.

   b) $x_1 = (3,2,1) \circ (6,5,4)$,
   $x_2 = (1,4,2,5,3,6)$,
   $x_3 = (1,5,2,6,3,4)$,
   $x_4 = (1,6,2,4,3,5)$.
   Ďalšie 4 permutácie x_5 až x_8 vzniknú zložením $(7,8)$ s každým z x_1 až x_4.

6.
   - Každú permutáciu je možné získať z $(1,i)$, kde $i \in \{2,\ldots,n\}$:
   $(a_1,a_2,\ldots,a_k) = (1,a_1) \circ (1,a_k) \circ (1,a_{k-1}) \circ \cdots \circ (1,a_1)$.
   - Ďalej každú perm. je možné získať z $(i,i+1)$, kde $i \in \{1,2,\ldots,n-1\}$:
   $(1,i) = (1,2) \circ (2,3) \circ \cdots \circ (i-1,i) \circ (i-1,i-2) \circ \cdots \circ (1,2)$.
   - Nakoniec $(i,i+1) = (1,2,\ldots,n)^{+i-1} \circ (1,2) \circ (1,2,\ldots,n)^{-i+1}$.
     - Pozn.: korekcia $t \circ s \circ t^{-1}$ „premenuje“ prvky s.

Kapitola 2: Teória čísel

2.1 Aritmetika a operácie na celých číslach

Teória čísel sa zaoberá vlastnosťami celých čísel.

Na množine $\mathbb{Z}$ uvažujeme dve základné binárne operácie: *sčítanie* $(+)$ a *násobenie* $(\cdot)$. Platia pre ne tieto vlastnosti $(\forall a, b, c \in \mathbb{Z})$:

- *Komutativita*: $a + b = b + a \quad \text{a} \quad a \cdot b = b \cdot a$,
- *Asociativita*: $(a + b) + c = a + (b + c) \quad \text{a} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$,
- *Distributivita násobenia cez sčítanie*: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Neutrálne prvky pre tieto operácie sú postupne 0 a 1: $a + 0 = a \quad \text{a} \quad a \cdot 1 = a$.

Inverzné prvky: $-a$ pre sčítanie (tzv. *opačný*), pretože $a + (-a) = 0$. Jediný prvok množiny $\mathbb{Z}$ s multiplikatívnou inverziou je 1, pretože $1^{-1} = 1$.

Odčítanie je binárnou operáciou na množine $\mathbb{Z}$, teda je definované pre ľubovoľné dve celé čísla, zatiaľ čo *delenie* nie je binárnou operáciou a teda je definované len pre nejaké celé čísla. Definície sú nasledovné:

Definícia 2.1. $a - b = a + (-b)$ pre všetky $a, b \in \mathbb{Z}$.

Definícia 2.2. $a/b = c$ práve vtedy, keď $a = b \cdot c$.

Veta 2.3 (Princíp dobrého usporiadania; Zermelova veta)**.** *V ľubovoľnej neprázdnej množine kladných celých čísel existuje najmenší prvok.*

Veta 2.4 (Priehradkový (Dirichletov) princíp)**.** *Ak n prvkov uložíme do k krabičiek, pričom $n > k$, tak aspoň jedna krabička obsahuje viac ako jeden prvok.*

Veta 2.5 (Princíp matematickej indukcie)**.** *Ak vieme, že:*

- *nejaký výrok je pravdivý pre $n = 1$,*
- *a predpokladáme, že to, že je výrok pravdivý pre n implikuje, že je pravdivý pre $(n + 1)$,*

tak je výrok pravdivý pre všetky prirodzené čísla.

2.2 Deliteľnosť

Definícia 2.6. Nech a, b sú celé čísla, $a \neq 0$. Potom a delí b práve vtedy, keď existuje nejaké celé číslo k tak, že $b = ka$.

- Ak a delí b, hovoríme, že a *je deliteľom* b, resp. že b *je násobkom* a a píšeme $a \mid b$.
- Ak a nedelí b, píšeme $a \nmid b$.

Lemma 2.7. *Každé celé číslo delí nulu, t. j.* $\forall a \in \mathbb{Z}$*:* $a \mid 0$.

Lemma 2.8. *Ak $a \mid b$, pričom $b \neq 0$, tak $|a| \leq |b|$.*

Pre ľubovoľné celé čísla a, b, c má relácia $\mid$ nasledovné vlastnosti:

Lemma 2.9.

1. *Ak $a \mid b$ a $b \mid c$, tak $a \mid c$.*
2. *Ak $a \mid b$ a $c \mid d$, tak $ac \mid bd$.*
3. *Ak $a \mid b$ a $a \mid c$, tak $a \mid b + c$.*

Dôkaz.

1. Ak $b = ma$ a $c = nb$, tak $c = (mn)a$.
2. Ak $b = ma$ a $d = nc$, tak $bd = (mn)(ac)$.
3. Ak $b = ma$ a $c = na$, tak $b + c = (m + n)a$. □

Lemma 2.10 (Deliteľnosť lineárnych kombinácií)**.** *Nech $a, b, c, m, n \in \mathbb{Z}$. Ak $c \mid a$ a $c \mid b$, tak $c \mid (am + bn)$.*

Dôkaz. Keďže $c \mid a$ a $c \mid b$, tak existujú nejaké k_1, k_2 také, že $a = k_1 c$ a $b = k_2 c$. Preto

$$am + bn = k_1 cm + k_2 cn = c(k_1 m + k_2 n),$$

a teda $c \mid (ma + nb)$. □

Veta 2.11 (O delení so zvyškom)**.** *Ak $a, b \in \mathbb{Z}$, pričom $b \neq 0$, tak existujú jedinečné $q, r \in \mathbb{Z}$ také, že $a = bq + r$, kde $0 \leq r < |b|$.*

Číslo a nazývame delenec, b deliteľ, q čiastočný podiel a r zvyšok.

Dôkaz existencie. Stačí uvážiť $b > 0$, pretože ak by $b < 0$, tak napíšeme $b' = -b$, $q' = -q$ a rovnosť $a = bq + r$ prepíšeme ako $a = b'q' + r$, kde $0 \leq r < |b'|$.

Ďalej stačí uvážiť $a \geq 0$, pretože ak by $a < 0$ ($b > 0$), tak napíšeme $a' = -a$, $q' = -q - 1$, $r' = b - r$ a rovnosť $a = bq + r$ prepíšeme ako $a' = bq' + r'$, kde $0 \leq r' < |b|$.

Nech $q_1 \geq 0$, $r_1 \geq 0$ spĺňajú $a = bq_1 + r_1$ (existujú vždy, lebo môžeme $q_1 = 0$, $r_1 = a$). Ak $r_1 < b$, sme hotoví. Inak $q_2 = q_1 + 1$, $r_2 = r_1 - b$ spĺňajú $a = bq_2 + r_2$ a $0 \leq r_2 < r_1$. Opakovaním dostaneme $q = q_k$ a $r = r_k$ také, že $a = bq + r$, kde $0 \leq r < b$. □

Dôkaz jedinečnosti podielu a zvyšku. Uvážme q, q', r, r', kde $0 \leq r$, $r' < |b|$, pričom $a = bq + r$ a zároveň $a = bq' + r'$.

Vieme, že $0 \leq r < |b|$ a $-|b| < -r' \leq 0$. Z toho $-|b| < r - r' < |b|$, teda $|r - r'| < |b|$.

Odčítaním dvoch rovností pre a dostaneme $b(q' - q) = (r - r')$. Z toho $|b|$ delí $|r - r'|$. Ak $|r - r'| \neq 0$, tak $|b| < |r - r'|$, čo je spor. Preto $|r - r'| = 0$, teda $r = r'$, teda $b(q' - q) = 0$. Keďže $b \neq 0$, tak $q = q'$. □

Definícia 2.12. Najväčší spoločný deliteľ celých čísel a, b je čo najväčšie celé číslo d, ktoré delí a a zároveň delí b. Píšeme $d = \mathrm{NSD}(a, b) = (a, b)$. Dodatočne definujeme $(0, 0) = 0$.

Poznámka. Niekedy sa NSD uvažuje vzhľadom k relácii deliteľnosti $|$, nie k relácii usporiadania $\leq$ celých čísel. Vtedy nie je d jednoznačne definované. Napr. pre $b \neq 0$ je $\mathrm{NSD}(0, b) = \pm b$.

Iná definícia dáva tiež nejednoznačné d: Ak $d|a, d|b$ a existuje také c, že $c|a, c|b$, tak $c|d$. Treba pamätať na to, že každé celé číslo má kladných aj záporných deliteľov.

Definícia 2.13. Celé čísla a, b sú nesúdeliteľné, ak $(a, b) = 1$.

Lemma 2.14. *Ak vydelíme dve celé čísla ich najväčším spoločným deliteľom, dostaneme dvojicu nesúdeliteľných čísel. Inak povedané, ak* $(a, b) = d$ *tak* $(a/d, b/d) = 1$.

Dôkaz. Nech k je kladné a $k \mid a/d$, $k \mid b/d$. Potom existujú kladné m, n také, že: $a/d = km$, $b/d = kn$. Z toho $a = kmd$, $b = knd$. Preto je kd spoločným deliteľom a aj b. Ďalej $kd \geq d$, ale $d = (a, b)$, teda $k = 1$. □

Lemma 2.15. *NSD dvoch celých čísel sa nezmení, ak pripočítame násobok jedného čísla k druhému. Nech* a, b, c *sú celé. Potom* $(a, b) = (a + cb, b)$.

Dôkaz. Nech k je spoločným deliteľom a aj b. Podľa Lemmy 2.10, $k \mid (a + cb)$, teda k je deliteľom $a + cb$.

Nech l je spoločným deliteľom $a + cb$ aj b. Podľa Lemmy 2.10, $l \mid ((a + cb) - cb) = a$, teda l je spoločným deliteľom a aj b. □

Dôsledok 2.16. $(a, b) = (a, b - a)$.

Dôsledok 2.17. *Ak* a, b, q, r *sú celé čísla, kde* $a = bq + r$, *tak* $(a, b) = (bq + r, b) = (r, b)$.

Veta 2.18 (Euklidov algoritmus)**.** *Nech* $a, b \in \mathbb{N}$.

$$\begin{aligned}
a &= q_1 \cdot b + r_1, & r_1 &< b \\
b &= q_2 \cdot r_1 + r_2, & r_2 &< r_1 \\
r_1 &= q_3 \cdot r_2 + r_3, & r_3 &< r_2 \\
&\dots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n, & 0 \neq r_n &< r_{n-1} \\
r_{n-1} &= q_{n+1} \cdot r_n
\end{aligned}$$

Potom r_n *je posledný nenulový zvyšok a* $r_n = (a, b)$.

Dôkaz.

$$\begin{aligned}
&\text{Z posledného riadka:} && r_n \mid r_{n-1} \\
&\text{Z predposledného riadka:} && r_n \mid r_{n-2} \\
&\dots \\
&\text{Z 2. riadka:} && r_n \mid b \\
&\text{Z 1. riadka:} && r_n \mid a
\end{aligned}$$

Teda r_n je spoločný deliteľ čísel a, b.
Nech $d \in \mathbb{N}$ delí a, b (iný spoločný deliteľ a, b).

Z 1. riadka:	$d \mid r_1$
Z 2. riadka:	$d \mid r_2$
...	
Z predposledného riadka:	$d \mid r_n$

Keďže $r_n \geq 0$, r_n je NSD(a, b). □

Dôkaz (iný). Podľa Dôsledku 2.17: $(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_n, 0) = r_n$. □

Veta 2.19 (Lamého)**.** *Euklidov algoritmus vyžaduje maximálne* 5*-násobok krokov delenia oproti počtu cifier menšieho z čísel* a, b*.*

Veta 2.20 (Bezoutova)**.** $\forall a, b \in \mathbb{Z}\ \exists m, n \in \mathbb{Z}$ *tak, že* $am + bn = (a, b)$*.*

Poznámka. NSD čísel a, b môžeme vždy vyjadriť ako lineárnu kombináciu čísel a, b. Koeficienty m, n tejto lineárnej kombinácie môžeme nájsť pomocou Euklidovho algoritmu.

Dôkaz. Nech x je najmenšie kladné celé číslo, ktoré vieme zapísať ako lineárnu kombináciu čísel a, b. Ďalej nech $d = (a, b)$. Potom x musí byť násobkom d, lebo a, b sú oba násobky d. Tvrdíme, že $x = d$.

Ak by naopak $x > d$, potom x nie je spoločným deliteľom a, b, takže $x \nmid a$ alebo $x \nmid b$. BUNV predpokladajme $x \nmid a$. Potom $a \div x = q$ R r, kde zvyšok r je kladný. Ale $r = a - qx$, takže r je lineárnou kombináciou a, b. Toto je spor, pretože r musí byť menšie ako x. □

Dôkaz (iný). Podľa Vety 2.18: $(a, b) = r_n = r_{n-2} - r_{n-1} \cdot q_n = r_{n-2} - (r_{n-3} - r_{n-2} \cdot q_{n-1}) \cdot q_n = r_{n-3} \cdot (-q_n) + r_{n-2} \cdot (1 + q_{n-1} \cdot q_n) = \cdots = am + bn$. □

Dôsledok 2.21. *Celé čísla* a*,* b *sú nesúdeliteľné, práve keď* $\exists m, n \in \mathbb{Z}$ *tak, že* $am + bn = 1$*.*

Dôsledok 2.22. *Nech* a*,* b*,* c *sú nenulové celé čísla. Potom* c *je lineárnou kombináciou* a, b *práve vtedy, keď* c *je násobkom* (a, b)*.*

Dôsledok 2.23. *Nech* a*,* b*,* c *sú celé čísla,* $(a, b) = 1$*,* $a \mid bc$*. Potom* $a \mid c$*.*

Dôkaz. Existujú celé čísla m, n také, že $am + bn = 1$. Vynásobme obe strany rovnice celým číslom c. Potom $amc + bnc = c$. Zrejme $a \mid amc$. Z predpokladu $a \mid bnc$. □

Definícia 2.24. Najmenší spoločný násobok celých čísel a, b je čo najmenšie kladné celé číslo n, ktoré je násobkom a a zároveň je násobkom b. Píšeme $n = \text{nsn}(a, b) = [a, b]$.

Poznámka. Pre $n = [a, b]$ platí: Ak $a|n, b|n$ a existuje také m, že $a|m, b|m$, tak $n|m$.

Veta 2.25. $(a, b) \cdot [a, b] = ab$*.*

2.3 Prvočísla

Definícia 2.26. Číslo $n \in \mathbb{N}$ je prvočíslo, ak je väčšie ako 1 a je deliteľné len 1 a samým sebou. Teda $n \geq 2$ a zároveň neexistujú $k, l \geq 2$ také, že $n = kl$.

Dôsledok 2.27. *Ak p, q sú prvočísla, potom $p = q$ alebo $(p, q) = 1$.*

Lemma 2.28. *Ak $p \mid q_1 \cdot \ldots \cdot q_n$, kde $p, q_1, \ldots, q_n$ sú prvočísla, potom $p \in \{q_1, \ldots, q_n\}$.*

Dôkaz. Indukciou z Dôsledku 2.23. □

Definícia 2.29. Každé prirodzené číslo $a > 1$, ktoré nie je prvočíslom sa nazýva zložené. Teda existujú nejaké $b > 1$, $c > 1$ také, že $a = bc$.

Veta 2.30 (Základná veta aritmetiky)**.** *Každé $n \in \mathbb{N}$ sa dá zapísať ako súčin prvočísel. Takýto rozklad je jednoznačný až na poradie činiteľov.*

Poznámka. 1 = súčin nula prvočísel (prázdny súčin).

Dôkaz existencie. Ak je n prvočíslo, dôkaz je triviálny. Predpokladajme teda, že n je zložené a je to čo najmenšie číslo, ktoré sa už nedá zapísať ako súčin prvočísel. Potom $n \geq 2$ a existujú $k, l \in \mathbb{N}$ také, že $2 \leq k, l < n$ a $n = kl$.

Čísla k, l sa dajú vyjadriť ako súčin prvočísel, povedzme $k = p_1 p_2 \ldots p_r$, $l = q_1 q_2 \ldots q_s$, teda $n = p_1 p_2 \ldots p_r q_1 q_2 \ldots q_s$ ※ . □

Dôkaz jednoznačnosti. Nech $p_1 \cdots p_m = q_1 \cdots q_n$, kde $p_1 \leq \cdots \leq p_m$ a $q_1 \leq \cdots \leq q_n$ sú dva rôzne rozklady nejakého čísla na súčin prvočísel. Chceme ukázať, že $m = n$ a tiež že $p_i = q_i$ pre každé i. BUNV predpokladajme, že $m \leq n$ a pokračujme indukciou podľa m.

Báza: Ak $m = 1$, tak $p_1 = q_1 \cdots q_n$. Keďže p_1 je prvočíslo, tak $n = 1$, teda $p_1 = q_1$.

IK: Ak $m > 1$, tak z predpokladu je p_m najväčší prvočíselný deliteľ čísla $p_1 \cdots p_m$, a q_n je najväčší prvočíselný deliteľ čísla $q_1 \cdots q_n$. Keďže $p_1 \cdots p_m = q_1 \cdots q_n$, tak $p_m = q_n$. Z toho dostávame $p_1 \cdots p_{m-1} = q_1 \cdots q_{n-1}$. Tento rozklad je ale z IP určený jednoznačne. □

Lemma 2.31 (Euklidova)**.** *Ak p je prvočíslo a $p \mid ab$, tak buď $p \mid a$ alebo $p \mid b$.*

Dôkaz. Predpokladajme $p \mid ab$, $p \nmid a$. Dokážme $p \mid b$. Keďže $p \nmid a$ a p je prvočíslo, tak $(p, a) = 1$. Potom existujú m, n také, že $ma + np = 1$. Po vynásobení b dostávame $mab + npb = b$. Keďže $p \mid mab$, $p \mid npb$, tak $p \mid b$. □

Lemma 2.32. *Ak p je prvočíslo a $p \mid a_1 \cdots a_n$, tak $p \mid a_i$ pre nejaké i.*

Dôkaz. Indukciou: Báza pre $n = 2$ je Euklidova lemma. Pre $n > 2$ zapíšme $a_1 \cdots a_n = (a_1 \cdots a_{n-1})a_n$. Z Euklidovej lemmy buď $p \mid a_1 \cdots a_{n-1}$ alebo $p \mid a_n$. V prvom prípade z IP $p \mid a_i$ pre nejaké $i \leq n - 1$. V druhom prípade $i = n$. □

Veta 2.33. *Číslo $n \in \mathbb{N}$, kde $n > 1$ je prvočíslom práve vtedy, keď nie je deliteľné žiadnym prvočíslom p, pričom $1 < p \leq \sqrt{n}$.*

Dôkaz. „$\Longrightarrow$“: Zrejmé. „$\Longleftarrow$“: Obmenou implikácie získame tvrdenie: Ak n je zložené, tak je deliteľné nejakým prvočíslom p, kde $1 < p \leq \sqrt{n}$. Nech $n = ab$ pre $a, b \in \mathbb{N}$, kde $a, b > 1$. Podľa Základnej vety aritmetiky sa dajú a, b rozložiť na súčin prvočísel. Ďalej musí platiť, že $a \leq \sqrt{n}$ alebo $b \leq \sqrt{n}$, pretože inak $ab > \sqrt{n} \cdot \sqrt{n} = n$. Preto nájdeme aspoň jedného deliteľa čísla n najviac do $\sqrt{n}$. V opačnom prípade je n prvočíslom. □

Dôsledok 2.34. *Každé $n \in \mathbb{N}$, kde $n > 1$ má aspoň jedného prvočíselného deliteľa.*

Veta 2.35. *Existuje nekonečne mnoho prvočísel.*

Dôkaz. Sporom. Predpokladajme, že existuje konečne mnoho prvočísel $p_1, p_2, \ldots, p_n$. Nech $Q = p_1 p_2 ... p_n + 1$. Toto číslo musí mať prvočíselného deliteľa, označme ho q. Ak dokážeme, že $q \notin \{p_1, p_2, \ldots, p_n\}$, dôjdeme k sporu.

Predpokladajme, že $q = p_i$ pre $1 \leq i \leq n$. Potom $q \mid p_1 p_2 ... p_n$ a teda $q \mid Q - p_1 p_2 ... p_n$. Z toho q delí 1, ale žiadne prvočíslo nedelí 1 ※ . Teda $q \notin \{p_1, p_2, \ldots, p_n\}$ a Q je prvočíslo. □

Kapitola 3: Kongruencie

3.1 Základné definície

Definícia 3.1. Nech $n \in \mathbb{N}$. Potom $[a]_n = \{a + kn \mid k \in \mathbb{Z}\}$ sú *zvyškové triedy* mod n.

Definícia 3.2. Nech $n \in \mathbb{N}$. Potom $\mathbb{Z}_n = \{[a]_n \mid a \in \mathbb{Z}\}$ je množina všetkých zvyškových tried podľa daného modulu n.

Veta 3.3. $|\mathbb{Z}_n| = n$.

Definícia 3.4. Nech $a, b \in \mathbb{R}$. Operáciu *modulo* definujeme ako zvyšok po delení, t. j.

$$a \bmod b := \begin{cases} a - b \left\lfloor \frac{a}{b} \right\rfloor & : b \neq 0; \\ a & : b = 0. \end{cases}$$

Definícia 3.5. Nech $n \in \mathbb{N}$. Dve celé čísla a, b sú spolu kongruentné modulo n; píšeme $a \equiv b \pmod{n}$; ak obe dávajú rovnaký zvyšok po delení číslom n.

Veta 3.6. *Nasledujúce podmienky sú ekvivalentné:*

1. $a \equiv b \pmod{n}$;
2. $n \mid (a - b)$;
3. $[a]_n = [b]_n$ *(nezáleží na výbere reprezentanta triedy).*

Dôkaz. Dokážeme postupne tri implikácie.

„1. ⇒ 2.“: Máme $a \equiv b \pmod{n}$, teda z definície $a \bmod n = b \bmod n$.

Nech $n = 0$. Potom $a \bmod 0 = b \bmod 0$, teda $a = b$. Z toho $a - b = 0$. Potom $n \mid (a - b)$.

Nech $n \neq 0$. Potom z definície $a \bmod n = a - n \left\lfloor \frac{a}{n} \right\rfloor$ a $b \bmod n = b - n \left\lfloor \frac{b}{n} \right\rfloor$. Preto $a - n \left\lfloor \frac{a}{n} \right\rfloor = b - n \left\lfloor \frac{b}{n} \right\rfloor$, takže $a - b = n \left(\left\lfloor \frac{a}{n} \right\rfloor - \left\lfloor \frac{b}{n} \right\rfloor \right)$. Číslo $\left\lfloor \frac{a}{n} \right\rfloor - \left\lfloor \frac{b}{n} \right\rfloor$ je celé, takže $a - b = kn$, teda z Definície 2.6 dostávame $n \mid (a - b)$.

„2. ⇒ 3.“: Máme $n \mid (a - b)$, teda z definície delenia $a - b = kn$, kde $k \in \mathbb{Z}$. Teda $a = b + kn$, čo je ekvivalentné s $[a]_n = [b]_n$.

„3. $\Rightarrow$ 1.“: Máme $k \in \mathbb{Z}$ také, že $a = b + kn$. Potom:

$$\begin{aligned} a \bmod n &= (b+kn) - n\left\lfloor \frac{b+kn}{n} \right\rfloor \\ &= (b+kn) - n\left\lfloor \frac{b}{n} + k \right\rfloor \\ &= (b+kn) - n\left\lfloor \frac{b}{n} \right\rfloor - kn \\ &= b - n\left\lfloor \frac{b}{n} \right\rfloor \\ &= b \bmod n \end{aligned}$$

□

Dôsledok 3.7. $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$.

3.2 Vlastnosti kongruencií

Veta 3.8. *Nech $a, b, c, d \in \mathbb{Z}$. Nech $m \in \mathbb{N}$. Potom:*

1. *Ak $a \equiv b \pmod m$, tak $b \equiv a \pmod m$. (Komutativita.)*
2. *Ak $a \equiv b \pmod m$, $b \equiv c \pmod m$, tak $a \equiv c \pmod m$. (Tranzitivita.)*
3. *Ak $a \equiv b \pmod m$, tak $a + c \equiv b + c \pmod m$. (Pripočítanie konštanty.)*
4. *Ak $a \equiv b \pmod m$, tak $ac \equiv bc \pmod m$. (Vynásobenie konštantou.)*
5. *Ak $a \equiv b \pmod m$, tak $ac \equiv bc \pmod{mc}$, kde $c > 0$. (Vynásobenie modulu.)*
6. *Ak $a \equiv b \pmod m$, $c \equiv d \pmod m$, tak $a+c \equiv b+d \pmod m$. (Súčet kongruencií.)*
7. *Ak $a \equiv b \pmod m$, $c \equiv d \pmod m$, tak $ac \equiv bd \pmod m$. (Súčin kongruencií.)*

Dôkaz. Dokážeme postupne všetky tvrdenia:

1. Máme $m \mid (a-b)$. Potom existuje k také, že $a - b = mk$. Z toho $b - a = m(-k)$ a teda $m \mid (b-a)$, teda $b \equiv a \pmod m$.
2. Máme $m \mid (a-b)$ a tiež $m \mid (b-c)$. Potom existujú k, l také, že $a = b + mk$ a $b = c + ml$. Preto $a = c + m(k+l)$ a z toho $a \equiv c \pmod m$.
3. Máme $m \mid (a-b)$. Ak pridáme a odrátame c, dostaneme: $m \mid ((a+c) - (b+c))$. Preto $a + c \equiv b + c \pmod m$.
4. Máme $m \mid (a-b)$. Potom existuje k také, že $a - b = mk$. Preto $ac - bc = m(kc)$. Teda $m \mid (ac - bc)$, teda $ac \equiv bc \pmod m$.
5. Máme $m \mid (a-b)$. Potom existuje k také, že $a - b = mk$. Preto $ac - bc = mc(k)$. Teda $mc \mid (ac - bc)$, teda $ac \equiv bc \pmod{mc}$.

6. Máme $m \mid (a-b)$ a tiež $m \mid (c-d)$. Potom existujú k, l také, že $a-b=mk$ a $c-d=ml$. Všimnime si, že $(a-b)+(c-d)=(a+c)-(b+d)=m(k+l)$. Preto $m \mid ((a+c)-(b+d))$, teda $a+c \equiv b+d \pmod{m}$.

7. Máme $a-b=mk$ a tiež $c-d=ml$. Preto $ca-cb=m(ck)$ a tiež $bc-bd=m(bl)$. Všimnime si, že $(ca-cb)+(bc-bd)=ac-bd=m(kc-lb)$. Preto $m \mid (ac-bd)$, teda $ac \equiv bd \pmod{m}$.

□

Veta 3.9. *Delenie kongruencií nemusí zachovávať kongruenciu, teda:*

1. *Nech $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$, $d=(m,c)$ a $ac \equiv bc \pmod{m}$. Potom $a \equiv b \pmod{m/d}$.*

2. *Nech $d=(m,c)=1$. Potom $a=b \pmod{m}$, ak $ac \equiv bc \pmod{m}$.*

Dôkaz. Časť 2. dostaneme priamo z 1.: Ak $ac \equiv bc \pmod{m}$, tak $m \mid (ac-bc)=c(a-b)$. Potom $c(a-b)=mk$. Vydelením oboch strán číslom d dostaneme $(c/d)(a-b)=k(m/d)$. Preto $(m/d, c/d)=1$. Z toho $m/d \mid (a-b)$. □

3.3 Operácie na zvyškových triedach

Veta 3.10. *Na $\mathbb{Z}_n$ definujeme operáciu $+$ vzťahom $[a]_n+[b]_n=[a+b]_n$.*

Dôkaz. Je nutné dokázať korektnosť definície tejto operácie.

Ak rovnakú množinu $[a]_n$ zadáme pomocou iného reprezentanta ako $[a']_n$ a podobne $[b]_n$ ako $[b']_n$, tak $[a+b]_n$ sa musí rovnať $[a'+b']_n$.

Vieme, že $n \mid (a-a')$ a tiež $n \mid (b-b')$. Chceme dosiahnuť, aby $n \mid ((a+b)-(a'+b'))$. To je ale to isté, ako $n \mid ((a-a')+(b-b'))$. Keď sčítame dve čísla deliteľné n, aj tento súčet bude deliteľný n. □

Veta 3.11. *Na $\mathbb{Z}_n$ definujeme operáciu $\cdot$ vzťahom $[a]_n \cdot [b]_n=[a \cdot b]_n$.*

Dôkaz. Je nutné dokázať korektnosť definície tejto operácie.

Ak $[a]_n=[a']_n$ a podobne $[b]_n=[b']_n$, tak $[a \cdot b]_n$ sa musí rovnať $[a' \cdot b']_n$.

Vieme, že $n \mid (a-a')$ a tiež $n \mid (b-b')$. Chceme dosiahnuť, aby $n \mid (a \cdot b-a' \cdot b')$. To je ale to isté, ako $n \mid (a \cdot b-a' \cdot b'+a' \cdot b-a' \cdot b)$. To je to isté, ako $n \mid (b \cdot (a-a')+a' \cdot (b-b'))$. Keď sčítame b-násobok čísla deliteľného n s a'-násobkom čísla deliteľného n, aj tento súčet bude deliteľný n. □

Veta 3.12. *$(\mathbb{Z}_n, +)$ je komutatívna grupa pre každé $n \in \mathbb{N}$.*

Dôkaz. Sčítanie zvyškových tried je komutatívne a asociatívne. Jednotkový prvok je $[0]_n$ a inverzný k $[a]_n$ je $[-a]_n$. □

Veta 3.13. *$(\mathbb{Z}_n, \cdot)$ je komutatívny monoid pre každé $n \in \mathbb{N}$.*

Dôkaz. Násobenie zvyškových tried je komut. a asociatívne. Jednotkový prvok je $[1]_n$. □

Lemma 3.14. *Nech $a \in \mathbb{Z}$, $n \in \mathbb{N}$. Potom $[a]_n \in (\mathbb{Z}_n, \cdot)$ má inverziu $\iff$ $(a,n)=1$.*

Dôkaz. „$\Longrightarrow$“: Nech $[b]_n$ je inverzia k $[a]_n$. Potom $[ba]_n = [ab]_n = [1]_n$. Preto $ab \equiv 1 \pmod{n}$, ekvivalentne $ab = kn + 1$, kde $k \in \mathbb{Z}$. Teda $ab + n(-k) = 1$ a z 2.21 $(a, n) = 1$.

„$\Longleftarrow$“: Ak $(a, n) = 1$, tak podľa Vety 2.20 $\exists u, v \in \mathbb{Z}$: $au + nv = 1$. Potom $[a]_n \cdot [u]_n = [au]_n = [1 - nv]_n = [1]_n$. Teda $[u]_n$ je inverziou k $[a]_n$. □

Definícia 3.15. Nech $(M, \cdot, e)$ je monoid. Potom $M^\times$ je množina všetkých invertibilných prvkov množiny M, t. j. $M^\times = \{a \in M \mid \exists b \in M : ab = ba = e\}$.

Lemma 3.16. *$M^\times$ je uzavretá na násobenie a inverziou ab je $b^{-1}a^{-1}$.*

Dôkaz. Máme $aa^{-1} = a^{-1}a = e$ a tiež $bb^{-1} = b^{-1}b = e$.

Potom $ab \cdot b^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$ a tiež $b^{-1}a^{-1} \cdot ab = b^{-1}eb = b^{-1}b = e$. □

Definícia 3.17. Nech p je prvočíslo. Potom $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{[0]_p\} = \mathbb{Z}_p^*$. (Lebo $(0, n) = n$.)

Veta 3.18. *$(\mathbb{Z}_p^\times, \cdot)$ je komutatívna grupa pre každé prvočíslo p.*

Dôkaz. Nech $[a]_p, [b]_p \in \mathbb{Z}_p^\times$. Potom $p \nmid a$, $p \nmid b$ a keďže p je prvočíslo, tak $p \nmid ab$. Teda $[a]_p \cdot [b]_p = [a \cdot b]_p \in \mathbb{Z}_p^\times$, takže $\mathbb{Z}_p^\times$ je grupoid. Podľa Vety 3.13 je $(\mathbb{Z}_p^\times, \cdot)$ komutatívny monoid. Nakoniec, keďže p je prvočíslo, tak pre každé $a \in \mathbb{Z}$, $p \nmid a$ platí $(a, p) = 1$. Každé také a teda má inverziu (Lemma 3.14). □

3.4 Eulerova funkcia

Definícia 3.19 (Eulerova funkcia ϕ)**.** $\phi : \mathbb{N} \to \mathbb{N}$, kde $\phi(n) = |\{a \mid a \leq n \wedge (a, n) = 1\}|$.

Veta 3.20. *Číslo p je prvočíslo práve vtedy, keď $\phi(p) = p - 1$.*

Dôkaz. „$\Longrightarrow$“: Každé prirodzené číslo menšie ako p je nesúdeliteľné s p.

„$\Longleftarrow$“: Predpokladajme, že p nie je prvočíslo. Potom $p = 1$ alebo p je zložené. Ak $p = 1$, tak $\phi(p) \neq p - 1$. Ak p je zložené, tak má kladného deliteľa, teda $\phi(p) \neq p - 1$ ※ . □

Veta 3.21. *Nech p je prvočíslo a $e \in \mathbb{N}$. Potom $\phi(p^e) = p^{e-1} \cdot (p - 1) = p^e(1 - \frac{1}{p})$.*

Dôkaz. Súdeliteľné s p^e sú $p, 2p, 3p, \ldots, p^{e-1}p$. Týchto čísel je p^{e-1}.

Nesúdeliteľných s p^e je potom $p^e - p^{e-1} = p^{e-1} \cdot (p - 1) = p^e(\frac{p-1}{p}) = p^e(1 - \frac{1}{p})$. □

Veta 3.22. *Nech prvočíselný rozklad čísla $n \in \mathbb{N}$ je $n = \prod_{i=1}^m p_i^{e_i} = p_1^{e_1}p_2^{e_2} \cdots p_m^{e_m}$, kde p_i sú po dvoch rôzne prvočísla. Potom*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_m}\right).$$

Dôkaz. Indukciou. Budeme opäť hľadať najprv čísla súdeliteľné s n.

Nech $n = p_1^{e_1}$. Existuje $\frac{n}{p_1}$ čísel menších ako n, ktoré sú deliteľné p_1. Počet čísel, ktoré toto nespĺňajú je teda $n - \frac{n}{p_1} = p_1^{e_1} - p_1^{e_1-1} = p_1^{e_1}(1 - \frac{1}{p_1}) = n(1 - \frac{1}{p_1})$.

Nech $n = p_1^{e_1}p_2^{e_2}$. Existuje $\frac{n}{p_1}$ čísel menších ako n, ktoré sú deliteľné p_1. Ďalej existuje $\frac{n}{p_2}$ čísel menších ako n, ktoré sú deliteľné p_2. Ak sčítame, dostaneme počet $\frac{n}{p_1} + \frac{n}{p_2}$, ale podľa

PIE[2] musíme odpočítať $\frac{n}{p_1p_2}$ čísel, teda máme $\frac{n}{p_1}+\frac{n}{p_2}-\frac{n}{p_1p_2}$. Počet čísel, ktoré toto nespĺňajú je teda $n-(\frac{n}{p_1}+\frac{n}{p_2}-\frac{n}{p_1p_2})=\frac{np_1p_2-np_2-np_++n}{p_1p_2}=n\frac{p_1p_2-p_2-p_1+1}{p_1p_2}=n(1-\frac{1}{p_1}-\frac{1}{p_2}+\frac{1}{p_1p_2})=n((1-\frac{1}{p_1})-\frac{1}{p_2}(1-\frac{1}{p_1}))=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})$.

IK: $\phi(n)=n-\left(\sum_{1\le i\le m}\frac{n}{p_i}-\sum_{1\le i_1<i_2\le m}\frac{n}{p_{i_1}p_{i_2}}+\cdots+(-1)^{m+1}\frac{n}{p_1p_2\ldots p_m}\right)$, z toho $\phi(n)=n\left(1-\sum_{1\le i\le m}\frac{1}{p_i}+\sum_{1\le i_1<i_2\le m}\frac{1}{p_{i_1}p_{i_2}}-\cdots+(-1)^m\frac{1}{p_1p_2\ldots p_m}\right)=n\prod_{p|n}\left(1-\frac{1}{p}\right)$. □

Veta 3.23. *Nech $a,b\in\mathbb{N}$. Ak $(a,b)=1$, tak $\phi(ab)=\phi(a)\cdot\phi(b)$.*

Dôkaz. Pri použití Vety 3.22 vidíme, že ak a,b sú nesúdeliteľné, majú rôzne činitele vo svojich prvočíselných rozkladoch a multiplikativita Eulerovej funkcie je potom zrejmá. □

Dôkaz (iný). Pozri [2, I.3.16]. □

3.5 Cvičenia

1. Spočítajte $[425]_{793}^{-1}$ v $(\mathbb{Z}_{793},+)$.
2. Spočítajte $[425]_{793}^{-1}$ v $(\mathbb{Z}_{793}^{\times},\cdot)$.
3. Spočítajte $|\mathbb{Z}_{2014}^{\times}|$.
4. Nájdite všetky $n\in\mathbb{N}$ také, že $|\mathbb{Z}_n^{\times}|=12$.
5. Určte zvyšok po delení čísla a číslom b:
   (a) $a=23^{2014}$, $b=25$;
   (b) $a=42^{2014}$, $b=60$;
   (c) $a=15^{15^{15}}$, $b=13$.
6. Určte najväčší rád prvku v grupe:
   (a) $\mathbb{S}_9$;
   (b) $\mathbb{S}_{10}$.
7. Určte rád prvku a v grupe G:
   (a) $a=[2]_{257}$, $G=(\mathbb{Z}_{257}^{\times},\cdot)$;
   (b) $a=[k]_n$, $G=(\mathbb{Z}_n,+)$, $k,n\in\mathbb{N}$;
   (c) $A=\left(\begin{smallmatrix}1&0\\2&1\end{smallmatrix}\right)$, $G=(GL_2(\mathbb{R}),\cdot)$;
   (d) $A=\left(\begin{smallmatrix}1&\sqrt{3}\\-\sqrt{3}&1\end{smallmatrix}\right)$, $G=(GL_2(\mathbb{R}),\cdot)$;
   (e) $A=\left(\begin{smallmatrix}1&-1\\3&2\end{smallmatrix}\right)$, $G=(GL_2(\mathbb{R}),\cdot)$.

[2] The Principle of Inclusion-Exclusion

3.6 Návody k riešeniu cvičení

1. $[425]_{793}^{-1} = [-425]_{793} = [368]_{793}$
2. $[425]_{793}^{-1} = [-153]_{793} = [640]_{793}$
3. $|\mathbb{Z}_{2014}^{\times}| = \phi(2014) = \phi(2) \cdot \phi(19) \cdot \phi(53) = 936$
4. Možné prvočísla: $2, 3, 5, 7, 13$.
   - Ak máme v rozklade 13: $n = 13, 26$
   - Ak nemáme v rozklade 13, máme 7: $n = 21, 42, 28$
   - Ak nemáme v rozklade $13, 7$, máme 5: neexistuje
   - Ak nemáme v rozklade $13, 7, 5$, máme $2, 3$: $n = 36$
5. (a) $\phi(25) = 20$, teda $23^{2014} \equiv 23^{14} \equiv (-2)^{14} \equiv 4^7 \equiv 4^{4+2+1} \equiv 9 \pmod{25}$
   (b) $42^{2014} = 12 \cdot 7 \cdot 21 \cdot 42^{2012} \mod 12 \cdot 5 = 12 \cdot (7 \cdot 21 \cdot 42^{2012} \mod 5)$;
   $7 \cdot 21 \cdot 42^{2012} \equiv 2 \cdot 1 \cdot 1 \pmod 5$, teda $42^{2014} \equiv 12 \cdot 2 \pmod{60} \equiv 24 \pmod{60}$
   (c) $\phi(13) = 12$, $15^{15} \equiv x \pmod{12}$;
   $(15^{15}, 12) = 3$, preto $15^{15} = 3 \cdot 5 \cdot 15^{14} \pmod{3 \cdot 4} = 3 \cdot (5 \cdot 15^{14} \mod 4)$;
   $5 \cdot 15^{14} \equiv 1 \cdot (-1)^{14} \equiv 1 \pmod 4$, preto $15^{15} \equiv 3 \cdot 1 \pmod{12}$;
   t. j. $a = 15^{15^{15}} \equiv 15^3 \equiv 8 \pmod{13}$
6. (a) Vezmeme mocniny prvočísel ≤ 9 (t. j. $2, 3, 2^2, 5, 7, 2^3, 3^2$):

Dĺžka cyklu	$(2) \circ (7)$	$(3) \circ (5)$	$(4) \circ (5)$	$(7) \circ (2)$	$(8) \circ (1)$	(9)
Rád (nsn)	14	15	**20**	14	8	9

   (b) 30.
7. (a) $2^8 \equiv -1 \pmod{257}$, $2^{16} \equiv 1 \pmod{257}$; rád $[2]_{257}$ je 16.
   (b) $kx \equiv 0 \pmod n \iff n \mid kx \iff (n,k) \cdot \frac{n}{(n,k)} \mid \frac{k}{(n,k)} \cdot x \cdot (n,k) \iff \frac{n}{(n,k)} \mid \frac{k}{(n,k)} \cdot x \iff \frac{n}{(n,k)} \mid x$. Najmenšie také x je $\frac{n}{(n,k)}$.
   (c) $\left(\begin{smallmatrix} 1 & 0 \\ 2 & 1 \end{smallmatrix}\right)^n = \left(\begin{smallmatrix} 1 & 0 \\ 2n & 1 \end{smallmatrix}\right)$; rád a je ∞.
   (d) $A^3 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \implies A^6 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$; rád a je 6.
   (e) $\det A = 5$; $\det A^n = 5^n$; rád a je ∞.

Kapitola 4: Grupy ďalej

4.1 Podgrupy a generovanie

Definícia 4.1. Nech $(G, \cdot)$ je grupa, H neprázdna podmnožina množiny G. Potom H je *podgrupa* grupy G; píšeme $H \leq G$; ak platí:

1. $1_G \in H$;
2. ak $a, b \in H$, tak $ab \in H$;
3. ak $a \in H$, tak $a^{-1} \in H$.

Dôsledok 4.2. *$(H, \cdot)$ je grupa. Ak $(G, \cdot)$ je komutatívna, tak aj $(H, \cdot)$ je komutatívna.*

Dôsledok 4.3. *$(\{e\}, \cdot)$ je tzv. triviálna podgrupa grupy $(G, \cdot)$ a je to najmenšia podgrupa. $(G, \cdot)$ je sama sebe podgrupou a je najväčšia. Iné podgrupy ako tieto dve nazývame vlastné.*

Dôsledok 4.4. *Vlastnosť „byť podgrupou“ je tranzitívna.*

Príklad 4.5. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$.

Príklad 4.6. $(\mathbb{Q}^*, \cdot) \leq (\mathbb{R}^*, \cdot) \leq (\mathbb{C}^*, \cdot)$.

Veta 4.7. *Nech $n \in \mathbb{N}_0$. Grupa $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ je jedinou podgrupou grupy $(\mathbb{Z}, +)$.*

Dôkaz. Nech H je nejaká netriviálna podgrupa grupy $(\mathbb{Z}, +)$. Nech $n \in H$ je najmenší kladný prvok v H. (Ak by tam bolo $-n$, kde $n \in \mathbb{N}$, tak je tam aj n.) Ukážeme, že $n\mathbb{Z} = H$:

- $n\mathbb{Z} \subseteq H$: Ak $n \in H$, tak aj $\ldots, -3n, -2n, -n, 0, n, 2n, 3n, \cdots \in H$.
- $n\mathbb{Z} \supseteq H$: Nech $m \in H \setminus n\mathbb{Z}$. Potom $m \neq 0$ a $-m \in H \setminus n\mathbb{Z}$. Predpokladajme $m > 0$ (inak vezmime $-m$). Z deliteľnosti platí $m = qn + r$, kde $0 \leq r < n$.

  Ak $r = 0$, tak $m = qn \in n\mathbb{Z}$, preto $0 < r < n$. Z toho ale $r = m - qn \in H$, čo by znamenalo, že n nebol najmenší kladný prvok v H. Preto $H \setminus n\mathbb{Z} = \emptyset$.

Pre $n = 0$ triviálne. □

Veta 4.8. *Nech $k, n \in \mathbb{N}$. $k\mathbb{Z}_n = \{k[x]_n \mid x \in \mathbb{Z}\}$ je jedinou podgrupou grupy $(\mathbb{Z}_n, +)$.*

Dôkaz. Nech H je nejaká netriviálna podgrupa grupy $(\mathbb{Z}_n, +)$ tvaru $k\mathbb{Z}_n$, kde $k \in \mathbb{N}, k \mid n$. Nech k je najmenšie kladné číslo také, že $[k]_n$ je prvkom H.

Všetko dokážeme analogicky predošlému dôkazu, stačí len overiť, že $k \mid n$. Nech $n = kq + r$, kde $q \in \mathbb{Z}$, $r \in \{0, 1, \ldots, k-1\}$.

- $[n]_n = [0]_n \in H$.
- $[n]_n = [k]_n \cdot q + [r]_n$. $[k]_n \in H$, $[k]_n \cdot q \in H$, preto musí aj $[r]_n \in H$, t. j. $r = 0$.

□

Dôsledok 4.9. *Z Viet 4.7, 4.8:*

- $k\mathbb{Z} \subseteq l\mathbb{Z} \iff l \mid k$.
- $k\mathbb{Z}_n \subseteq l\mathbb{Z}_n \iff l \mid k$, *kde* $k, l \mid n$.
- $k\mathbb{Z} \cap l\mathbb{Z} = nsn(k, l) \cdot \mathbb{Z}$.
- $\langle k\mathbb{Z} \cup l\mathbb{Z} \rangle = NSD(k, l) \cdot \mathbb{Z}$.

Lemma 4.10. *Prienik H ľubovoľného systému[3] $(H_i)_{i \in I}$ podgrúp grupy $(G, \cdot)$ je znovu podgrupou grupy $(G, \cdot)$.*

[3] Systém je v podstate množina množín, len s iným značením: $(H_i)_{i \in I} = \{H_i \mid i \in I\}$.

Dôkaz. Ak $I = \emptyset$, tak $H = G$.
Ak $I \neq \emptyset$, tak $1 \in H$; ďalej $\forall i \in I : a, b \in H_i \implies ab, a^{-1} \in H_i$; a teda $ab, a^{-1} \in H$. □

Lemma 4.11. *Nech $(G, \cdot)$ je grupa, $M \subseteq G$ je podmnožinou množiny G. Potom existuje najmenšia (vzhľadom k inklúzii) podgrupa grupy $(G, \cdot)$ obsahujúca množinu M.*

Túto najmenšiu podgrupu značíme $\langle M \rangle$ a čítame „podgrupa generovaná množinou M“.

Dôkaz. Nech $(H_i)_{i \in I}$ je systém všetkých podgrúp grupy $(G, \cdot)$ obsahujúcich množinu M. Do tohto systému patrí G a $\langle M \rangle = \bigcap_{i \in I} H_i$. $\langle M \rangle$ je najmenšia, lebo $\forall i \in I : \langle M \rangle \subseteq H_i$. □

Veta 4.12. *Ľubovoľná množina generuje podgrupu. Nech $(G, \cdot)$ je grupa, $M \subseteq G$ je podmnožinou množiny G. Potom $\langle M \rangle = X = \{g_1^{e_1} \cdot \ldots \cdot g_n^{e_n} \mid n \in \mathbb{N}_0, g_i \in M, e_i \in \{-1, 1\}\}$.*

Vzorový dôkaz pre generovanie:

1. $M \subseteq X$.
2. X je podgrupa.
3. Ak Y je podgrupa a $M \subseteq Y$, tak $X \subseteq Y$.

□

Ukážka použitia dôkazu:

1. Nech $g \in M$. Volíme $n = 1, g_n = g, e_n = 1$. Potom $M \subseteq \langle M \rangle = X = \{g\}$.
2. X je podgrupa.
   (a) Neutrálny prvok dostanem pre $n = 0$ alebo vezmem $g \in M$ a uvážim $g \cdot g^{-1}$.
   (b) Nech $a = g_1^{e_1} \cdot \ldots \cdot g_m^{e_m}$, $b = h_1^{f_1} \cdot \ldots \cdot h_n^{f_n}$. Potom ab je nášho tvaru.
   (c) Nech $a = g_1^{e_1} \cdot \ldots \cdot g_m^{e_m}$. Potom $a^{-1} = g_m^{-e_m} \cdot \ldots \cdot g_1^{-e_1}$ je nášho tvaru.
3. $\forall g_1, \ldots, g_m \in M$ platí $g_i \in Y$. Ďalej $g_1^{e_1}, \ldots, g_m^{e_m} \in Y$. Nakoniec $g_1^{e_1} \cdot \ldots \cdot g_m^{e_m} \in Y$.

□

Dôsledok 4.13. *Nech $M = \{a\}$. Potom $\langle M \rangle = \langle \{a\} \rangle = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$.*

Definícia 4.14. Grupa $(G, \cdot)$ je cyklická, ak existuje $a \in G$ také, že $\langle a \rangle = G$.

Príklad 4.15. $(\mathbb{Z}, +)$, kde $a = 1$ alebo $(\mathbb{Z}_n, +)$, kde $a = [1]_n$. (Iné neexistujú, pozri 4.22.)

Lemma 4.16. *Nech $(S, \cdot)$ je pologrupa, $M \subseteq S$. Potom $\langle M \rangle_{SEMIGROUPS} = \{a_1 \cdot \ldots \cdot a_n \mid n \in \mathbb{N}, a_1, \ldots, a_n \in M\}$.*

Lemma 4.17. *Nech $(S, \cdot, e)$ je monoid, $M \subseteq S$. Potom $\langle M \rangle_{MONOIDS} = \{\ldots n \in \mathbb{N}_0 \ldots\}$*

4.2 Homomorfizmy grúp

Definícia 4.18. Zobrazenie $\varphi\colon G \to H$ je (homo)morfizmus grupy $(G, \cdot)$ do grupy $(H, \circ)$, ak pre všetky $a, b \in G$ platí: $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$.

Lemma 4.19. *Nech $\varphi\colon (G, \cdot) \to (H, \circ)$ je homomorfizmus grúp. Potom:*

1. $\varphi(1_G) = 1_H$;
2. $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

Dôkaz. $\forall a \in G$:

1. $\varphi(a) = \varphi(1_G \cdot a) = \varphi(1_G) \circ \varphi(a)$. Analogicky $\varphi(a \cdot 1_G)$. Teda $\varphi(1_G)$ je jednička v H.
2. $\varphi(a \cdot a^{-1}) = \varphi(1_G) = 1_H$. Ďalej $\varphi(a \cdot a^{-1}) = \varphi(a) \circ \varphi(a^{-1}) = 1_H$, teda $\varphi(a^{-1}) = (\varphi(a))^{-1}$.

□

Definícia 4.20. Bijektívny homomorfizmus nazývame *izomorfizmus*. Ak existuje izomorfizmus medzi grupami G, H, nazývame ich izomorfné a píšeme $G \cong H$.

Príklad 4.21. $(\mathbb{R}^+, \cdot) \cong (\mathbb{R}, +)$, pretože $log(a \cdot b) \mapsto log(a) + log(b)$.

Poznámka. Izomorfizmus definuje reláciu ekvivalencie. Z hľadiska algebry medzi izomorfnými objektmi nerozlišujeme – zaujíma nás len štruktúra objektov.

Veta 4.22. *$(\mathbb{Z}, +)$ a $(\mathbb{Z}_n, +)$ sú (až na izomorfizmus) jediné dve cyklické grupy.*

Dôkaz. Nech $(G, \cdot)$ je cyklická grupa s generátorom a.

a) Nech rád a je 0 (t. j. grupa G je nekonečná). Vieme, že $\ldots, a^{-1}, 1, a, a^2, \ldots$ sú po dvoch rôzne. Definujme preto zobrazenie $\varphi\colon G \to \mathbb{Z}$ vzťahom $a^k \mapsto k$.
   - Morfizmus: $\varphi(a^k \cdot a^l) = \varphi(a^{k+l}) = k + l$ a aj $\varphi(a^k) + \varphi(a^l) = k + l$.
   - Injektívny: $\ldots, a^{-1}, 1, a, a^2, \ldots$ sú po dvoch rôzne.
   - Surjektívny: $\forall k \in \mathbb{Z}$ vrátim a^k.

b) Nech rád a je $n \in \mathbb{N}$ (t. j. grupa G je konečná). Potom $a^k = a^l$ práve keď $k \equiv l \pmod{n}$, kde $k, l \in \mathbb{Z}$. Definujme preto zobrazenie $\varphi\colon G \to \mathbb{Z}_n$ vzťahom $a^k \mapsto [k]_n$.
   - Morfizmus: $\varphi(a^k \cdot a^l) = \varphi(a^{k+l}) = [k+l]_n$ a aj $\varphi(a^k) + \varphi(a^l) = [k]_n + [l]_n = [k+l]_n$.
   - Injektívny: $1, a, a^2, \ldots, a^{n-1}$ sú po dvoch rôzne.
   - Surjektívny: $\forall [k]_n \in \mathbb{Z}_n$ vrátim a^k.

□

Príklad 4.23. $(\{-1, 1\}, \cdot) \cong (\mathbb{Z}_2, +)$, pretože $1 \mapsto 0$ a $-1 \mapsto 1$.

Príklad 4.24. $(\mathbb{Z}, +) \cong (n\mathbb{Z}, +)$, pretože $a \mapsto na$.

Definícia 4.25. Počet prvkov konečnej grupy $(G, \cdot)$ nazývame rád grupy a značíme ho $|G|$.

Veta 4.26. *Nech $(G, \cdot)$ je cyklická grupa s generátorom a. Rád generátora je rovný $|G|$.*

Definícia 4.27. *Endomorfizmus* je homomorfizmus grupy G na seba.

Definícia 4.28. *Automorfizmus* je izomorfizmus grupy G na seba.

Veta 4.29. *$(End(G), \circ)$ je monoid.*

Veta 4.30. *$(Aut(G), \circ)$ je grupa.*

4.3 Súčiny grúp

Definícia 4.31. Nech $(G, \cdot)$, $(H, \circ)$ sú grupy. Na množine $G \times H$ definujeme operáciu $\times$ vzťahom $(g, h) \times (g', h') = (g \cdot g', h \circ h')$.

Dôsledok 4.32. *$(G \times H, \times)$ je grupa. Súčin komutatívnych grúp je komutatívna grupa.*

Dôkaz. Operácie v G, H sú korektné a asociatívne (a príp. komutatívne). Neutrálnym prvkom je $(1_G, 1_H)$ a $(g, h)^{-1} = (g^{-1}, h^{-1})$. □

Lemma 4.33. *Zobrazenie $\Sigma : G \times H \to G$ definované $(g, h) \mapsto g$ je surjektívny homomorfizmus $(G, \cdot) \times (H, \circ)$ na $(G, \cdot)$.*

Definícia 4.34. Nech $(G_1, \cdot), \ldots, (G_n, \cdot)$ sú grupy a $n \geq 2$. Na množine $G_1 \times \cdots \times G_n$ definujeme súčin analogicky vzťahom $(g_1, \ldots, g_n) \times (g'_1, \ldots, g'_n) = (g_1 \cdot g'_1, \ldots, g_n \cdot g'_n)$.

Veta 4.35 (Klasifikácia Abelovských grúp)**.** *Nech $(G, \cdot)$ je komutatívna grupa, $|G| = n$. Potom $(G, \cdot) \cong (\mathbb{Z}_{p_1^{e_1}}, +) \times \cdots \times (\mathbb{Z}_{p_m^{e_m}}, +)$, kde $p_1, \ldots, p_m$ sú prvočísla (nie nutne rôzne), $e_1, \ldots, e_m \in \mathbb{N}$ a $n = p_1^{e_1} \cdot \ldots \cdot p_m^{e_m}$. Tento rozklad je jednoznačný (až na poradie činiteľov).*

Príklad 4.36. $(\mathbb{Z}_2, +) \times (\mathbb{Z}_3, +) \cong (\mathbb{Z}_6, +)$. Obe sú cykl.; generované $([1]_2, [1]_3)$ resp. $[1]_6$.

Príklad 4.37. $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +) \ncong (\mathbb{Z}_4, +)$. Prvá grupa nie je cyklická, druhá áno.

Príklad 4.38. Ak $n = 8$, tak existujú tri navzájom neizomorfné grupy (nepíšeme $+$): $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$; $\mathbb{Z}_2 \times \mathbb{Z}_4$; $\mathbb{Z}_8$.

Príklad 4.39. Ak $n = 36$, tak existujú štyri navzájom neizomorfné grupy (nepíšeme $+$): $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$; $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$; $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9$; $\mathbb{Z}_4 \times \mathbb{Z}_9$. Ďalej napr. $\mathbb{Z}_{36} \cong \mathbb{Z}_4 \times \mathbb{Z}_9$.

4.4 Cayleyho vety

Lemma 4.40. *Nech $(M, \cdot), (N, \circ)$ sú monoidy. Definujme homomorfizmus φ: $(M, \cdot) \to (N, \circ)$. Potom $\varphi(M)$ je podmonoid monoidu $(N, \circ)$.*

Poznámka. Morfizmus monoidov vyžaduje $1_M \mapsto 1_N$, teda v tomto prípade $1_M \mapsto id_{\varphi_N}$.

Veta 4.41 (Cayleyova pre monoidy)**.** *Ľubovoľný monoid $(M, \cdot)$ je izomorfný nejakému podmonoidu moniodu $(T(A), \circ)$. Za A je možné vziať M.*

Poznámka. Každá operácia v monoide sa dá previesť na skladanie zobrazení.

Dôkaz. Definujme zobrazenie $\varphi\colon M \to T(M)$ vzťahom $a \mapsto f_a$, kde $f_a\colon M \to M$ je transformácia definovaná vzťahom $x \mapsto ax$.

- φ je homomorfizmus z $(M, \cdot)$ do $(T(M), \circ)$. Pre všetky $x \in M$:
  - $\varphi(a \cdot b)(x) = f_{ab}(x) = (ab)x$
  - $(\varphi(a) \circ \varphi(b))(x) = (f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(bx) = a(bx) = (ab)x$
- φ je injektívne (t. j. ak $a \neq b$, tak $\varphi(a) \neq \varphi(b)$, t. j. $f_a \neq f_b$): Nech $f_a = f_b$. Potom $f_a(1) = f_b(1)$, t. j. $a \cdot 1 = b \cdot 1$, t. j. $a = b$.
- φ je surjektívne (t. j. $\forall f_a \in T(M)\ \exists a \in M\colon \varphi(a) = f_a$): vzorom f_a je a.

Našli sme bijektívny homomorfizmus, teda izomorfizmus. □

Veta 4.42 (Cayleyova pre pologrupy)**.** *Ľubovoľná pologrupa $(S, \cdot)$ je izomorfná nejakej podpologrupe pologrupy $(T(A), \circ)$. Za A je možné vziať S^1, kde $S^1 = S$, ak $(S, \cdot)$ je monoid, a $S^1 = S \cup \{e\}$, kde e je nový (dodefinovaný) neutrálny prvok, ak $(S, \cdot)$ je pologrupa.*

Dôkaz. Presne ako dôkaz Cayleyovej vety 4.41 pre monoidy. □

Veta 4.43 (Cayleyova pre grupy)**.** *Ľubovoľná grupa $(G, \cdot)$ je izomorfná nejakej podgrupe grupy permutácií $(S(A), \circ)$ nejakej množiny A. Za A je možné vziať G.*

Dôkaz. Definujme zobrazenie $\varphi\colon G \to S(G)$ vzťahom $a \mapsto f_a$, kde $f_a\colon G \to G$ je transformácia definovaná vzťahom $x \mapsto ax$.

Z dôkazu Vety 4.41 vieme, že f_a je injektívny homomorfizmus.

- f_a je injektívne: Nech $f_a(x) = f_a(y)$. Potom $ax = ay$, t. j. $x = y$.
- f_a je surjektívne: Nech $y \in G$. Hľadáme $x \in G$ také, že $f_a(x) = y$, t. j. $ax = y$, t. j. vezmem $x = a^{-1}y$.

□

4.5 Rozklady grúp podľa podgrúp

4.5.1 Ľavé triedy

Definícia 4.44. Nech $(G, \cdot)$ je grupa, H jej podgrupa, $a \in G$. Množinu $aH = \{ah \mid h \in H\}$ nazývame *ľavá trieda* (angl. coset) grupy G podľa podgrupy H.

Veta 4.45. *Pre grupu $(G, \cdot)$, jej podgrupu H a prvky $a, b \in G$ sú ekvivalentné vzťahy:*

1. $aH = bH$;
2. $a \in bH$;
3. $b^{-1}a \in H$.

Dôkaz. Dokážeme postupne tri implikácie.

„1. $\Rightarrow$ 2.“: $a = a \cdot 1_H \in aH$ a tiež $1_H \in bH$, teda $a \cdot 1_H \in bH$.

„2. $\Rightarrow$ 3.“: $\exists h \in H : a = bh$, preto po vynásobení b^{-1} máme $b^{-1}a = h \in H$.

„3. $\Rightarrow$ 1.“: $\exists h \in H : h^{-1}ah \in H$, preto $aH \subseteq bH$. Ďalej ak $b^{-1}a \in H$, tak $a^{-1}b \in H$ a teda $\exists h \in H : h^{-1}bh \in H$, preto $aH \supseteq bH$. □

Definícia 4.46. Nech $(G, \cdot)$ je grupa, H jej podgrupa, $a \in G$. Definujme *množinu všetkých ľavých tried* $G/H = \{aH \mid a \in G\}$, kde $aH = \{ah \mid h \in H\}$.

Lemma 4.47. *Množina G/H je rozklad na množine G. Všetky triedy tohto rozkladu sú rovnako mohutné.*

Dôkaz. Vyjdeme z definície rozkladu množiny:

1. $\emptyset \notin G/H$ (triedy rozkladu sú neprázdne): $a \in aH$.
2. Ak $A, B \in G/H$, tak $A \cap B = \emptyset \vee A = B$: Nech $c \in aH \wedge c \in bH$. Potom $aH = bH$. Máme $c = ah = bh'$, kde $h, h' \in H$, chceme $b^{-1}a \in H$: $ah = bh'$, teda $b^{-1}ah = h'$, teda $b^{-1}a = h'h^{-1} \in H$.
3. $\bigcup_{A \in G/H} A = G$ (zjednotenie všetkých rozložených podmnožín je pôvodná množina): $\bigcup_{a \in G} aH \supseteq \bigcup_{a \in G} \{a\} = G$.

□

Príklad 4.48. $G = (\mathbb{Z}, +), H = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}; \quad G/H = \mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$.

4.5.2 Lagrangeova veta

Veta 4.49 (Lagrangeova)**.** *Nech $(G, \cdot)$ je konečná grupa, $|G| = n$, H je podgrupou G.*

1. *$|G| = |G/H| \cdot |H|$.*
2. *Rád podgrupy delí rád grupy, t. j. $|H| \mid n$.*
3. *Rád prvku delí rád grupy, t. j. pre $a \in G$ rádu m platí $m \mid n$.*
4. *Ak je n prvočíslo, tak $(G, \cdot)$ je cyklická.*
5. *Pre $a \in G$ platí $a^n = 1$.*

Dôkaz.

1. G je zjednotením $|G/H|$ disjunktných množín (daných rozkladom G/H), z ktorých každá má rovnaký počet prvkov (pozri Lemma 4.47) a tento počet je $|H|$.
2. $n = k \cdot |H|$, kde $k = |G/H|$ (podľa 1.).
3. Rád prvku a je rovný rádu podgrupy $\langle a \rangle$. Ak $|\langle a \rangle| = m$, tak z 2. $m \mid n$.
4. Rád prvku $a \in G$ musí byť podľa 3. rovný 1 alebo n, takže $G = \langle a \rangle$ je cyklická grupa generovaná prvkom a. Ak má platiť 2., tak jediné možné podgrupy sú $\{1\}$ a G.

5. Z 3.: Ak $m \mid n$, tak $n = km$. Potom $a^n = a^{km} = 1$.

□

Veta 4.50 (Malá Fermatova)**.** *Ak p je prvočíslo, $a \in \mathbb{N}$, pričom $p \nmid a$, tak $a^{p-1} \equiv 1 \pmod{p}$.*

Dôkaz. Plynie z 5. časti Vety 4.49. □

Veta 4.51 (Eulerova)**.** *Ak $a, n \in \mathbb{N}$, pričom $(a, n) = 1$, tak $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Dôkaz. Uvážme $(\mathbb{Z}_n, \cdot)$. Potom $[a]_n$ má inverziu, práve keď $(a, n) = 1$. Ďalej $\mathbb{Z}_n^\times$ je množina všetkých invertibilných prvkov $\mathbb{Z}_n$. Potom $|\mathbb{Z}_n^\times| = \phi(n)$.

Použijeme 5. časť Vety 4.49 na $(\mathbb{Z}_n^\times, \cdot)$ a dostávame: $([a]_n)^{\phi(n)} = [1]_n$. □

Dôsledok 4.52. *Ak a je prvkom $(\mathbb{Z}_n, \cdot)$, tak $a^{-1} = a^{\phi(n)-1}$.*

4.5.3 Faktorové grupy

Definícia 4.53. Podgrupa $H \subseteq (G, \cdot)$ je *normálna*, ak $\forall g \in G\, \forall h \in H\colon g^{-1}hg \in H$.

Príklad 4.54. Nech $H = \{id, (1,2)\} \subseteq (\mathbb{S}_3, \circ)$. Potom $(1,2,3)^{-1} \circ (1,2) \circ (1,2,3) = (1,3)$, preto H *nie je* normálna.

Lemma 4.55. *Ak $(G, \cdot)$ je komutatívna, tak všetky jej podgrupy sú normálne* [2, I.9.3].

Definícia 4.56. Grupa $(G, \cdot)$ je *prostá* (angl. simple), ak je konečná a jedinými jej normálnymi podgrupami sú $\{1\}$ a G.

Príklad 4.57. $(\mathbb{Z}_p, +)$ alebo $(\mathbb{A}_n, \circ)$, kde $n \geq 5$ sú prosté grupy.

Veta 4.58. *Nech H je normálna v $(G, \cdot)$. Potom predpis $aH \cdot bH = (ab)H$ korektne definuje operáciu na množine G/H a $(G/H, \cdot)$ bude grupou.*

Dôkaz. Korektnosť: Nech $aH = cH$, $bH = dH$. Chceme $(ab)H = (cd)H$. Ak $aH = cH$, tak $c^{-1}a \in H$ (z Vety 4.45) a tiež ak $bH = dH$, tak $d^{-1}b \in H$. Chceme $(cd)^{-1}ab \in H$. Vezmime $(cd)^{-1}ab = d^{-1}c^{-1}ab = d^{-1}bb^{-1}c^{-1}ab$. Tento výraz patrí do H, lebo H je normálna.

Asociativita: $(aH \cdot bH) \cdot cH = (ab)H \cdot cH = ((ab)c)H = abcH$ a tiež $aH \cdot (bH \cdot cH) = \ldots$

Neutrálny prvok: H, lebo $H \cdot aH = 1H \cdot aH = aH = aH \cdot H$.

Inverzný prvok k aH je $a^{-1}H$, lebo $a^{-1}H \cdot aH = (a^{-1}a)H = H$ a tiež $aH \cdot a^{-1}H = \ldots$ □

Veta 4.59. *Nech H je normálna v $(G, \cdot)$. Potom $p\colon a \mapsto aH$ je surjektívny homomorfizmus $(G, \cdot)$ na $(G/H, \cdot)$. Zobrazenie p nazývame projekcia.*

Dôkaz. $p(ab) = (ab)H$ a tiež $p(a) \cdot p(b) = aH \cdot bH = (ab)H$. (Surjektivita triviálna.) □

Definícia 4.60. $(G/H, \cdot)$ je *faktorgrupa* grupy $(G, \cdot)$ podľa jej normálnej podgrupy H.

Príklad 4.61. $(\mathbb{Z}, +)/n\mathbb{Z} =: (\mathbb{Z}_n, +)$, kde $n \in \mathbb{N}_0$.

Príklad 4.62. $(\mathbb{R}^*, \cdot)/\{-1, 1\} \cong (\mathbb{R}^+, \cdot)$, pričom $(\mathbb{R}^*, \cdot)/\{-1, 1\} = \{a \cdot \{-1, 1\} \mid a \in \mathbb{R}^*\} = \{\{|a|, -|a|\} \mid a \in \mathbb{R}^*\}$. Bijekcia do $\mathbb{R}^+$ je daná predpisom $\{|a|, -|a|\} \mapsto |a|$.

Príklad 4.63. $(G, \cdot)/\{1\} \cong (G, \cdot)$.

Príklad 4.64. $(G, \cdot)/G \cong (\{1\}, \cdot)$.

Príklad 4.65. $(\mathbb{S}_n, \circ)/\mathbb{A}_n \cong (\{-1, 1\}, \cdot)$.

4.5.4 Veta Delo

Definícia 4.66. Nech $f\colon (G,\cdot) \to (H,\circ)$ je homomorfizmus grúp. Potom *jadro* homomorfizmu f je množina $Ker(f) = \{a \in G \mid f(a) = 1\}$.

Lemma 4.67. *Homomorfizmus $f\colon (G,\cdot) \to (H,\circ)$ je prostý, práve keď $Ker(f) = \{1\}$.*

Dôkaz. „$\Longrightarrow$“: 1 ide vždy na 1 a ak je zobrazenie prosté, tak nič ďalšie nejde na 1.

„$\Longleftarrow$“: Nech $f(a) = f(b)$. Chceme $a = b$. Po úprave $f(a) \cdot (f(b))^{-1} = 1$. Zároveň $f(a) \cdot (f(b))^{-1} = f(ab^{-1})$, teda $ab^{-1} \in Ker(f)$ + predpoklad $ab^{-1} = 1$, t. j. $a = b$. □

Veta 4.68 (Delo)**.** *Nech zobrazenie $\alpha\colon (G,\cdot) \to (H,\cdot)$ je surjektívny homomorfizmus grúp. Potom $Ker(\alpha)$ je normálna podgrupa v $(G,\cdot)$.*

Ďalej $\beta\colon aKer(\alpha) \mapsto \alpha(a)$ je surjektívny homomorfizmus $(G,\cdot)/Ker(\alpha)$ na $(H,\cdot)$.

Poznámka (Použitie)**.** Máme dané $(G,\cdot)$, K. Hľadáme $(G,\cdot)/K$. Uhádneme $(H,\cdot)$ a surjektívny homomorfizmus $\alpha\colon (G,\cdot) \to (H,\cdot)$ s jadrom K.

Príklad 4.69. Nech $G = (GL_n(\mathbb{R}),\cdot)$, $K = (SL_n(\mathbb{R}),\cdot)$. Uhádneme $(H,\cdot) = (\mathbb{R}^*,\cdot)$ a surjektívny homomorfizmus $\alpha\colon A \cdot K \mapsto |A|$.

Musíme ukázať, že α je surjektívny homomorfizmus s jadrom K:

Homomorfizmus: $\alpha(AK \cdot BK) = \alpha((AB)K) = |AB|$ a aj $\alpha(AK) \cdot \alpha(BK) = |A| \cdot |B|$.

Surjektívny: pre $r \in \mathbb{R}^*$ vezmeme $\begin{pmatrix} r & & 0 \\ & 1 & \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$.

S jadrom K: $AK \mapsto 1 \iff |A| = 1 \iff A \in SL_n(\mathbb{R})$.

Dôkaz. **Dôkaz Vety Delo**:

- $Ker(\alpha)$ je podgrupa: Chceme $1 \in Ker(\alpha)$. Nech $a, b \in Ker(\alpha)$, t. j. $\alpha(a) = \alpha(b) = 1$. Potom $\alpha(ab) = \alpha(a) \cdot \alpha(b) = 1$; $\alpha(a^{-1}) = (\alpha(a))^{-1} = 1^{-1} = 1$.
- $Ker(\alpha)$ je normálna: Nech $h \in Ker(\alpha)$, t. j. $\alpha(h) = 1$. Nech $a \in G$. Potom $\alpha(a^{-1}ha) = \alpha(a^{-1}) \cdot \alpha(h) \cdot \alpha(a) = 1$.
- β je homomorfizmus: $\beta(aKer(\alpha) \cdot bKer(\alpha)) = \beta((ab)Ker(\alpha)) = \alpha(ab)$; a aj $\beta(aKer(\alpha)) \cdot \beta(bKer(\alpha)) = \alpha(a) \cdot \alpha(b) = \alpha(ab)$.
- β je surjektívne: Nech $b \in H$. Potom $\exists a \in G\colon \alpha(a) = b$ a tak $\beta(aKer(\alpha)) = \alpha(a) = b$.
- β je injektívne: Nech $\beta(aKer(\alpha)) = 1_H$. Potom $\alpha(a) = 1_H = a$, t. j. $a \in Ker(\alpha)$, t. j. (podľa 4.45) $aKer(\alpha) = Ker(\alpha)$. Keďže $Ker(\alpha) = \{1\}$, použijem Lemmu 4.67.

□

4.6 Cvičenia

1. Popíšte grupu symetrií rovnostranného trojuholníka ($\mathbb{D}_3 = \mathbb{S}_3$) jej prezentáciou.
2. Popíšte všetky podgrupy grupy $\mathbb{Z}_6$.
3. Dokážte, že $M = \{a + b\sqrt{7} \mid a, b \in \mathbb{R}, a \neq 0 \vee b \neq 0\}$ je podgrupou grupy $(\mathbb{C}^*, \cdot)$.
4. Určte podgrupu $\mathbb{S}_8$ generovanú permutáciami $\sigma = (1,2,3,4) \circ (5,6,7,8)$ a $\pi = (1,8,3,6) \circ (2,7,4,5)$.
5. Popíšte všetky podgrupy grupy $\mathbb{A}_4$.
6. Je dané zobrazenie korektne definovaným homomorfizmom, resp. izomorfizmom? Ak áno, určte jeho jadro a obraz.
   (a) $\alpha\colon \mathbb{Z}_6 \times \mathbb{Z}_8 \to \mathbb{Z}_{48}$, $([a]_6, [b]_8) \mapsto [4a + 6b]_{48}$, kde $a, b \in \mathbb{Z}$;
   (b) $\beta\colon (\mathbb{Z}_6, +) \times (\mathbb{Z}_8, +) \to (\mathbb{Z}_{24}, +)$, $([a]_6, [b]_8) \mapsto [4a + 6b]_{24}$, kde $a, b \in \mathbb{Z}$;
   (c) $\gamma\colon (\mathbb{Z}_3, +) \times (\mathbb{Z}_8, +) \to (\mathbb{Z}_{24}, +)$, $([a]_3, [b]_8) \mapsto [8a + 3b]_{24}$, kde $a, b \in \mathbb{Z}$;
   (d) $\delta\colon (\mathbb{Z}_7, +) \times (\mathbb{Z}_7, +) \to (\mathbb{Z}_7, +)$, $([a]_7, [b]_7) \mapsto [ab]_7$, kde $a, b \in \mathbb{Z}$.
7. Nech $(G, \circ)$ je grupa. Popíšte všetky homomorfizmy $(\mathbb{Z}, +) \to (G, \circ)$.
8. Popíšte endomorfizmus $\varphi\colon (\mathbb{Z}, +) \to (\mathbb{Z}, +)$.
9. Popíšte automorfizmus $\varphi\colon (\mathbb{Z}, +) \to (\mathbb{Z}, +)$.
10. Ukážte, že grupy $(\mathbb{Q}^*, \cdot)$ a $(\mathbb{Q}, +)$ nie sú izomorfné.
11. Ukážte, že grupy $(\mathbb{Z}, +)$ a $(\mathbb{Q}, +)$ nie sú izomorfné.
12. Nech G je grupa, $g \in G$. Homomorfizmus $\varphi\colon (\mathbb{Z}_n, +) \to (G, \cdot)$ taký, že $\varphi([1]_n) = g$ existuje práve vtedy, keď rád g delí n. Potom je tento homomorfizmus jediný.
13. Pre ktoré $n \in \mathbb{N}$ v $(S_{10}, \circ)$ existuje podgrupa izomorfná so $(\mathbb{Z}_n, +)$?
14. Pre ktoré $m, n \in \mathbb{N}$ je $(S_n, \circ, id)$ izomorfná s podgrupou monoidu $(T_m, \circ, id)$?
15. Nech $G = GL_2(\mathbb{R})$, $H = \{\left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right) \mid a, b \in \mathbb{R}^*\}$ je podgrupa G. Popíšte ľavé a pravé triedy rozkladu G podľa H.
16. Nech $G = (\{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \mid a, b \in \mathbb{R}, a \neq 0\}, \cdot)$, $H = \{\left(\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right) \mid x \in \mathbb{R}\}$ je podgrupa G. Dokážte, že H je normálna v G a určte, čomu je izomorfná grupa G/H.
17. Nech $G = (\{\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \mid a, b \in \mathbb{Z}\}, \cdot)$, $H = \{\left(\begin{smallmatrix} 1 & 0 & x \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right) \mid x \in \mathbb{Z}\}$ je podgrupa G. Dokážte, že H je normálna v G a určte, čomu je izomorfná grupa G/H.
18. Nech $G = (\{\left(\begin{smallmatrix} 1 & a & b+c\sqrt{2} \\ 0 & d & e \\ 0 & 0 & 1 \end{smallmatrix}\right) \mid a, e \in \mathbb{Z}, b, c \in \mathbb{Q}, d \in \{1, -1\}\}, \cdot)$, $H = \{\left(\begin{smallmatrix} 1 & 2p & q \\ 0 & 1 & r \\ 0 & 0 & 1 \end{smallmatrix}\right) \mid p, r \in \mathbb{Z}, q \in \mathbb{Q}\}$ je podgrupa G. Dokážte, že H je normálna v G a určte G/H.
19. Určte $GL_n(\mathbb{R})/SL_n(\mathbb{R})$.

20. Určte $(\mathbb{R},+)/(\mathbb{Z},+)$.

21. $G = (\{f\colon \mathbb{R}\to\mathbb{R} \mid \exists a\in\mathbb{R}^*\exists b\in\mathbb{R}\colon \forall x\in\mathbb{R}\colon f(x)=ax+b\},\circ)$. Ktorá z podgrúp $H=\{f \mid \exists a\in\mathbb{R}^*\colon \forall x\colon f(x)=ax\}$, $K=\{f \mid \exists b\in\mathbb{R}\colon \forall x\colon f(x)=x+b\}$ je norm.?

4.7 Návody k riešeniu cvičení

1.
   - Generátory: a = otočenie o $\frac{2\pi}{3}$, t. j. $(1,2,3)$; b = zrkadlenie podľa osi y, t. j. $(2,3)$
     - $\mathbb{D}_n$ je podgrupou $\mathbb{S}_n$ generovanou perm. $(1,2,\ldots,n)$ a $(1,n)\circ(2,n-1)\circ\ldots$
   - Pravidlá: $a^3=1$; $b^2=1$; $ab=baa$
   - Pomocou nich je možné každý prvok vyjadriť ako b^ia^j, kde $i\in\{0,1\}$, $j\in\{0,1,2\}$

2. $0\mathbb{Z}_6$, $1\mathbb{Z}_6$, $2\mathbb{Z}_6$, $3\mathbb{Z}_6$.

3.
   - Uzavrenosť: $(a+b\sqrt{7})\cdot(c+d\sqrt{7})=(ac+7bd)+(ad+bc)\sqrt{7}\in M$;
   - Neutrálny prvok: $1\in M \iff a=1,b=0$;
   - Inverzný prvok: $\forall x\in M\colon x^{-1}\in M$.

4. $\langle\sigma,\pi\rangle=\{id,\sigma,\pi,\sigma^2,\sigma^3,\sigma\circ\pi,\pi\circ\sigma,\sigma^2\circ\pi\}$.

5. $\mathbb{A}_4=\{id, a=(1,2)\circ(3,4), b=(1,3)\circ(2,4), c=(1,4)\circ(2,3), d=(1,2,3), e=(1,2,4), f=(1,3,4), g=(2,3,4), h=(1,3,2), i=(1,4,2), j=(1,4,3), k=(2,4,3)\}$.
   - Rád 1: $\{id\}$;
   - Rád 2: $\{a,id\},\{b,id\},\{c,id\}$;
   - Rád 3: $\{d,h,id\},\{e,i,id\},\{f,j,id\},\{g,k,id\}$;
   - Rád 4: $\{a,b,c,id\}$;
   - Rád 6: (nič);
   - Rád 12: $\mathbb{A}_4$;

6. (a)
   - Korektnosť: Ak $[a]_6=[c]_6$ a $[b]_8=[d]_8$, chceme $[4a+6b]_{48}=[4c+6d]_{48}$. Vieme, že $6\mid a-c$ a $8\mid b-d$. Protipríklad: $b=d=8$, $a=7$, $c=1$.
   - Záver: nie je zobrazením.

   (b)
   - Korektnosť: Ak $[a]_6=[c]_6$ a $[b]_8=[d]_8$, chceme $[4a+6b]_{24}=[4c+6d]_{24}$. Vieme, že $4\mid a-c$ a $6\mid b-d$. Potom aj $24\mid 4(a-c)+6(b-d)$.
   - Homomorfizmus:
     Ľ: $\beta(([a]_6,[b]_8)\circ([c]_6,[d]_8))=\beta(([a+c]_6,[b+d]_8))=[4(a+c)+6(b+d)]_{24}=[4a+6b+4c+6d]_{24}$
     P: $\beta(([a]_6,[b]_8))+\beta(([c]_6,[d]_8))=[4a+6b]_{24}+[4c+6d]_{24}=[(4a+6b)+(4c+6d)]_{24}=$ Ľ.

- Jadro: Ker $\beta = \{([a]_6, [b]_8) \mid a, b \in \mathbb{Z}, \beta(([a]_6, [b]_8)) = [0]_{24}\}$.
  $([a]_6, [b]_8) \in \text{Ker } \beta \iff \beta(([a]_6, [b]_8)) = [0]_{24} \iff [4a+6b]_{24} = [0]_{24} \iff 24 \mid 4a + 6b \iff 12 \mid 2a + 3b \iff 3 \mid a, 2 \mid b \iff a = 3x, b = 2y \iff 12 \mid 6x + 6y \iff 2 \mid x + y$.
  $\text{Ker } \beta = \{([0]_6, [0]_8), ([0]_6, [4]_8), ([3]_6, [2]_8), ([3]_6, [6]_8)\}$.
- Obraz β je podgrupa v $\mathbb{Z}_{24}$, t. j. je tvaru $k \cdot \mathbb{Z}_{24}$, kde $k \mid 24$ a $|k \cdot \mathbb{Z}_{24}| = \frac{24}{k}$. Obraz β je v $2 \cdot \mathbb{Z}_{24}$. Stačí ukázať, že generátor $2 \cdot \mathbb{Z}_{24}$, t. j. $[2]_{24}$ leží v obraze β. Potom budeme vedieť, že Im $\beta = 2 \cdot \mathbb{Z}_{24}$.
  Teda $[4a + 6b]_{24} = [2]_{24} \implies a = -1, b = 1$.
- Záver: je homomorfizmus, nie je izomorfizmus.

(c)
- Korektnosť, homomorfizmus: ako v (b).
- Jadro: Ker $\gamma = \{([0]_3, [0]_8)\}$, lebo $24 \mid 8a + 3b \iff 8 \mid b, 3 \mid a$. Hom. je inj.
- Obraz: $[1]_{24} \in \text{Im } \gamma$ ($a = -1, b = 3$). Hom. je surjektívny.
- Záver: je izomorfizmus. (Tiež $|\mathbb{Z}_3 \times \mathbb{Z}_8| = |\mathbb{Z}_{24}|$.)

(d)
- Korektnosť: platí.
- Homomorfizmus:
  Ľ: $\delta(([a]_7, [b]_7) + ([c]_7, [d]_7)) = \delta(([a + c]_7, [b + d]_7)) = [ab + ad + bc + cd]_7$
  P: $\delta(([a]_7, [b]_7)) + \delta(([c]_7, [d]_7)) = [ab]_7 + [cd]_7 = [ab + cd]_7 \neq$ Ľ.
  Protipríklad: $a = b = 1, c = 2, d = 3$.
- Záver: Je zobrazením, nie je homomorfizmom.

7. Každý homomorfizmus stačí zadať na nejakej množine generátorov. Množinou generátorov $\mathbb{Z}$ je $\{1\}$.

   Nech g generuje G. Definujeme zobrazenie $\alpha_g \colon 1 \mapsto g$. Potom $\alpha_g(1) \circ \alpha_g(1) \circ \alpha_g(1) \circ \cdots = g \circ g \circ g \circ \ldots$, teda $\alpha_g(n) = g^n$ pre $n \in \mathbb{N}$, kde $n = 1 + 1 + 1 + \ldots$.

   Ďalej $g^{-n} = (g^n)^{-1} = (g^{-1})^n$, teda definujeme $\forall z \in \mathbb{Z} \colon \alpha_g(z) = g^z$.

8. Zobrazenie $\varphi \colon (\mathbb{Z}, +) \to (\mathbb{Z}, +)$ je endomorfizmus práve vtedy, keď pre všetky $z \in \mathbb{Z}$ platí: $\varphi_k(z) = kz$, kde $k \in \mathbb{Z}$.

   - „ $\implies$ “: Nech φ je endomorfizmus, $\varphi_k(1) = k$. Keďže $z = 1 + \cdots + 1$ pre každé kladné z, tak $\varphi_k(z) = \varphi_k(1) + \cdots + \varphi_k(1) = k + \cdots + k = kz$ pre kladné z.
     Ďalej $\varphi_k(1) = \varphi_k(1 + 0) = \varphi_k(1) + \varphi_k(0)$, teda $\varphi_k(0) = 0 = 0k$. Z toho $\varphi_k(-1) = -k$ a nakoniec $\varphi_k(-n) = -kn$.
   - „ $\impliedby$ “: Nech $k \in \mathbb{Z}$ je také, že pre všetky $z \in \mathbb{Z}$ platí: $\varphi_k(z) = kz$. Potom $\varphi_k(z + y) = k(z + y) = kz + ky = \varphi_k(z) + \varphi_k(y)$. Dané zobrazenie je homomorfizmus.

   Potom $f \colon End((\mathbb{Z}, +)) \cong (\mathbb{Z}, \cdot)$. Platí $f(\varphi_k) = k$. Ak je to izomorfizmus, musí $f(\varphi_k \circ \varphi_l) = f(\varphi_k(\varphi_l)) = f(\varphi_{kl}) = kl$ a tiež $f(\varphi_k) \cdot f(\varphi_l) = k \cdot l$.

   Prvú časť overíme: $(\varphi_k \circ \varphi_l)(z) = \varphi_k(\varphi_l(z)) = \varphi_k(lz) = klz$ a tiež $(\varphi_k \circ \varphi_l)(1) = \varphi_k(\varphi_l(1)) = \varphi_k(l1) = kl1$. Preto $f(\varphi_k \circ \varphi_l) = (\varphi_k \circ \varphi_l)(1) = kl1$.

   Druhá časť: $f(\varphi_k) \cdot f(\varphi_l) = \varphi_k(1) \cdot \varphi_l(1) = k \cdot l$.

9. $Aut((\mathbb{Z},+)) \cong (\{1,-1\},\cdot)$.

10. Každé racionálne číslo q ide zapísať ako súčet dvoch rovnakých racionálnych čísel, teda $q = r + r$. Ale toto neplatí pre súčin dvoch rovnakých čísel. (Napr. $q = 2$.)

11. $(\mathbb{Z},+)$ je cyklická grupa generovaná prvkom 1. Naopak $(\mathbb{Q},+)$ cyklická nie je, lebo keby a/b bol jej generátor, tak by nebolo možné vygenerovať prvok c/d taký, že $(b,d) = 1$, keďže sčítaním zlomkov s rovnakým menovateľom dostaneme opäť zlomok s rovnakým menovateľom, príp. násobky.

12. „$\Longrightarrow$“: Ak $\varphi([1]_n) = g$, tak $\forall a \in \mathbb{Z}$ platí $\varphi([a]_n) = g^a$. Keď $a = n$, tak $\varphi([n]_n) = g^n$ a zároveň $\varphi([n]_n) = \varphi([0]_n) = g^0 = 1$, teda $g^n = 1$. To nastáva, práve keď rád g delí n.

    „$\Longleftarrow$“: Ak rád g delí n, tak $g^n = 1$. Ukážeme, že predpis $\varphi([a]_n) = g^a$ korektne zadáva homomorfizmus. Korektnosť: $\varphi([a+kn]_n) = g^{a+kn} = g^a \cdot (g^n)^k = g^a \cdot 1^k = g^a$. Homomorfizmus: ...

    Tento homomorf. je surjektívny, práve keď g generuje G. $\varphi(\mathbb{Z}_n) = \{g^a \mid a \in \mathbb{Z}\}$.

    Tento homomorfizmus je injektívny, práve keď rád g je rovný n.

    - „$\Longleftarrow$“: Nech φ zobrazí dva prvky na to isté, teda $\varphi([a]_n) = \varphi([b]_n)$, t. j. $g^a = g^b$, t. j. $g^{a-b} = 1$, t. j. rád g delí $a-b$. Rád g je z predpokladu n, takže ak $n \mid (a-b)$, tak $[a]_n = [b]_n$.
    - „$\Longrightarrow$“: obmenou. Nech rád g je nejaké $r \neq n$. Stačí uvažovať $r < n$. Potom $[0]_n \neq \varphi([r]_n) = g^r = 1$, teda φ nie je injektívne.

13. $(\mathbb{Z}_n,+)$ je komutatívna cyklická grupa. V S_m môžeme generovať cyklické komutatívne podgrupy len a práve jedným prvkom. Postup riešenia je teda zistiť všetky možné rády prvkov z S_m (pre nás S_{10}).

    Rád permutácie je nsn veľkostí jeho disjunktných cyklov.

    Riešením je $n \in \{1,2,3,4,5,6,7,8,9,10,12,14,15,20,21,30\}$.

14. Musí platiť, že $n \geq m$. T_m má m^m prvkov, ale len $m!$ z nich má inverziu (jedná sa práve o bijekcie).

    Pre $m < n$ má T_m menej invertibilných prvkov než S_n – teda nemôže existovať injektívny homomorfizmus z S_n do T_m.

    Pre $m \geq n$ má T_m aspoň toľko invertibilných prvkov ako je prvkov v S_n. Potom môže injektívny homomorfizmus fungovať takto: pošleme $f \in S_n$ na $g \in T_m$ tak, že $g(x) = f(x)$ pre $x \leq n$ a $g(x) = x$ pre $x > n \leq m$.

15. Ľavé: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \cdot H = \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) \cdot H$, práve keď $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)^{-1} \cdot \left(\begin{smallmatrix} e & f \\ g & h \end{smallmatrix}\right) \in H$, t. j. keď $\frac{1}{ad-bc}\left(\begin{smallmatrix} de-gb & df-bh \\ ag-ce & ah-cf \end{smallmatrix}\right) \in H$, t. j. keď $df - bh = 0 \wedge ag - ce = 0$.

    Pravé: $\ldots be - af = 0 \wedge ch - dg = 0$.

    Podgrupa H nie je v G normálna, pretože ľavé triedy sa $\neq$ pravým.

16. Normálna: $\left(\begin{smallmatrix} c & b \\ 0 & 1 \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} c & b \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a/c \\ 0 & 1 \end{smallmatrix}\right) \in H$.

    Množina ľavých tried: $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot H = \left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \cdot H$, práve keď $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \in H$, t. j. keď $\left(\begin{smallmatrix} c/a & (d-b)/a \\ 0 & 1 \end{smallmatrix}\right) \in H$, t. j. keď $c = a$.

    Hypotéza: $G/H \cong (\mathbb{R}^*, \cdot)$, t. j. $h\colon G/H \to (\mathbb{R}^*, \cdot)$, kde $h(\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot H) = a$.

    Korektnosť: $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot H = \left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \cdot H$; dokázané skôr.

    Homomorfizmus: $h(\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot H \cdot \left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \cdot H) = h(\left(\begin{smallmatrix} ac & ad+b \\ 0 & 1 \end{smallmatrix}\right) \cdot H) = ac$ a to sa rovná $h(\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot H) \cdot h(\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \cdot H) = a \cdot c$.

    Surjektívny: ak dostaneme $r \in \mathbb{R}^*$, chceme nájsť $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot H$ také, že $h(\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot H) = r$. Volíme $\left(\begin{smallmatrix} r & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

    Injektívny: ak $h(\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot H) = h(\left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \cdot H)$, tak $a = c$ a z korektnosti $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \cdot H = \left(\begin{smallmatrix} c & d \\ 0 & 1 \end{smallmatrix}\right) \cdot H$. Alternatívne z Vety Delo (4.68): H je jadro surjektívneho homomorfizmu h: $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in Ker(h)$, práve keď $h(\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right)) = 1$, t. j. keď $a = 1$, t. j. keď $\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right) \in H$.

    Potom H je normálna podgrupa v G a platí naša hypotéza.

17. Množina ľ. tried: $\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \cdot H = \left(\begin{smallmatrix} 1 & c & d \\ 0 & 1 & c \\ 0 & 0 & 1 \end{smallmatrix}\right) \cdot H$, práve keď $\left(\begin{smallmatrix} 1 & c-a & d-ac+a^2-b \\ 0 & 1 & c-a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in H$, t. j. $c = a$.

    Hypotéza: $G/H \cong (\mathbb{Z}, +)$, t. j. $\alpha\colon G \to (\mathbb{Z}, +)$, kde $\alpha(\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right)) = a$.

    Homomorfizmus: ...

    Surjektívny: vzorom $z \in \mathbb{Z}$ je $\left(\begin{smallmatrix} 1 & z & 3 \\ 0 & 1 & z \\ 0 & 0 & 1 \end{smallmatrix}\right)$.

    Injektívny: H je jadro surjektívneho homomorfizmu α: $\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in Ker(\alpha)$, práve keď $\alpha(\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right)) = 0$, t. j. keď $a = 0$, t. j. keď $\left(\begin{smallmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{smallmatrix}\right) \in H$.

    Potom H je normálna podgrupa v G a platí naša hypotéza.

18. Množina ľ. tried: $\ldots 2 \mid f - \frac{ai}{d} \wedge h - c = 0 \wedge \frac{i}{d} = 1$, t. j. keď $h = c \wedge i = d \wedge [f]_2 = [a]_2$ (posledná podmienka: keďže $i = d$, tak z $2 \mid f - \frac{ai}{d}$ dostávame $2 \mid f - a$).

    Hypotéza: $G/H \cong (\mathbb{Q}, +) \times (\{1, -1\}, \cdot) \times (\mathbb{Z}_2, +)$, t. j. $\alpha\colon G \to \mathbb{Q} \times \{1, -1\} \times \mathbb{Z}_2$, kde $\alpha(\left(\begin{smallmatrix} 1 & a & b+c\sqrt{2} \\ 0 & d & e \\ 0 & 0 & 1 \end{smallmatrix}\right)) = (c, d, [a]_2)$.

    Homomorfizmus: ...

    Surjektívny: vzorom $(c, d, [a]_2)$ je $\left(\begin{smallmatrix} 1 & a & c\sqrt{2} \\ 0 & d & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right)$.

    Injektívny: ...

19. Odhad: $(GL_n(\mathbb{R}), \cdot)/SL_n(\mathbb{R}) = \{A \cdot SL_n(\mathbb{R}) \mid A \in GL_n(\mathbb{R})\}$. V tomto popise výslednej množiny ale nedokážeme rozlíšiť dve rôzne matice zadávajúce rovnakú množinu.

    Kedy $A \cdot SL_n(\mathbb{R}) = B \cdot SL_n(\mathbb{R})$? Práve keď $A^{-1}B \in SL_n(\mathbb{R})$, t. j. keď $|A^{-1}B| = 1$, t. j. keď $|A| = |B|$. Preto

$$(GL_n(\mathbb{R}), \cdot)/SL_n(\mathbb{R}) = \left\{ \begin{pmatrix} r & & & \\ & 1 & & 0 \\ & & 1 & \\ & 0 & & \ddots \\ & & & & 1 \end{pmatrix} \cdot SL_n(\mathbb{R}) \mid r \in \mathbb{R}^* \right\}.$$

Táto grupa je v bijekcii α s $(\mathbb{R}^*,\cdot)$, kde $\alpha\left(\begin{pmatrix} r & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}\cdot SL_n(\mathbb{R})\right) = r$.

Iné riešenie: keďže $|A\cdot B| = |A|\cdot|B|$, dá sa odhadnúť $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \cong (\mathbb{R}^*,\cdot)$. Potom $\varphi\colon GL_n(\mathbb{R}) \to \mathbb{R}^*$, kde $\varphi(A) = |A|$. Potom φ je surjektívny homomorfizmus (vzorom ľub. $r \in \mathbb{R}^*$ je matica vyššie). Nakoniec $A \in Ker(\varphi)$, práve keď $\varphi(A) = 1$, t. j. keď $|A| = 1$, t. j. keď $A \in SL_n(\mathbb{R})$. Podľa Vety Delo...

20. Nech $x, y \in \mathbb{R}$. Potom $x+\mathbb{Z} = y+\mathbb{Z}$, práve keď $x-y \in \mathbb{Z}$, t. j. keď $x - \lfloor x\rfloor = y - \lfloor y\rfloor$.

    Odhad: $(\mathbb{R},+)/(\mathbb{Z},+) \cong G := (\{z\in\mathbb{C} \mid |z| = 1\},\cdot)$. Definujeme $\varphi\colon \mathbb{R}\to G$ také, že $\varphi(x) = e^{i2\pi x}$. Potom φ je homomorfizmus... Tento homomorfizmus je surjektívny, pretože každé $z \in \mathbb{C}$, kde $|z| = 1$ je tvaru $z = e^{i2\pi x}$ pre nejaké $x \in \mathbb{R}$.

    Nakoniec určíme $Ker(\varphi)$. Platí: $\varphi(x) = 1$, práve keď $2\pi x \in 2\pi\mathbb{Z}$, t. j. keď $x \in \mathbb{Z}$.

21. a) H: Nech $h \in H$, $g \in G$; $h(x) = ax$, $g(x) = bx+c$. Pýtame sa, či $g^{-1}\circ h\circ g \in H$: $(g^{-1}\circ h\circ g)(x) = g^{-1}(h(g(x))) = g^{-1}(a(bx+c)) = \frac{a(bx+c)-c}{b} = ax + \frac{c(a-1)}{b}$.

    Protipríklad: ak $h(x) = 2x$ a $g(x) = 5x+1$, tak $2x + \frac{1(2-1)}{5} \notin H$ – nie je norm.

    b) K: Analogicky. $g^{-1}\circ h\circ g \in K$, lebo $(g^{-1}\circ h\circ g)(x) = x + \frac{a}{b}$ – K je norm.

    Potom $G/K \cong (\mathbb{R}^*,\cdot)$: $g\circ K = i\circ K$, práve keď $g^{-1}\circ i \in K$, t. j. keď $b = d$. (Lebo $g^{-1}\circ i(x) = g^{-1}(dx+e) = \frac{dx+e-c}{b}$.) Potom $G\to\mathbb{R}^*$, $g\mapsto b$.

4.8 Appendix: šifrovanie

Veta 4.70 (Čínska zvyšková)**.** *Nech $a,b\in\mathbb{Z}$, $m,n\in\mathbb{N}$, $(m,n) = 1$. Potom*

$$a \equiv b \pmod m, \quad a\equiv b \pmod n \iff a \equiv b \pmod{mn}.$$

Dôkaz. „$\Longleftarrow$“: Máme $kmn = a-b$, teda $kn\cdot m, km\cdot n \mid (a-b)$.
„$\Longrightarrow$“: Máme $a-b = km = ln$, kde $m \mid l$, $mp = n$; teda $a-b = lmn$. □

Veta 4.71. *Nech p,q sú dve rôzne prvočísla, $n = pq$. Potom*

$$\forall a\in\mathbb{Z} \quad \exists k\in\mathbb{Z}\colon\ a^{k\varphi(n)} \equiv 1 \pmod n.$$

Dôkaz. Ak $(a,n) = 1$, tak platí Eulerova veta: $a^{\varphi(n)} \equiv 1 \pmod n$. Vezmeme k ľubovoľné a dostávame $(a^{\varphi(n)})^k \equiv 1^k \pmod n$, teda $a^{k\varphi(n)} \equiv 1 \pmod n$.

Ak $(a,n) \neq 1$, tak $a \equiv 0 \pmod p$ alebo $a\equiv 0 \pmod q$ (alebo oboje). Na základe Vety 4.70 stačí ukázať, že $a^{k\varphi(n)} \equiv 1$ modulo p a q zvlášť. V prvom prípade $a^{k(p-1)(q-1)} = (a^{p-1})^{k(q-1)} \equiv 1^{k(q-1)} \equiv 1 \pmod p$. Analogicky ukážeme druhý prípad modulo q. □

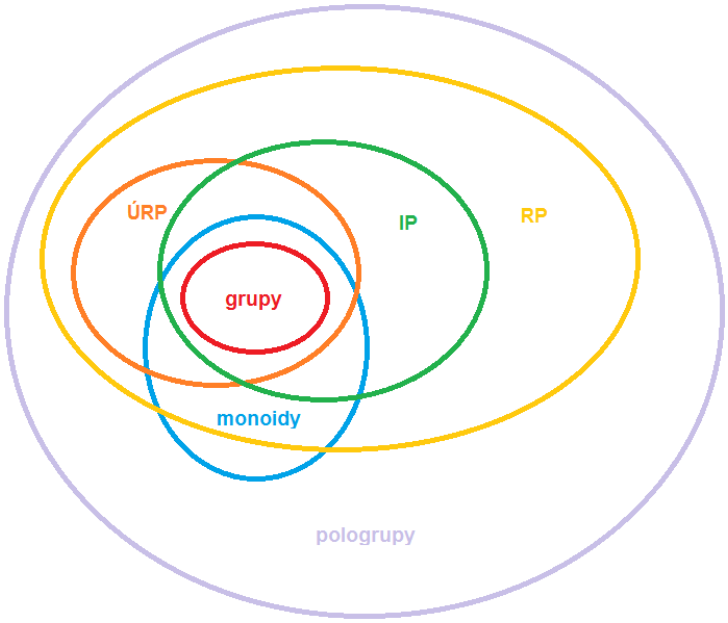
Veta 4.72 (RSA)**.** *Vezmime dve rôzne tajné prvočísla p,q. Spočítajme verejné $n = pq$. Spočítajme $\varphi(n)$. Vyberme verejné e také, že platí: $1 < e < \varphi(n)$ a $(e,\varphi(n)) = 1$. Spočítajme tajné d také, že $ed \equiv 1 \pmod{\varphi(n)}$.*

Šifrovanie: $c \equiv m^e \pmod n$ $(0 \le m < n)$. Dešifrovanie: $m \equiv c^d \pmod n$.

4.9 Appendix: ďalšie vlastosti grupových štruktúr

Definícia 4.73. Regulárne, inverzné a úplné regulárne pologrupy:

- **Regulárna** pologrupa („Každý jej prvok je regulárny.“):
  $\forall a \exists b\colon aba = a$
- **Inverzná** pologrupa („Každý jej prvok má jedinú inverziu.“):
  $\forall a \exists! b\colon aba = a, bab = b$
- **Úplná regulárna** pologrupa:
  $\forall a \exists b\colon aba = a, bab = b, ab = ba$



Príklad 4.74. Pologrupa $(T(A), \circ)$ je regulárna; nie je inverzná ani úplne regulárna.

Príklad 4.75. Pologrupa všetkých bijekcií (relácií) $(B(A \times A), \circ)$ nie je vždy regulárna.

Definícia 4.76 (Problém rozšírenia)**.** Máme dané grupy $(G, \cdot)$, $(H, \cdot)$. Hľadáme všetky dvojice $(K, \cdot)$, L také, že $(K, \cdot)$ je grupa, L je jej normálna podgrupa a platí: $(L, \cdot) \cong (G, \cdot)$ a zároveň $(K/L, \cdot) \cong (H, \cdot)$. Potom K je *rozšírením* grupy G pomocou grupy H.

Príklad 4.77. Pre dané G, H je príkladom rozšírenia $(K = G \times H, \cdot)$, $L = G \times \{1\}$. Podľa Vety 4.68: $\alpha\colon G \times H \to H$, kde $(g, h) \mapsto h$.

- α je morfizmus: $\alpha((g,h)\cdot(g',h')) = \alpha((gg', hh')) = hh'$ a aj $\alpha((g,h))\cdot\alpha((g',h')) = h\cdot h'$
- α je injektívne: $(1, h) \mapsto h$
- α má jadro K: $(g,h) \in Ker(\alpha) \iff \alpha((g,h)) = 1 \iff Ker(\alpha) = G \times \{1\}$

Definícia 4.78. Nech $(S, \cdot)$ je pologrupa, $a, b \in S$. Definujeme *Greenove relácie* $\mathcal{L}, \mathcal{R}, \mathcal{J}$:

- $a\mathcal{L}b \iff \exists p, q \in S^1 : pa = b, qb = a$;
- $a\mathcal{R}b \iff \exists u, v \in S^1 : au = b, bv = a$;
- $a\mathcal{J}b \iff \exists p, q, u, v \in S^1 : pau = b, qbv = a$.

Ďalej definujeme *Greenove relácie* $\mathcal{H}, \mathcal{D}$:

- $a\mathcal{H}b \iff a\mathcal{L}b \wedge a\mathcal{R}b$;
- $a\mathcal{D}b \iff \exists c \in S : a\mathcal{L}c \wedge c\mathcal{R}b \iff \exists c' \in S : a\mathcal{R}c' \wedge c'\mathcal{L}b$; resp. $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$.

Kapitola 5: Okruhy

5.1 Základné pojmy a vlastnosti okruhov

Definícia 5.1. Množina R s operáciami $+, \cdot$ sa nazýva (komutatívny) *okruh*, ak platí:

1. $(R, +)$ je komutatívna grupa,
2. $(R, \cdot)$ je (komutatívny) monoid,
3. $\forall a, b, c \in R: \quad a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$ (distributivita).

Príklad 5.2. $(R, +, \cdot)$ pre $R = \mathbb{Z}_n, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je okruh.

Príklad 5.3. $(Mat_n(R), +, \cdot)$ pre $R = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ je okruh.

Poznámka. Neutrálny prvok komutatívnej grupy $(R, +)$ značíme 0 (nulový prvok, nula), neutrálny prvok monoidu $(R, \cdot)$ značíme 1 (jednotkový prvok, „jednička“).

Definícia 5.4. Okruh $(\{0\}, +, \cdot)$ je tzv. *triviálny*. Okruhy s viac ako 1 prvkom sú *netriviálne*.

Definícia 5.5. Netriviálny komutatívny okruh R je *obor integrity*, ak $\forall a, b \in R$ platí: $a, b \neq 0 \implies a \cdot b \neq 0$. (T. j. práve keď $(R^*, \cdot)$ je grupoid.)

Prvky $a, b \in R^*$ také, že $a \cdot b = 0$ sa nazývajú *delitelia nuly*.

Lemma 5.6. *Netriviálny komutatívny okruh R je obor integrity, práve keď pre každé $a \in R^*$, $b, c \in R$ platí: $ab = ac \implies b = c$ (zákon o krátení).*

Dôkaz. „$\implies$“: $0 = ab - ac = a(b - c)$. V obore integrity $xy = 0 \iff x = 0 \vee y = 0$. Keďže $a \in R^*$, musí $b - c = 0$, t. j. $b = c$.

„$\impliedby$“: Nech R je netriviálny komut. okruh, kde platí zákon o krátení. Ak by existovali $a, b \in R^*$ také, že $ab = 0$, tak potom $ab = 0 = a \cdot 0$, teda zo zákona o krátení $b = 0$ ※. □

Definícia 5.7. Netriviálny komutatívny okruh R je *teleso*, ak každý jeho nenulový prvok je invertibilný, t. j. keď $\forall a \in R$ platí: $a \neq 0 \implies a^{-1} \in R$. (T. j. práve keď $(R^*, \cdot)$ je grupa.)

Invertibilné prvky monoidu $(R, \cdot)$ sa nazývajú *jednotky* (angl. units) okruhu R.

Príklad 5.8. Najmenšie teleso je $(\{0, 1\}, +, \cdot)$ (analógia triviálneho okruhu / OI).

Veta 5.9. *Každé teleso je obor integrity.*

Dôkaz. Nech R je teleso, $a, b \in R^*$. Potom $b = a^{-1} \cdot (a \cdot b)$, takže $a \cdot b \neq 0$. □

Veta 5.10. *Každý konečný obor integrity je teleso.*

Dôkaz. Nech R je konečný obor integrity, $a \in R^*$. Keďže $(R^*, \cdot)$ je grupoid, predpis $r_a(x) = ax$ definuje zobrazenie $r_a \colon R^* \to R^*$. Z Lemmy 5.6 plynie, že r_a je injektívne. Keďže R^* je konečná množina, je r_a aj surjektívne. Potom $\exists x \in R^* \colon r_a(x) = 1$, t. j. $ax = 1$ a keďže R je komutatívny okruh, $x = a^{-1}$. □

Poznámka. Hierarchia: telesá $\subset$ obory integrity $\subset$ komutatívne okruhy $\subset$ okruhy.
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ $\quad$ $\mathbb{Z}$ (nie je teleso) $\quad$ $\mathbb{Z}_n$ (nie je vždy OI)

Veta 5.11. *$\mathbb{Z}_p$ je teleso, práve keď p je prvočíslo.*

Dôkaz. Ak je p prvočíslo, tak $\mathbb{Z}_p$ je teleso podľa 3.12 a 5.9. Ak $n := p$ nie je prvočíslo, tak $n = ab$, kde $1 < a, b < n$. Keďže $[a][b] = [ab] = [0]$, tak $[a], [b]$ sú delitelia nuly v $\mathbb{Z}_n$. □

5.2 Podokruhy

Definícia 5.12. Nech $(R, +, \cdot)$ je okruh, H neprázdna podmnožina množiny R. Potom H je *podokruh* okruhu R; píšeme $H \leq R$; ak platí:

1. $0_R, 1_R \in H$;
2. ak $a, b \in H$, tak $a + b, ab \in H$;
3. ak $a \in H$, tak $-a \in H$.

Dôsledok 5.13. *$(H, +, \cdot)$ je okruh. Ak $(R, +, \cdot)$ je komutatívny (resp. OI), tak aj $(H, +, \cdot)$ je komutatívny (resp. OI).*

Dôsledok 5.14. *$(\{0\}, +, \cdot)$ je tzv. triviálny podokruh okruhu R a je to najmenší podokruh. R je sám sebe podokruhom a to najväčším. Iné podokruhy ako tieto dva nazývame vlastné.*

Dôsledok 5.15. *Vlastnosť „byť podokruhom“ je tranzitívna.*

Príklad 5.16. $(\mathbb{Z}, +, \cdot) \leq (\mathbb{Q}, +, \cdot) \leq (\mathbb{R}, +, \cdot) \leq (\mathbb{C}, +, \cdot)$.

Príklad 5.17. Nech $n \in \mathbb{Z}$ a $\alpha = \sqrt{-n}$. Potom $\mathbb{Z}[\alpha] = \{a + \alpha b \mid a, b \in \mathbb{Z}\}$ je podokruh okruhu $\mathbb{C}$ [2, II.3.3].

Príklad 5.18. Voľbou $\alpha = \sqrt{-1} = i$ dostávame okruh *Gaussových čísel* $\mathbb{G} := \mathbb{Z}[i]$.

Lemma 5.19. *$\mathbb{G}$ je obor integrity. Existuje v ňom delenie so zvyškom. Aj keď podiel a zvyšok nie je určený jednoznačne, existencia postačuje na dôkaz NSD a Bezoutovej rovnosti pre Gaussove čísla* [2, II.3.4].

Príklad 5.20. $(\mathbb{Z}, +, \cdot) \leq (\mathbb{G}, +, \cdot) \leq (\mathbb{C}, +, \cdot)$.

Príklad 5.21. Okruh *kvaterniónov* tvorí množina $\mathbb{K} = \{[a + ib + jc + kd \mid a, b, c, d \in \mathbb{R}\}$ s operáciami sčítania po zložkách a násobením definovaným pomocou nasledovnej tabuľky:

×	**1**	***i***	***j***	***k***
1	1	*i*	*j*	*k*
i	*i*	−1	*k*	−*j*
j	*j*	−*k*	−1	*i*
k	*k*	*j*	−*i*	−1

5.3 Homomorfizmy okruhov

Definícia 5.22. Zobrazenie $\varphi\colon R_1 \to R_2$ je (homo)morfizmus okruhu $(R_1, +, \cdot)$ do okruhu $(R_2, \oplus, \circ)$, ak pre všetky $a, b \in R_1$ platí: $\varphi(a + b) = \varphi(a) \oplus \varphi(b)$ a $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$. Ďalej musí platiť ešte tretie pravidlo, že $\varphi(1_{R_1}) = 1_{R_2}$.

Poznámka. Ide vlastne o hom. grupy $(R_1, +)$ do $(R_2, \oplus)$ a hom. monoidu $(R_1, \cdot)$ do $(R_2, \circ)$.

Definícia 5.23. Bijektívny homomorfizmus nazývame *izomorfizmus*. Ak existuje izomorfizmus medzi okruhmi R_1, R_2, nazývame ich izomorfné a píšeme $R_1 \cong R_2$.

Príklad 5.24. Ak $H \leq R$, tak $H \to R$ je homomorfizmus okruhov. Obzvlášť $R \cong R$.

Príklad 5.25. $\varphi\colon \mathbb{Z} \to \mathbb{Z}_n$, kde $a \mapsto [a]_n$ je homomorfizmus okruhov.

Príklad 5.26. $\varphi\colon \mathbb{C} \to \mathbb{C}$, kde $a \mapsto \overline{a}$ (komplexne združené číslo, 7.47) je hom. okruhov.

Definícia 5.27. Nech $f\colon (R_1, +, \cdot) \to (R_2, \oplus, \circ)$ je homomorfizmus okruhov. Potom *jadro* homomorfizmu f je množina $Ker(f) = \{a \in R_1 \mid f(a) = 0\}$.

Lemma 5.28. *Homomorfizmus* $f\colon (R_1, +, \cdot) \to (R_2, \oplus, \circ)$ *je prostý* $\iff Ker(f) = \{0\}$.

Dôkaz. Keďže sa jedná o hom. grupy $(R_1, +)$ do $(R_2, \oplus)$, tvrdenie plynie z Lemmy 4.67. □

Veta 5.29. *Prostý homomorfizmus* φ *z okruhu* R *do telesa* T *existuje, len ak* R *je OI.*

Dôkaz. Okruh R musí byť netriviálny. Ak by bol R triviálny, tak $0_R \mapsto 1_T$ (z definície), ale potom $\varphi(0 + 0) = \varphi(0) = 1$ a to sa nerovná $\varphi(0) + \varphi(0) = 1 + 1 = 0$.

Ďalej, okruh R musí byť komutatívny. Pri zobrazení do telesa musí platiť $\varphi(a) \cdot \varphi(b) = \varphi(b) \cdot \varphi(a)$, teda $\varphi(ab) = \varphi(ba)$, teda v pôvodnom okruhu $ab = ba$.

Nakoniec, R nesmie mať deliteľov nuly. Ak by $ab = 0$, tak $\varphi(a) \cdot \varphi(b) = \varphi(0) = 0$.

R je teda netriviálny, komutatívny a bez deliteľov nuly, teda je to OI. □

5.4 Súčiny okruhov a podielové telesá

Definícia 5.30. Nech $(R_1, \oplus, \odot)$, $(R_2, \boxplus, \boxdot)$ sú okruhy. Na množine $R_1 \times R_2$ definujeme operácie $+, \cdot$ vzťahmi $[a,b]+[c,d] = [a \oplus c, b \boxplus d]$, $[a,b]\cdot[c,d] = [a \odot c, b \boxdot d]$ (po zložkách).

Dôsledok 5.31. *$(R_1 \times R_2, +, \cdot)$ je okruh.*

Dôkaz. $(R_1 \times R_2, +)$ je komutatívna grupa; nulovým prvkom je $[0_{R_1}, 0_{R_2}]$, opačným k prvku $[a,b]$ je $[-a,-b]$. $(R_1 \times R_2, +)$ je monoid; jednotkovým prvkom je $[1_{R_1}, 1_{R_2}]$. □

Lemma 5.32. *Ak R_1, R_2 sú netriviálne, tak $(R_1 \times R_2, +, \cdot)$ nikdy nie je obor integrity.*

Dôkaz. $[1,0]\cdot[0,1] = [0,0]$. □

Lemma 5.33. *Nech R je OI. Definujme na množine $R \times R^*$ reláciu $\equiv$ vzťahom $[a,b] \equiv [c,d] \iff ad = bc$ pre všetky $a, c \in R,\ b, d \in R^*$. Potom $\equiv$ je relácia ekvivalencie.*

Dôkaz. Uvažujme $a, c, e \in R,\ b, d, f \in R^*$.

- *Reflexivita*: $[a,b] \equiv [a,b]$, lebo $ab = ba$.
- *Symetria*: ak $[a,b] \equiv [c,d]$, tak $ad = bc$ a z kom. násobenia $cb = da$, teda $[c,d] \equiv [a,b]$.
- *Tranzitivita*: ak $[a,b] \equiv [c,d]$ a $[c,d] \equiv [e,f]$, tak $ad = bc$ a $cf = de$. Po vynásobení f dostávame $adf = bcf = bde$. Z toho $adf - bde = 0$, teda $d(af - be) = 0$. Keďže $d \in R^*$ a R je OI, tak $af - be = 0$, t. j. $af = be$, t. j. $[a,b] \equiv [e,f]$.

(V dôkaze tranzitivity nesmieme násobiť inverziou d^{-1} – tá nemusí vôbec existovať!) □

Dôsledok 5.34. *Relácia ekvivalencie $\equiv$ určuje rozklad na množine $R \times R^*$. Množinu $R \times R^*/\equiv$ tried tohto rozkladu označíme $Q(R)$. Triedu obsahujúcu prvok $[a,b]$ označíme $\frac{a}{b}$. Potom platí: $\frac{a}{b} = \frac{c}{d} \iff ad = bc$ (krížové pravidlo pre zlomky).*

Veta 5.35. *Nech R je OI. Definujme súčet a súčin dvoch prvkov $\frac{a}{b}, \frac{c}{d} \in Q(R)$ vzťahmi $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ (súčet a súčin zlomkov). Potom $+, \cdot$ sú operácie na $Q(R)$ a $(Q(R), +, \cdot)$ je teleso, tzv. podielové.*

Dôkaz. Korektnosť ($+, \cdot$ sú operácie): ak $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$, kde $a, a', c, c' \in R$, $b, b', d, d' \in R^*$, tak musí $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{a'}{b'} \cdot \frac{c'}{d'}$. To platí [2, II.4.15].

$(Q(R), +)$ je kom. grupa: platí kom., asoc., nulový prvok je $\frac{0}{1}$ a opačný k $\frac{a}{b}$ je $\frac{-a}{b}$.

$(Q(R), \cdot)$ je kom. monoid: platí kom., asoc., jednotkový prvok je $\frac{1}{1}$. Platí distributivita.

$(Q(R), +, \cdot)$ je teda kom. okruh. Je aj netriviálny, lebo ak by $\frac{0}{1} = \frac{1}{1}$, tak by $0 = 1$.

$(Q(R), +, \cdot)$ je teleso: ak $\frac{a}{b} \neq \frac{0}{1}$, tak $a \neq 0$, teda $\frac{b}{a} \in Q(R)$. Platí $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$, teda $(\frac{a}{b})^{-1} = \frac{b}{a}$, takže každý nenulový prvok má inverziu. □

Veta 5.36. *Nech R je OI. Potom zobrazenie $k\colon R \to Q(R)$ definované $k(a) = \frac{a}{1}$ pre ľubovoľné $a \in R$ je injektívny homomorfizmus okruhov. Ak je R teleso, tak k je izomorfizmus.*

Dôkaz. Nech $a, b \in R$. Homomorfizmus: $k(a) + k(b) = \frac{a}{1} + \frac{b}{1} = \frac{1a+1b}{1} = \frac{a+b}{1} = k(a+b)$, ďalej $k(a) \cdot k(b) = \frac{a}{1} \cdot \frac{b}{1} = \frac{a \cdot b}{1} = \frac{ab}{1} = k(ab)$ a tiež $k(1) = \frac{1}{1}$ (jednička ide na jedničku).

Injektívny: ak $k(a) = k(b)$, tak $\frac{a}{1} = \frac{b}{1}$, t. j. $a = a \cdot 1 = 1 \cdot b = b$.

Nech R je teleso, $a \in R, b \in R^*$. Surjektívny: $k(ab^{-1}) = \frac{ab^{-1}}{1} = \frac{a}{b}$, lebo $ab^{-1}b = 1a$. Potom k je izomorfizmus. □

Definícia 5.37. $\mathbb{Q} := Q(\mathbb{Z})$.

Veta 5.38 (O univerzalite)**.** *Nech R je OI, T je teleso a $\alpha\colon R \to T$ prostý homomorfizmus. Potom existuje jediný homomorfizmus $\beta\colon Q(R) \to T$ taký, že $\beta \circ k = \alpha$* [2, II.4.19].

5.5 Charakteristiky okruhov

Definícia 5.39. Buď R okruh. Najmenšie $n \in \mathbb{N}$ také, že $n1 = 0$ nazývame *charakteristika* okruhu R. Ak také n neexistuje (t. j. $k1 \neq 0$ pre každé $k \in \mathbb{N}$), tak $n := 0$.

Poznámka. Ak char. n okruhu R nie je 0, tak n je rád 1 v grupe $(R, +)$ [2, II.2.2].

Príklad 5.40. Charakteristiky okruhov $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sú 0. Charakteristika $\mathbb{Z}_n$ je n.

Lemma 5.41. *Charakteristika oboru integrity je buď* 0 *alebo prvočíslo.*

Dôkaz. Ak by $n = kl$, kde $k, l \geq 2$, tak $(1 + \cdots + 1)(1 + \cdots + 1)$ (postupne k-krát a l-krát) má deliteľov nuly. □

5.6 Cvičenia

1. Sú okruhy $(\mathbb{Z}, +, \cdot) \times (\mathbb{Z}, +, \cdot)$ a $(\mathbb{Z}[i], +, \cdot)$ izomorfné?
2. Sú okruhy $(\mathbb{R}, +, \cdot) \times (\mathbb{R}, +, \cdot)$ a $(\mathbb{C}, +, \cdot)$ izomorfné?
3. Sú okruhy $(\mathbb{Q}[\sqrt{5}], +, \cdot)$ a $(\mathbb{Q}[\sqrt{3}], +, \cdot)$ izomorfné?
4. Existuje injektívny homomorfizmus zo $(\mathbb{Z}, +, \cdot)$ do nejakého telesa?
5. Existuje injektívny homomorfizmus zo $(\mathbb{Z}_2, +, \cdot) \times (\mathbb{Z}_3, +, \cdot)$ do nejakého telesa?
6. Čo sa stane, ak definujeme ekvivalenciu z Lemmy 5.33 na okruhu $R = \mathbb{Z}_4$?
7. Pre okruh $(R, +, \cdot)$ definujeme okruh $(R[i], +, \cdot)$ vzťahmi: $R[i] = R \times R$, $(a, b) + (c, d) = (a + c, b + d)$, $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$. Prvky môžete písať v tvare $a + bi$. Aký tvar majú prvky $Q(\mathbb{Z}[i])$?
8. Dokážte, že okruhy $((Q(\mathbb{Z})[i], +, \cdot))$ a $(Q(\mathbb{Z}[i]), +, \cdot)$ sú izomorfné.

5.7 Návody k riešeniu cvičení

1. Nie sú. $\mathbb{G} = (\mathbb{Z}[i], +, \cdot)$ je OI, ale $(\mathbb{Z}, +, \cdot) \times (\mathbb{Z}, +, \cdot)$ nie je OI. Napr. $(1, 0) \cdot (0, 1) = (0, 0)$.
2. Nie sú. $\mathbb{C}$ je teleso a teda OI, ale $(\mathbb{R}, +, \cdot) \times (\mathbb{R}, +, \cdot)$ nie je OI. Napr. $(1, 0) \cdot (0, 1) = (0, 0)$.
3. Nie, pretože $\sqrt{5} \notin \mathbb{Q}[\sqrt{3}]$.

   Nech p je prvočíslo, $\sqrt{p} \notin \mathbb{Q}$. Ak by $\sqrt{p} \in \mathbb{Q}$, potom $\sqrt{p} = a/b$, kde $a, b \in \mathbb{N}$ a $\mathrm{NSD}(a, b) = 1$ (v opačnom prípade ich môžeme krátiť). Úpravou dostaneme rovnosť $p \cdot b^2 = a^2$, teda $p \mid a^2$.

   $\sqrt{p} \notin \mathbb{N}$, teda $p \mid a$ (to je vidieť z toho, že a má jednoznačný rozklad na prvočísla a a^2 má ten istý rozklad, ale každý člen je umocnený na druhú) a môžeme písať $a = px, x \in \mathbb{N}$. Potom ale $p \cdot b^2 = p^2 \cdot x^2$ a $b^2 = p \cdot x^2$, teda $p \mid b^2$ a preto tiež $p \mid b$. Našli sme deliteľa a, b rôzneho od 1, čo je spor.

Predpokladajme, že $\sqrt{5} \in \mathbb{Q}[\sqrt{3}]$, teda $\sqrt{5} = a+b\sqrt{3}$, kde $a, b \in \mathbb{Q}, b \neq 0$ (to môžeme predpokladať, lebo $\sqrt{5} \notin \mathbb{Q}$). Umocníme obe strany výrazu: $5 = a^2 + 2ab\sqrt{3} + 3b^2$.

Predpokladajme, že $a \neq 0$, potom úpravou rovnosti dostaneme výraz $\sqrt{3} = (5 - a^2 - 3b^2)/2ab \in \mathbb{Q}$ – spor. Nech teda $a = 0$, potom $\sqrt{5} = b\sqrt{3}$, teda $\sqrt{5}\sqrt{3} = 3b \in \mathbb{Q}$. Dokážeme, že $\sqrt{15} \notin \mathbb{Q}$. Použijeme rovnaký postup ako pri dôkaze, že $\sqrt{p} \notin \mathbb{Q}$.

4. $f\colon (\mathbb{Z}, +, \cdot) \to (\mathbb{R}, +, \cdot)$, kde $f(a) = a$.

5. Nie. V $(\mathbb{Z}_2 \times \mathbb{Z}_3)$ existujú delitelia nuly, napr. $(0,1) \cdot (1,0) = (0,0)$. Táto vlastnosť sa zachová aj v obraze (delitelia nuly ostávajú pri ľubovoľnom rozšírení daného obrazu), ktorý potom nemôže byť podgrupou telesa.

6. Potom $\equiv$ nie je reláciou ekvivalencie. Napr. v $\mathbb{Z}_4$ je $[2,2] \equiv [0,2]$, lebo $2 \cdot 2 = 0 \cdot 2$ a $[0,2] \equiv [0,1]$, lebo $0 \cdot 2 = 0 \cdot 1$, ale $[2,2] \equiv [0,1]$ by dalo $2 \cdot 1 = 0 \cdot 2$, teda $2 = 0$ ※ . Potom $\equiv$ nie je ekvivalencia (a teda neurčuje rozklad na množine, ako je požadované).

   Toto platí pre všetky $\mathbb{Z}_n$, kde n je zložené, lebo potom R nie je OI.

7. Gaussove racionálne čísla $\mathbb{Q}[i] := Q(\mathbb{Z}[i]) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

8. $f([a,b],[c,d]) = [(ad + cbi), (bd)]$, teda $(a/b) + (ci/d) = (ad + cbi)/(bd)$.

Kapitola 6: Varenie čísel

Motivácia:

$\mathbb{N}_0$: Vieme $+, \cdot, \leq$. Nevieme odčítať.

$\mathbb{Z}$: Vieme $+, \cdot, \leq, -$. Nevieme deliť nenulovým prvkom.

$\mathbb{Q}$: Vieme $+, \cdot, \leq, -, \div$. Neexistujú konvergentné Cauchyovské postupnosti.

$\mathbb{R}$: Vieme $+, \cdot, \leq, -, \div$. Nevieme odmocňovať ($\mathbb{R}$ nie sú algebraicky uzavrené).

$\mathbb{C}$: Vieme $+, \cdot, \leq, -, \div, \sqrt{}$.

Definícia 6.1. Konštrukcia $\mathbb{N}_0$ (Z-F teória množín): $0 := \emptyset$, $n + 1 := n \cup \{n\}$. Potom $\mathbb{N}_0$ je najmenšia množina obsahujúca $\emptyset$ a uzavretá na operáciu $'$ definovanú $n' = n \cup \{n\}$.

Príklad 6.2. $1 = 0 + 1 = \emptyset \cup \{\emptyset\} = \{\emptyset\}$, $2 = 1 + 1 = 1 \cup \{1\} = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}$, ...

Definícia 6.3. Operácie na $\mathbb{N}_0$:

- $m < n \iff m \subsetneq n$;
- $m \leq n \iff m < n \vee m = n$;
- $m + 0 = m, \qquad m + 1 = m', \qquad m + n = (m + 1) + (n - 1)$;

- $m \cdot 0 = 0, \qquad m \cdot 1 = m, \qquad m \cdot n = m \cdot (n-1) + m.$

Definícia 6.4. Konštrukcia $\mathbb{Z}$: na $\mathbb{N}_0 \times \mathbb{N}_0$ definujeme reláciu $\sim$ tak, že $(a,b) \sim (c,d) \iff a+d = b+c$. Potom $\sim$ je ekvivalencia. Celé čísla definujeme ako triedy ekvivalencie $[(a,b)]_\sim$ usporiadaných dvojíc (a,b) dvoch prirodzených čísel. Namiesto $[(a,b)]_\sim$ píšeme $a-b$.

Definícia 6.5. Operácie na $\mathbb{Z}$:

- $(a-b)+(c-d) = (a+c)-(b+d)$;
- $(a-b)\cdot(c-d) = (ac+bd)-(ad+bc)$;
- $a-b \leq c-d \iff a+d \leq b+c$.

Definícia 6.6. Konštrukcia $\mathbb{Q}$: pozri Definíciu 5.37.

Definícia 6.7. Operácie na $\mathbb{Q}$: $\frac{a}{b} \leq \frac{c}{d} \iff ad \leq bc$, pre $a,b,c,d > 0$.

Kapitola 7: Polynómy

7.1 Základné pojmy

Definícia 7.1. Analytická definícia polynómu ako zobrazenia nevyhovuje v algebre. Polynóm tu budeme uvažovať ako postupnosť koeficientov.

Nech R je okruh. *Polynóm nad okruhom* R je nekonečná postupnosť $f = (f_0, f_1, \dots)$, kde $f_i \in R$ pre $i \in \mathbb{N}_0$ také, že množina $\{i \in \mathbb{N}_0 \mid f_i \neq 0\}$ je konečná.

Poznámka. Prvky $f_0, f_1, \dots, f_i, \dots$ nazývame *koeficienty* polynómu.

Nulový polynóm („nula“) je nekonečná postupnosť $0 = (0,0,0,\dots,0,\dots)$.

Jednotkový polynóm („jednička“) je nekonečná postupnosť $1 = (1,0,0,\dots,0,\dots)$.

Konštantný polynóm je nekonečná postupnosť $a = (a,0,0,\dots,0,\dots)$, kde $a \in R$.

Definícia 7.2. $R[x]$ je množina všetkých polynómov nad daným okruhom R.

Veta 7.3. *Buď R okruh. Na $R[x]$ definujeme operácie $+,\cdot$ vzťahmi*

$$(f+g)_i = f_i + g_i, \qquad (f\cdot g)_i = \sum_{k=0}^{i} f_k \cdot g_{i-k}.$$

Potom $(R[x],+,\cdot)$ je okruh („okruh polynómov“) nad R. Ak je R kom., tak aj $R[x]$ je kom.

Dôkaz. Korektnosť: $+,\cdot$ sú operácie na $R[x]$, lebo $f+g, fg$ sú polynómy. Totiž ak $f,g \in R[x]$, tak $f+g, fg \in R[x]$, lebo množ. $\{i \in \mathbb{N}_0 \mid f_i + g_i \neq 0\}, \{i \in \mathbb{N}_0 \mid \sum_{k=0}^{i} f_k g_{i-k} \neq 0\}$ sú konečné.

Keďže sčítanie polynómov je definované po zložkách, $(R[x],+)$ je kom. grupa. Platí kom., asociativita, nulovým prvkom je nulový polynóm a opačným k f je $(-f_0, -f_1, \dots)$.

Ďalej $(R[x],\cdot)$ je monoid. Jedničkou je jednotkový polynóm (asociativitu netreba na skúšku, dôkaz je v [2, II.5.2]). Overíme tiež distributivitu.

Ak je R kom., tak $\forall f,g \in R[x]$: $(fg)_i = \cdots = (gf)_i$ (z definície). □

Poznámka. Hovoríme „polynóm f nad okruhom R“ alebo značíme $f \in R[x]$.

Definícia 7.4. Nech f je nenulový polynóm nad okruhom R. Najväčšie $n \in \mathbb{N}_0$ také, že $f_n \neq 0$ sa nazýva *stupeň polynómu* f a značí sa $\mathrm{st}(f)$. Stupeň nulového polynómu je $-\infty$.

Koeficient f_n sa potom nazýva *vedúci koeficient* polynómu f.

Veta 7.5. *Ak je R OI, tak aj $R[x]$ je OI.*

Dôkaz. Ak je R OI, tak $R[x]$ je kom. okruh podľa Vety 7.3. Ten je netriviálny, lebo obsahuje aspoň dva rôzne prvky: nulu a jedničku. Ak by existovali nenulové polynómy $f, g \in R[x]$ také, že $fg = 0$, tak by súčin ich vedúcich koeficientov bol 0, ale R je OI ※ . □

Lemma 7.6. *O generujúcich polynómoch platia nasledovné tvrdenia:*

- *Konštantné polynómy sú nulové polynómy alebo polynómy stupňa 0 a sú tvaru $a := (a, 0, 0, 0, \ldots, 0, \ldots)$, kde $a \in R$;*
- *Lineárne polynómy sú polynómy stupňa 1 a sú tvaru $x := (0, 1, 0, 0, \ldots, 0, \ldots)$;*
- *Kvadratické polynómy sú polynómy stupňa 2 a sú tvaru $x^2 := (0, 0, 1, 0, \ldots, 0, \ldots)$;*
- *Kubické polynómy sú polynómy stupňa 3 a sú tvaru $x^3 := (0, 0, 0, 1, 0, \ldots, 0, \ldots)$.*

Veta 7.7. *Nech R je okruh a $f \in (R[x], +, \cdot)$ je polynóm stupňa n. Potom $f = f_n \cdot x^n + \cdots + f_1 \cdot x + f_0$. (Jednotlivé koeficienty f_i chápeme ako konštantné polynómy.)*

Dôkaz. Indukciou z definície násobenia polynómov dostaneme $(x^k)_k = 1$ a $(x^k)_i = 0$ pre $i \neq k$. Preto $(f_n \cdot x^n + \cdots + f_1 \cdot x + f_0)_i = \sum_{k=0}^{n} (f_k \cdot x^k)_i = \sum_{k=0}^{n} f_k \cdot (x^k)_i = f_i$. □

Veta 7.8. *Nech f, g sú polynómy nad okruhom R. Potom:*

1. *$st(f + g) \leq max\{st(f), st(g)\}$;*
2. *$st(f \cdot g) \leq st(f) + st(g)$. Ak R je OI, tak táto nerovnosť prejde v rovnosť.*

Dôkaz. Nerovnosti plynú okamžite z definície súčtu a súčinu polynómov (7.3).

Ak R je OI a $\mathrm{st}(f) = n \geq 0$, $\mathrm{st}(g) = m \geq 0$, potom $(fg)_{n+m} = f_n g_m \neq 0$, takže $\mathrm{st}(fg) = \mathrm{st}(f) + \mathrm{st}(g)$. Ak $f = 0$ (alebo $g = 0$), tak $fg = 0$, preto $\mathrm{st}(fg) = \mathrm{st}(f) + \mathrm{st}(g) = -\infty$. □

Lemma 7.9. *Nech R je OI a $f \in R[x]$. Potom f je jednotka okruhu $R[x]$, práve keď f je konštantný polynóm, ktorý je jednotkou okruhu R.*

Dôkaz. „$\Longleftarrow$“: Zrejmé. „$\Longrightarrow$“: Nech R je OI a f jednotka v $R[x]$. Potom $0 = \mathrm{st}(1) = \mathrm{st}(f \cdot f^{-1}) = \mathrm{st}(f) + \mathrm{st}(f^{-1})$, takže $\mathrm{st}(f) = \mathrm{st}(f^{-1}) = 0$. Teda f je konštantný polynóm, ktorého inverzný prvok je f^{-1}, teda f je jednotkou v R. □

Dôsledok 7.10. *Okruh $R[x]$ nemôže byť nikdy teleso, lebo polynóm x nemá inverziu.*

Príklad 7.11. Ak R nie je OI, tak môžu existovať nekonštantné jednotky v $R[x]$. Napr. v $\mathbb{Z}_4[x]$ máme $f = g = 2x + 1$ a potom $f^{-1} = g$ a $fg = 1$.

Definícia 7.12. Nech R je teleso. Polynómy $f, g \in R[x]$ sa nazývajú *asociované*, ak existuje nenulové $c \in R$ také, že $f = cg$.

7.2 Deliteľnosť polynómov

Veta 7.13. *Nech R je OI, $f, g \in R[x]$ a vedúci koeficient polynómu g je jednotkou v R. Potom existuje práve jedna dvojica polynómov $q, r \in R[x]$ taká, že $st(r) < st(g)$ a $f = qg + r$.*

Dôkaz. Existencia q, r: Ak $\mathrm{st}(f) < \mathrm{st}(g)$, tak $r := f$ a $q := 0$. Nech $\mathrm{st}(f) \geq \mathrm{st}(g)$. Veďme indukciu k $n = \mathrm{st}(f)$:

- Báza: Ak $n = 0$, tak $m = \mathrm{st}(g) = 0$. Z Lemmy 7.9 vyplýva, že g má inverziu v $R[x]$. Potom $r := 0$ a $q := g^{-1}f$.
- IP: Ľubovoľný polynóm stupňa menšieho než n je možné deliť so zvyškom.
- IK: Nech $n \geq m \geq 0$. Polynóm $p = (f_n g_m^{-1})x^{n-m}g$ má vedúci koeficient f_n a stupeň n. Potom polynóm $h = f - p$ má stupeň menší než n a z IP plynie, že existuje dvojica polynómov $q, r \in R[x]$ taká, že $\mathrm{st}(r) < \mathrm{st}(g)$ a $h = qg + r$, Teda $f = p + qg + r = g(f_n g_m^{-1} x^{n-m} + q) + r$, takže f je možné deliť so zvyškom polynómom g.

Jednoznačnosť q, r: Ak R nie je OI, tak q, r nemusia byť určené jednoznačne. Nech pre $f, g \in R[x]$, $g \neq 0$ platí: $f = qg + r = q'g + r'$, kde $\mathrm{st}(r)$, $\mathrm{st}(r') < \mathrm{st}(g)$. Teda $r - r' = g(q' - q)$, takže z Vety 7.8 plynie, že $\mathrm{st}(g) > \mathrm{st}(r - r') = \mathrm{st}(g) + \mathrm{st}(q' - q)$. Potom ale $\mathrm{st}(q' - q) = -\infty$, t. j. $q' - q = 0$. Potom aj $r - r' = 0$, takže $q = q'$ a $r = r'$. □

Príklad 7.14. Podiel a zvyšok nie sú určené jednoznačne, ak vedúci koeficient polynómu g nie je jednotkou daného okruhu. Napr. nad okruhom $\mathbb{Z}_4$ platí: $2x + 1 = 1 \cdot (2x + 1) + 0 = 2x \cdot (2x + 1) + 1$.

Veta 7.15. *Nech R je teleso, f, g sú nenulové polynómy v $R[x]$. Potom existuje $NSD(f, g)$.*

Dôkaz. Z Vety 7.13 plynie, že $\exists n \in \mathbb{N}_0$ a polynómy $q_1, \ldots, q_{n+1}, r_1, \ldots, r_{n+1} \in R[x]$ také, že $\mathrm{st}(g) > \mathrm{st}(r_1) > \mathrm{st}(r_n) \leq 0$ a platí:

$$\begin{aligned} f &= q_1 \cdot g + r_1, \\ g &= q_2 \cdot r_1 + r_2, \\ r_1 &= q_3 \cdot r_2 + r_3, \\ &\ldots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n, \\ r_{n-1} &= q_{n+1} \cdot r_n \end{aligned}$$

Potom $r_n = (a, b)$ ako vo Vete 2.18. □

Veta 7.16 (Bezoutova rovnosť)**.** *Nech R je teleso, f, g sú nenulové polynómy v $R[x]$. Potom existujú polynómy $u, v \in R[x]$ také, že $fu + gv = (f, g)$.*

Dôkaz. Analogicky ako Veta 2.20. □

Definícia 7.17. Polynóm sa nazýva *normovaný*, ak je jeho vedúci koeficient rovný 1.

Lemma 7.18. *Pre ľubovoľné dva polynómy existuje ich normovaný NSD* [2, II.5.22].

7.3 Rozklad a ireducibilita polynómov

Definícia 7.19. Nech R je komutatívny okruh. Prvok $a \in R$ je *ireducibilným prvkom* R, ak je nenulový, nie je jednotka a nemá vlastných deliteľov v R.

Poznámka. Toto odpovedá takým konštantným polynómom, ktoré sú „prvočísla“.

Definícia 7.20. Nech R je okruh. Polynóm $f \in R[x]$ je *ireducibilný nad* R, ak je nekonštantný a nedá sa rozložiť na súčin dvoch nekonštantných polynómov.

Veta 7.21. *Nech R je teleso. Polynóm $f \in R[x]$ je ireducibilným prvkom $R[x]$, práve keď je nekonštantný a nedá sa rozložiť na súčin dvoch nekonštantných polynómov.*

Dôkaz. „$\Longleftarrow$“: Z definície. „$\Longrightarrow$“: Ak je f ireducibilný, tak je nekonštantný a nemá vlastných deliteľov. Nech g je vlastným deliteľom polynómu f. Potom g nie je konštantný a ani nie je asociovaný s f a platí $f = gh$. Polynóm h je nekonštantný, lebo inak by bol g asociovaný s f. Teda polynóm, ktorý má vlastných deliteľov je možné rozložiť na súčin nekonštantných polynómov. □

Poznámka. Veta hovorí, že ak R je teleso, tak polynómy ireducibilné nad R splývajú s ireducibilnými prvkami okruhu $R[x]$.

Príklad 7.22. Polynóm 2 je ireducibilným prvkom okruhu $\mathbb{Z}[x]$. Polynóm $2x$ je ireducibilný nad $\mathbb{Z}$, ale nie je ireducibilným prvkom $\mathbb{Z}[x]$, lebo 2 je jeho vlastný deliteľ.

Príklad 7.23. Ak je R OI, tak každý lineárny polynóm je ireducibilný nad R.

Príklad 7.24. Každý kvadratický polynóm so záporným diskriminantom je ireduc. nad $\mathbb{R}$.

Lemma 7.25. *Nech R je teleso, h, f nesúdeliteľné polynómy nad R a $g \in R[x]$ polynóm taký, že $h \mid fg$. Potom $h \mid g$.*

Dôkaz. Keďže $(h, f) = 1$, tak podľa Vety 7.16 $\exists u, v \in R[x]$: $hu + fv = 1$. Teda $ghu + gfv = g$. Keďže $h \mid h$ a $h \mid fg$, tak $h \mid g$. □

Veta 7.26. *Nech R je teleso, $f \in R[x]$ je nenulový polynóm. Potom existujú $k \in \mathbb{N}_0$, ireducibilné normované polynómy $p_1, \ldots, p_k \in R[x]$ a prvok $a \in R$ tak, že $f = ap_1 \ldots p_k$. Tento rozklad je jednoznačný (až na poradie činiteľov).*

Dôkaz. Existencia: indukciou podľa $n = \mathrm{st}(f)$. Báza: $n = 0 \implies$ rozklad na prvočísla. IP: každý nenulový polynóm nad R stupňa menšieho než $n \geq 0$ má rozklad nášho tvaru. IK: nech $f \in R[x]$ je polynóm stupňa n. Ak je f konštantný alebo ireducibilný, potom tvrdenie zrejme platí. Nech je teda f nekonštantný reducibilný v R. Potom $f = gh$ je súčinom dvoch nekonštantných polynómov $g, h \in R[x]$. Podľa Vety 7.8 je $\mathrm{st}(g), \mathrm{st}(h) < \mathrm{st}(f)$. Podľa IP je možné rozložiť g, h na súčin ireducibilných polynómov. Teda aj f.

Jednoznačnosť: nech $f = ap_1 \ldots p_k = bq_1 \ldots q_l$ sú dva rozklady polynómu f na súčin ireducibilných normovaných polynómov. Postupujeme indukciou podľa k. Báza: $f = a = b$. IP: rozklad je jednoznačný pre $k \geq 0$. IK: $p_k \mid bq_1 \ldots q_l$. Ak by sa p_k nerovnalo žiadnemu z $q_1, \ldots, q_l$, bolo by $(p_k, q_1) = \cdots = (p_k, q_l) = 1$, čo je spor s Lemmou 7.25. Teda musí existovať $i = 1, \ldots, l$ také, že $p_k = q_i$. Teda $ap_1 \ldots p_{k-1} = bq_1 \ldots q_{i-1}q_{i+1}q_l$ sú rozklady polynómu stupňa menšieho než n na súčin ireducibilných polynómov. Z IP je tento rozklad jednoznačný, takže aj rozklad f je jednoznačný. □

7.4 Korene polynómov

Definícia 7.27. Nech R je okruh, $f = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$, $c \in R$. Potom prvok $f(c) := a_n c^n + \cdots + a_1 c + a_0$ nazývame *hodnota polynómu* f v prvku c.

Veta 7.28. *Nech R je komutatívny okruh, $f, g \in R[x]$, $c \in R$. Potom $(f+g)(c) = f(c) + g(c)$ a tiež $(f \cdot g)(c) = f(c) \cdot g(c)$.*

Dôkaz. $+$ zrejmé. Ak $f = a_n x^n + \cdots + a_1 x + a_0$, $g = b_m x^m + \cdots + b_1 x + b_0$, tak $(f \cdot g)(c) = \sum_{i=0}^{n+m} \sum_{k=0}^{i} a_k \cdot b_{i-k} \cdot c_i$ a aj $f(c) \cdot g(c) = \sum_{i=0}^{n} a_i c^i \cdot \sum_{j=0}^{m} b_j c^j = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i c^i b_j c^j = \sum_{i=0}^{n} \sum_{j=0}^{m} a_i b_j c^{i+j}$. □

Definícia 7.29. Nech R je okruh, $f \in R[x]$, $c \in R$. Potom c je *koreň polynómu* f, ak $f(c) = 0$.

Veta 7.30. *Nech R je komutatívny okruh, $f \in R[x]$, $c \in R$. Potom c je koreňom polynómu f, práve keď $(x-c) \mid f$.*

Dôkaz. „$\Longrightarrow$“: Podľa Vety 7.13 $\exists q, r \in R[x]$: $f = q(x-c) + r$, kde r je konštantný. Potom $r = f - q(x-c)$ a $r = r(c) = f(c) - q(c)(c-c) = 0$. Teda zvyšok je nulový a $(x-c) \mid f$.

„$\Longleftarrow$“: Ak $(x-c) \mid f$, tak $f = q(x-c) + 0$. Potom $f(c) = q(c)(c-c) = 0$. □

Definícia 7.31. Nech R je komutatívny okruh, $f \in R[x]$, $c \in R$ koreňom f. Potom číslo $k \in \mathbb{N}$ je *násobnosť* koreňa c, ak $(x-c)^k \mid f$ a $(x-c)^{k+1} \nmid f$.

Korene násobnosti 1 nazývame *jednoduché*. (0-násobný koreň by nebol koreňom.)

Veta 7.32. *Nech R je OI. Potom nenulový polynóm $f \in R[x]$ má najviac $n = st(f)$ koreňov, ak počítame aj násobné.*

Dôkaz. Indukciou. Báza pre $n = 0$ je triviálna, pretože konštantný polynóm nemá korene. IP: polynóm stupňa n má najviac n koreňov. IK: nech f je polynóm stupňa $n+1$. Ak existuje $c \in R$, ktoré je koreňom f, potom podľa Vety 7.30 existuje $q \in R[x]$ taký, že $f = q(x-c)$, pričom q je stupňa n. Podľa IP má teda q najviac n koreňov. Každý koreň polynómu q je aj koreňom f a každé $d \neq c$, ktoré je koreňom f je aj koreňom q. Potom f má najviac $n+1$ koreňov. □

Definícia 7.33. Nech R je okruh, $f \in R[x]$. Definujme zobrazenie $\gamma(f)\colon R \to R$ vzťahom $\gamma(f)(c) = f(c)$ pre každé $c \in R$. Zobrazenie $\gamma(f)$ nazývame *polynomická funkcia* určená polynómom f.

Lemma 7.34. *Nech R je nekonečný OI, $f, g \in R[x]$. Potom $\gamma(f) = \gamma(g)$, práve keď $f = g$.*

Dôkaz. „$\Longleftarrow$“: Zrejmé. „$\Longrightarrow$“: Ak $\gamma(f) = \gamma(g)$, tak $\forall c \in R$: $(f-g)(c) = f(c) - g(c) = 0$. Preto polynóm $f - g$ má ∞ mnoho koreňov v R. Z Vety 7.32: $f - g = 0$, teda $f = g$. □

Poznámka. Na polynómy nad $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sa môžeme dívať ako na funkcie. Neplatí to ale napr. nad $\mathbb{Z}_2$, kde rôzne polynómy x, x^2 určujú rovnakú polynomickú funkciu.

Definícia 7.35. Nech $f = a_n x^n + \cdots + a_1 x + a_0$ je polynóm nad okruhom R. Polynóm $f' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$ nad okruhom R sa nazýva *derivácia* polynómu f.

Pre $k \in \mathbb{N}$ značíme k-tu deriváciu polynómu ako $f^{(k)}$.

Veta 7.36. *Nech R je okruh, $f, g \in R[x]$. Potom:*

$$(f+g)' = f' + g'; \tag{1}$$
$$(fg)' = f'g + fg' \tag{2}$$

Dôkaz. (1): $((f+g)')_i = (i+1)\cdot(f+g)_{i+1} = (i+1)\cdot f_{i+1} + (i+1)\cdot g_{i+1} = (f')_i + (g')_i$.

(2): Najprv v špeciálnom prípade $f = ax^n$, $g = bx^m$. Potom $(fg)' = (abx^{n+m})' = (n+m)abx^{n+m-1}$ a tiež $f'g + fg' = nax^{n-1}bx^m + ax^n mbx^{m-1}$.

IP: (2) platí pre polynómy f, g aj f, h. Potom $(f(g+h))' = (fg+fh)' = (fg)'+(fh)' = f'g+fg'+f'h+fh' = f'(g+h)+f(g+h)'$, takže (2) platí aj pre polynómy $f, g+h$. Keďže každý polynóm je súčet polynómov tvaru ax^n, vzťah (2) platí pre ľubovoľné polynómy. □

Veta 7.37. *Nech R je komutatívny okruh, $k \in \mathbb{N}$. Ak je $c \in R$ k-násobným koreňom polynómu $f \in R[x]$, tak je c koreňom polynómov $f', \ldots, f^{(k-1)}$.*

Dôkaz. Indukciou podľa k z 7.36 (2) dostávame: $((x-c)^k)' = k(x-c)^{k-1}$. Teda ak $f = g(x-c)^k$, tak $f' = g'(x-c)^k + gk(x-c)^{k-1} = (x-c)^{k-1}(kg + g'(x-c))$. □

Veta 7.38. *Nech R je teleso charakteristiky 0, $k \in \mathbb{N}$. Potom $c \in R$ je k-násobným koreňom polynómu $f \in R[x]$, práve keď je c koreňom $f, f', \ldots, f^{(k-1)}$ a nie je koreňom $f^{(k)}$.*

S každou deriváciou sa násobnosť koreňa zníži o 1.

Dôkaz. „ $\Longrightarrow$ “: Nech c je k-násobným koreňom polynómu f. Potom $f = g(x-c)^k$, kde $x - c \nmid g$. Z dôkazu Vety 7.37 vieme, že $f' = (x-c)^{k-1}(kg + g'(x-c))$. Ak by $(x-c)^k \mid f'$, tak by $(x-c) \mid kg$, teda by $h(x-c) = kg = (k1)g$. Pritom $k1 \neq 0$, lebo R má charakteristiku 0. Potom by $g = h(x-c)(k1)^{-1}$, takže by $(x-c) \mid g$ ※ . Tým sme dokázali, že c je $(k-1)$-násobným koreňom f'.

„ $\Longleftarrow$ “: Nech je c koreňom $f, f', \ldots, f^{(k-1)}$ a nie je koreňom $f^{(k)}$. Nech n je násobnosť koreňa c polynómu f. Potom $(x-c)$ delí $f, f', \ldots, f^{(n-1)}$ a nedelí $f^{(n)}$. Položme $n = k$. □

7.5 Polynómy nad telesom komplexných čísel

Definícia 7.39. Teleso R sa nazýva *algebraicky uzavrené*, ak každý nekonštantný polynóm z $R[x]$ má koreň v R.

Veta 7.40 (Základná veta algebry)**.** *Teleso $\mathbb{C}$ je algebraicky uzavrené* [2, II.7.2].

Veta 7.41. *Žiadne konečné teleso nie je algebraicky uzavrené.*

Dôkaz. Nech $R = \{a_1, \ldots, a_n\}$ je konečné teleso ($|R| \geq 2$). Potom polynóm $(x-a_1)\cdot\cdots\cdot(x-a_n)+1$ nemá koreň v R. □

Veta 7.42. *Teleso je algebraicky uzavrené $\Longleftrightarrow$ ireduc. polynómy v ňom sú práve lineárne.*

Dôsledok 7.43. *Polynóm $f \in \mathbb{C}[x]$ je ireducibilný v $\mathbb{C}$, práve keď je lineárny.*

Dôkaz. „ $\Longleftarrow$ “: Z 7.23 . „ $\Longrightarrow$ “: Ak je f ireducibilný v $\mathbb{C}$, tak je nekonštantný, takže podľa 7.40 má koreň $c \in \mathbb{C}$. Potom $(x-c) \mid f$ a keďže f je ireducibilný, musí byť lineárny. □

Veta 7.44 (Vzťah ireducibility a koreňov). *Nad telesom R pre polynóm $f \in R[x]$ stupňa n platí:*

- *Pre $n = 1$: f je ireducibilný $\implies$ f má koreň.*
- *Pre $n = 2, 3$: f je ireducibilný $\iff$ f nemá koreň.*
- *Pre $n \geq 4$: f je ireducibilný $\implies$ f nemá koreň.*

Veta 7.45 (Jednoznačnosť vyjadrenia). *Nech R je algebraicky uzavreté teleso charakteristiky 0, $a \in R^*$ je jeho nenulový prvok, $f \in R[x]$ je nenulový polynóm, $c_1, \ldots, c_p$ sú jeho jednoduché korene, $d_1, \ldots, d_q$ sú jeho násobné korene násobností $k_1, \ldots, k_q \geq 2$, pričom všetky korene sú po dvoch rôzne. Potom každý f je možné vyjadriť ako*

$$f = a(x - c_1) \ldots (x - c_p)(x - d_1)^{k_1} \ldots (x - d_q)^{k_q},$$

kde $st(f) = p + k_1 + \cdots + k_q = n$.

Dôsledok 7.46. *Polynóm $f/NSD(f, f')$ má rovnaké korene ako f, všetky jednoduché.*

Dôkaz. $f' = a(x - d_1)^{k_1 - 1} \ldots (x - d_q)^{k_q - 1}(x - l_1)^{e_1} \ldots (x - l_r)^{e_r}$, kde $e_1, \ldots, e_r \geq 1$. Ďalej $\mathrm{NSD}(f, f') = a(x - d_1)^{k_1 - 1} \ldots (x - d_q)^{k_q - 1}$. □

7.6 Polynómy nad telesom reálnych čísel

Definícia 7.47. Nech $c = c_1 + ic_2$ je komplexné číslo, $c_1, c_2 \in \mathbb{R}$. Potom číslo *komplexne združené* k c je $\overline{c} = c_1 - ic_2$.

Lemma 7.48. *Nech $c, e \in \mathbb{C}$. Potom $\overline{c + e} = \overline{c} + \overline{e}$ a tiež $\overline{c \cdot e} = \overline{c} \cdot \overline{e}$.*

Veta 7.49. *Ak je $c \in \mathbb{C}$ koreňom polynómu $f \in \mathbb{R}[x]$, tak aj $\overline{c}$ je koreňom tohto polynómu.*

Dôkaz. Nech $f(x) = \sum_{i=0}^{n} a_i x^i$ a $f(c) = 0$. Potom $f(\overline{c}) = \sum_{i=0}^{n} a_i \overline{c}^i = \sum_{i=0}^{n} a_i \overline{c^i} = \sum_{i=0}^{n} \overline{a_i c^i} = \overline{\sum_{i=0}^{n} a_i c^i} = \overline{0} = 0$. □

Veta 7.50. *Ireducibilné polynómy v $\mathbb{R}[x]$ sú práve lineárne polynómy a kvadratické polynómy so záporným diskriminantom.*

Dôkaz. „$\Longleftarrow$“: Každý lineárny polynóm je zrejme ireducibilný. Takisto kvadratický so záporným diskriminantom, lebo nemá reálne korene.

„$\Longrightarrow$“: Ak je f ireducibilný v $\mathbb{R}$, tak podľa Základnej vety algebry má koreň $c \in \mathbb{C}$. Ak $c \in \mathbb{R}$, tak $(x - c) \mid f$, takže f musí byť lineárny. Ak $c \notin \mathbb{R}$, tak z Vety 7.49 plynie, že polynóm $g = a(x - c)(x - \overline{c}) \in \mathbb{R}[x]$, kde $a \in \mathbb{R}^*$ delí f, t. j. že $f = a(x - c)(x - \overline{c})g$ je kvadratický polynóm so záporným diskriminantom. To, že skutočne $g \in \mathbb{R}[x]$ dokazuje vzťah: $f = hg$, $f = \overline{f} = \overline{hg} = \overline{h}\,\overline{g} = h\overline{g}$, teda $g = \overline{g}$. □

Veta 7.51 (Hornerova schéma). *Nech $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{R}[x]$, kde $n \geq 2$ a $a_n \neq 0$. Nech c je kandidát na koreň.*

Nech p je predošlé políčko tabuľky. Potom $a = bq + r$, resp.

$$a_n x^n + \cdots + a_1 x + a_0 = (b_{n-1} x^{n-1} + \cdots + b_1 x + b_0)(x - c) + f(cp + a_0),$$

kde $b_{n-1} = a_n, b_{n-2} = cb_{n-1} + a_{n-1}, \ldots, b_0 = cb_1 + a_1, f(c) = cb_0 + a_0$.

Poznámka. Pri hľadaní koreňov Hornerovou metódou potrebujeme minimum operácií.

	a_n	a_{n-1}	a_{n-2}	$\dots$	a_i	$\dots$
c	a_n	$ca_n + a_{n-1}$	$c(ca_n + a_{n-1}) + a_{n-2}$	$\dots$	$cp + a_i$	$\dots$

7.7 Polynómy nad okruhmi racionálnych a celých čísel

7.7.1 Primitívne polynómy, obsah

Definícia 7.52. Polynóm $f \in \mathbb{Z}[x]$ je *primitívny*, ak NSD jeho koeficientov je 1.

Lemma 7.53 (Gaussova)**.** *Súčin dvoch primitívnych polynómov je primitívny polynóm.*

Dôkaz. Nech $g = b_m x^m + \dots + b_0$, $h = c_n x^n + \dots + c_0$ sú dva primitívne polynómy, $b_m, c_n \neq 0$, $m, n \in \mathbb{N}$. Pre spor predpokladajme, že gh nie je primitívny. Potom existuje prvočíslo p, ktoré delí všetky koeficienty polynómu gh. Avšak, p nemôže deliť všetky koeficienty polynómov g, h, lebo g, h sú primitívne.

Nech teda i, j sú čo najmenšie celé čísla také, že koeficienty b_i, c_j nie sú deliteľné p. Potom koeficient polynómu gh na indexe $i + j$, teda $(gh)_{i+j}$ je tvaru

$$b_0 c_{i+j} + b_1 c_{i+j-1} + \dots + b_{i-1} c_{j+1} + b_i c_j + b_{i+1} c_{j-1} + \dots + b_{i+j-1} c_1 + b_{i+j} c_0.$$

Vieme, že p má deliť $b_0, \dots, b_{i-1}$ ale nie b_i; podobne p má deliť $c_0, \dots, c_{j-1}$ ale nie c_j. Potom keďže $p \nmid b_i$ a zároveň $p \nmid c_j$, tak $p \nmid b_i c_j$ ※ . □

Definícia 7.54. Nech $f \in \mathbb{Z}[x]$ je polynóm. Potom jeho *obsah* (angl. content) $c(f) \in \mathbb{Z}$ definujeme ako NSD jeho koeficientov.

Ak $f \in \mathbb{Q}[x]$, potom $\exists n \in \mathbb{N}$: $nf \in \mathbb{Z}[x]$. Potom $c(f) := \frac{c(nf)}{n} \in \mathbb{Q}$.

Poznámka. Primitívny polynóm je teda polynóm, ktorého obsah je 1.

Veta 7.55 (Jednoznačný rozklad na súčin obsahu a primitívneho polynómu)**.** *Nech $f \in \mathbb{Q}[x]$, $f \neq 0$. Potom existujú jednoznačné $c(f) \in \mathbb{Q}$, $p(f)$ primitívny tak, že $f = c(f)p(f)$.*

Daný $p(f)$ obvykle volíme s kladným vedúcim koeficientom, inak násobíme (-1).

Dôkaz. Existencia: Z Definície 7.54 obsahu. (Polynóm vynásobím NSN menovateľov zlomkov a vyjmem NSD nových koeficientov.)

Jednoznačnosť: Musíme ukázať, že ak primitívny polynóm $p(f)$ vynásobíme nejakým $\frac{p}{q}$, kde $p, q \in \mathbb{Z}$ sú nesúdeliteľné, tak dostaneme primitívny polynóm jedine vtedy, ak $\frac{p}{q} = \pm 1$. Nech teda $p(f) = a_n x^n + \dots + a_0$. Potom q delí všetky jeho koeficienty. Keďže $p(f)$ je primitívny, tak $q = \pm 1$. Potom $\frac{p}{\pm 1} \cdot$ prim. = prim., teda $p = \pm 1$. □

Príklad 7.56. $-10x^2 + 5x + 5 = (-5) \cdot (2x^2 - x - 1)$.

Príklad 7.57. $\frac{1}{3}x^5 + \frac{7}{2}x^2 + 2x + 1 = \frac{1}{6}(2x^5 + 21x^2 + 12x + 6)$.

7.7.2 Ireducibilita

Tvrdenie 7.58. *Všetky lineárne polynómy v $\mathbb{Z}[x]$ sú ireducibilné nad $\mathbb{Z}$.*

Tvrdenie 7.59. *Všetky primitívne polynómy v $\mathbb{Z}[x]$ sú ireducibilné nad $\mathbb{Z}$.*

Veta 7.60 (Gauss). *$f \in \mathbb{Z}[x]$ je ireducibilný nad $\mathbb{Z}$, práve keď je ireducibilný nad $\mathbb{Q}$.*

Dôkaz. „$\Longleftarrow$“: Zrejmé. „$\Longrightarrow$“: f je ireducibilný nad $\mathbb{Z}$. Dá sa zapísať jedine v tvare $f = c(f)p(f)$, kde $c(f) \in \mathbb{Z}$. Predpokladajme pre spor, že $f = gh$, kde g, h sú nekonštantné nad $\mathbb{Q}$. Teda $f = c(g)p(g)c(h)p(h) = c(g)c(h)p(g)p(h)$, kde $c(g)c(h) \in \mathbb{Z}$ a $p(g)p(h)$ je primitívny polynóm. □

Veta 7.61 (Eisensteinovo kritérium). *Nech $f = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ je polynóm stupňa $n > 0$. Ak existuje prvočíslo p také, že $p \mid a_0, \ldots, a_{n-1}$, $p \nmid a_n$ a $p^2 \nmid a_0$, tak f je ireducibilný nad $\mathbb{Z}$* [2, II.8.8].

Tvrdenie 7.62. *Nech $f \in \mathbb{Z}[x]$. Potom $f(x)$ je ireducibilný, práve keď $f(x + a)$ je ireducibilný. (Posun o konštantu $a \in \mathbb{Z}$.)*

Tvrdenie 7.63. *$\forall n \in \mathbb{N}$: existuje polynóm $f \in \mathbb{Z}_p[x]$ stupňa n ireducibilný nad $\mathbb{Z}$.*

7.7.3 Hľadanie koreňov

Veta 7.64 (*Rational root theorem*). *Nech $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, kde $a_n \neq 0$. Nech $\frac{r}{s} \in \mathbb{Q}$ je taký koreň polynómu f, že $(r, s) = 1$. Potom $r \mid a_0$ a $s \mid a_n$.*

Dôkaz. Keďže $\frac{r}{s}$ je koreň, $f\left(\frac{r}{s}\right) = a_n \left(\frac{r}{s}\right)^n + \cdots + a_0 = 0$. Vynásobením s^n dostaneme: $a_n r^n + a_{n-1} r^{n-1} s + \cdots + a_0 s^n = 0$. Modulo r máme: $a_0 s^n \equiv 0 \pmod{r}$. Keďže $(r, s) = 1$, dostávame $r \mid a_0$. Analogicky modulo s dostávame $s \mid a_n$. □

Dôsledok 7.65. *Nech $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, kde $a_n \neq 0$.*

- *Ak je $r \in \mathbb{Z}$ koreňom polynómu f, tak $r \mid a_0$. (Dôkaz: $s = 1$.)*
- *Ak je f normovaný, tak každý jeho racionálny koreň je celé číslo. (Dôkaz: $1 \mid a_n = 1$.)*

Veta 7.66. *Nech $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, kde $a_n \neq 0$. Nech $\frac{r}{s} \in \mathbb{Q}$ je taký koreň polynómu f, že $(r, s) = 1$. Potom $\forall z \in \mathbb{Z}$: $(r - sz) \mid f(z)$.*

Dôkaz. Polynóm f, ktorý má koreň $\frac{r}{s}$ sa dá zapísať v tvare $f = (x - \frac{r}{s})g$. Vynásobením s dostaneme: $sf = (sx - r)g$. Podľa Vety 7.55: $sc(f)p(f) = c(g)(sx - r)p(g)$. Potom $sc(f) \in \mathbb{Z}$, $p(f)$ je primitívny a tiež $(sx - r)p(g)$ je primitívny, lebo je súčinom dvoch primitívnych, takže $c(g) \in \mathbb{Z}$. Teda $(sx - r) \in \mathbb{Z}[x]$, preto môžeme dosadiť z za x do vzťahu $sf = (sx - r)g$ vyššie. Dostaneme $gf(z) = (sz - r)g(r)$, kde $(sz - r)$ delí $f(z)$. □

7.8 Cvičenia

1. Určite všetky korene polynómu $x^9 + 2x^8 + x^7 + 2x^6 + 5x^5 - 3x^3 + 2x^2 + 3x + 1$ nad $(\mathbb{Z}_7, +, \cdot)$ (skrátene nepíšeme napr. $[2]_7 x^8$).
2. Určite všetky korene polynómu $x^3 - 2x^2 + 4x + 1$ nad $(\mathbb{Z}_7, +, \cdot)$.
3. Nájdite všetky ireducibilné polynómy nad $\mathbb{Z}_2$ stupňa najviac 4.
4. Určite všetky korene polynómu $12x^8 - 16x^7 - 25x^6 + 75x^5 - 72x^4 - 129x^3 + 75x^2 + 40x - 20$ nad $(\mathbb{Z}, +, \cdot)$ a nájdite jeho rozklad nad $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

5. Nájdite rozklad polynómu $x^6 + 6x^5 + 15x^4 + 20x^3 + 12x^2 - 4$ nad $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.
6. Nájdite NSD polynómov $f = x^6 + x^5 + 2x^4 - x^3 - x + 2, g = 2x^4 + x^3 + 4x^2 - x + 2$ nad $\mathbb{Z}_5$ a určite koeficienty v Bezoutovej rovnosti.
7. Nájdite NSD $f = x^4 + 1, g = x^3 + 1$ nad $\mathbb{R}$ a určite koeficienty v Bezoutovej rovnosti.
8. Dokážte, že polynóm $f = 3x^4 - 12x^3 + 16x^2 - 4x + 3$ je ireducibilný nad $\mathbb{Q}$.

7.9 Návody k riešeniu cvičení

1. $[1]_7, [4]_7, [5]_7, [5]_7, [5]_7, [6]_7$.
2. Je ireducibilný v $\mathbb{Z}_7$, takže tam nemá koreň.
3. Je ich 9: $x, x+1, x^2+x+1, x^3+x+1, x^3+x^2+1, x^4+x^3+x^2+x+1, x^4+x^3+1, x^4+x+1, x^4+x^2+1$.
4. $-1, 2, \frac{1}{2}, \frac{1}{2}, -\frac{2}{3}$.
   - Nad $\mathbb{Z}$: $(x+1)(x-2)(2x-1)(2x-1)(3x+2)(x^3+5)$
   - Nad $\mathbb{Q}$: $12(x+1)(x-2)(x-\frac{1}{2})(x-\frac{1}{2})(x+\frac{2}{3})(x^3+5)$
   - Nad $\mathbb{R}$: $12(x+1)(x-2)(x-\frac{1}{2})(x-\frac{1}{2})(x+\frac{2}{3})(x+\sqrt[3]{5})(x^2-x\sqrt[3]{5}+\sqrt[3]{25})$
   - Nad $\mathbb{C}$: $12(x+1)(x-2)(x-\frac{1}{2})(x-\frac{1}{2})(x+\frac{2}{3})(x+\sqrt[3]{5})(x\pm(\frac{1}{2}+\frac{\sqrt{3}}{2}i)\sqrt[3]{5})$
5. Odstránime racionálne korene: nemá. Odstránime násobné korene: $\mathrm{NSD}(f, f') = x^2+2x+2 = g$, $x_{1,2} = -1 \pm i$ sú dvojnásobné v f. Potom $f/(g \cdot g) = x^2+2x-1$, $x_{5,6} = -1 \pm \sqrt{2}$.
   - Nad $\mathbb{C}$: $(x+1+i)^2(x+1-i)^2(x+1+\sqrt{2})(x+1-\sqrt{2})$
   - Nad $\mathbb{R}$: $(x^2+2x+2)^2(x+1+\sqrt{2})(x+1-\sqrt{2})$
   - Nad $\mathbb{Q}$, $\mathbb{Z}$: $(x^2+2x+2)^2(x^2+2x-1)$
6. $(f, g) = x^2 + x - 3 = f(-x-1) + g(3x^3+2x^2+2x-3)$.
7. $(f, g) = 1 = f\frac{x^2+x+1}{2} + g\frac{x^3+x^2+x-1}{-2}$.
8. Taylorov rozvoj v 1:

	3	−12	16	−4	3
1	3	−9	7	3	6
1	3	−6	1	4	
1	3	−3	−2		
1	3	0			
1	3				

   Potom $f = 3(x-1)^4 - 2(x-1)^2 + 4(x-1) + 6$ spĺňa Eisensteina pre $p = 2$.

Kapitola 8: Okruhy ďalej

8.1 Ideály

Definícia 8.1. Nech R je okruh. Neprázdna podmnožina $I \subseteq R$ sa nazýva *ideál* v okruhu R, ak platí:

1. ak $a, b \in I$, tak $a + b \in I$;
2. ak $a \in I$, $r \in R$ tak $a \cdot r, r \cdot a \in I$.

Poznámka. Množiny $\{0\}, R$ sú tzv. *nevlastné* ideály v ľubovoľnom okruhu R. Iné ideály ako tieto dva nazývame *vlastné*.

Lemma 8.2. *Nech I je ideál okruhu R. Potom I je podgrupa komutatívnej grupy $(R, +)$.*

Dôkaz. Ideál je z definície uzavrený na sčítanie. Ďalej $I \neq \emptyset$, takže existuje $a \in I$. Potom $0 = a \cdot 0 \in I$. Tiež $-a = a \cdot (-1) \in I$. □

Lemma 8.3. *Nech I je ideál okruhu R. Potom $1 \in I$, práve keď $I = R$.*

Dôkaz. Ak $1 \in I$, tak $a = a \cdot 1 \in I$ pre ľubovoľné $a \in R$. □

Veta 8.4. *Nech R je netriviálny komutatívny okruh. Potom R je teleso, práve keď R má len nevlastné ideály.*

Dôkaz. „$\Longrightarrow$“: Nech I je ideál telesa R. Ak $I \neq \{0\}$, tak existuje $0 \neq a \in I$, takže $1 = a \cdot a^{-1} \in I$. Podľa Lemmy 8.3 $I = R$.

„$\Longleftarrow$“: Nech R je je netriviálny komutatívny okruh, ktorý nemá vlastné ideály. Nech $0 \neq a \in R$. Potom tento prvok generuje celý ideál, t. j. $(a) = R$. Z Lemmy 8.3 plynie, že $(a) = R$, práve keď $1 \in (a)$, t. j. práve keď $a \mid 1$. To ale znamená, že a je jednotkou okruhu R. Teda R je teleso. □

8.2 Faktorové okruhy

Definícia 8.5. Nech I je ideál okruhu R.

Pripomeňme z 4.46: $G/H = \{aH \mid a \in G\}$, kde $aH = \{ah \mid h \in H\}$.

Definujme množinu $R/I = \{a + I \mid a \in R\}$, kde $a + I = \{a + i \mid i \in I\}$.

Veta 8.6. *Pripomeňme z 4.58: $(G/H, \cdot)$ je komutatívna grupa (tzv. faktorová).*

Na základe Lemmy 8.2 vieme zostrojiť komutatívnu faktorovú grupu $(R/I, +)$.

Veta 8.7. *Nech I je ideálom okruhu $(R, +, \cdot)$ a prvky $a + I, b + I$ patria do R/I. Potom predpis $(a+I)\cdot(b+I) = (ab)+I$ korektne definuje operáciu na množine R/I a $(R/I, +, \cdot)$ bude okruhom.*

Dôkaz. Korektnosť: Nech $a + I = c + I$, $b + I = d + I$. Chceme $(ab) + I = (cd) + I$. Ak $a + I = c + I$, tak $a - c \in I$ a tiež ak $b + I = d + I$, tak $b - d \in I$. Chceme $ab - cd \in I$. Vezmime $ab - cd = ab + ad - ad - cd = a(b - d) + d(a - c) \in I$. Potom $a(b - d) \in I$, $d(a - c) \in I$.

Asociativita: $((a + I) \cdot (b + I)) \cdot (c + I) = ((ab) + I) \cdot (c + I) = ((ab)c) + I = abc + I$ a tiež $(a + I) \cdot ((b + I) \cdot (c + I)) = \ldots$

Neutrálny prvok: $1 + I$, lebo $I \cdot (a + I) = (1 + I) \cdot (a + I) = a + I = (a + I) \cdot I$.

Distributivita: ... □

Definícia 8.8. $(R/I, +, \cdot)$ je *faktorový okruh* okruhu $(R, +, \cdot)$ podľa jeho ideálu I.

Veta 8.9. *Nech I je ideálom okruhu $(R, +, \cdot)$. Potom projekcia $p\colon R \to R/I$ definovaná vzťahom $a \mapsto a + I$ je surjektívny homomorfizmus okruhov. (Analógia 4.59.)*

Dôkaz. Z dôkazu Vety 4.59 plynie, že p je surjektívne zobrazenie, ktoré zachováva operáciu $+$. Ďalej $\forall a, b \in R$: $p(ab) = (ab) + I$ a tiež $p(a) \cdot p(b) = (a + I) \cdot (b + I) = (ab) + I$, takže p zachováva aj operáciu $\cdot$. Nakoniec $p(1) = 1 + I$ je jednotkovým prvkom okruhu R/I. □

Definícia 8.10. Nech R je teleso a $f = a_n x^n + \cdots + a_0 \in R[x]$ ireducibilný polynóm stupňa n. Ideál $(f) = \{gf \mid g \in R[x]\}$ je tzv. *hlavný ideál* generovaný polynómom f.

Veta 8.11. *V štruktúre $R[x]/(f) = \{g + (f) \mid g \in R[x]\}$ platí: $g + (f) = h + (f)$, práve keď $g - h \in (f)$.*

Dôkaz. $R[x]/(f) = \{g + (f) \mid g \in R[x]\} = \{g + (f) \mid \text{st } g < \text{st } f\}$. Teda $g - h \in (f)$, práve keď $f \mid (g - h)$, t. j. keď g, h dávajú po delení f rovnaký zvyšok. □

Dôsledok 8.12. *V štruktúre $R[x]/(f) = \{g + (f) \mid g \in R[x]\}$ sú rôzne zapísané prvky rôzne. (Vo všeobecnom $R/I = \{a + I \mid a \in R\}$ môžu rôzne a dať rovnaké $a + I$.)*

Veta 8.13. *Nech množina $R[x]/(f)$ je v „prirodzenej“ bijekcii α s $\mathbb{R}^n$, kde $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \mapsto (a_0, a_1, \ldots, a_{n-1})$, kde $n = st(f)$. Potom $(R[x]/(f), +, \cdot) \cong (\mathbb{R}^n, \oplus, \odot)$.*

Dôkaz. Aby sa bijekcia stala izomorfizmom, musíme ukázať, že operácie $\oplus, \odot$ sú v skutočnosti rovnaké ako $+, \cdot$ v okruhu $R[x]/(f)$.

Vezmime iný polynóm $b_0 + b_1 x + \cdots + b_{n-1} x^{n-1}$. Potom operácia $\oplus$ bude sčítanie po zložkách, t. j. $(a_0, a_1, \ldots, a_{n-1}) \oplus (b_0, b_1, \ldots, b_{n-1}) = (a_0 + b_0, a_1 + b_1, \ldots, a_{n-1} + b_{n-1})$.

Operácia $\odot$ bude definovaná: $(a_0, a_1, \ldots, a_{n-1}) \odot (b_0, b_1, \ldots, b_{n-1}) = (c_0, c_1, \ldots, c_{n-1})$, kde $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$ je zvyšok po delení polynómu $(a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}) \cdot (b_0 + b_1 x + \cdots + b_{n-1} x^{n-1})$ polynómom $\frac{1}{x}$. (Nemôžeme len tak násobiť, lebo by sme skočili do príliš vysokých stupňov.) □

Dôsledok 8.14. *Prvky telesa $R[x]/(f)$ a polynómy $r \in R[x]$ stupňa menšieho než n si vzájomne jednoznačne odpovedajú. Potom prvky telesa T môžeme stotožniť s odpovedajúcimi polynómami, t. j. položiť $R[x]/(f) = \{r \in R[x] \mid st(r) < n\}$.*

Príklad 8.15. Teleso $(\mathbb{R}[x]/(x^2+1), +, \cdot)$ je zložené z polynómov tvaru $a+bx$, kde $a, b \in \mathbb{R}$. Sčítanie je po zložkách: $(a + bx) + (c + dx) = (a + c) + (b + d)x$ a násobenie je definované takto: $(a + bx) \cdot (c + dx) = ac + adx + bcx + bdx^2 = \cancel{bd(x^2 + 1)} + ac - bd + (ad + bc)x$.

Ak polynóm $a + bx$ považujeme za komplexné číslo $a + bi$, potom dostávame elegantnú definíciu $(\mathbb{C}, +, \cdot) := (\mathbb{R}[x]/(x^2 + 1), +, \cdot)$.

Bijekcia $\alpha\colon (\mathbb{R}[x]/(x^2 + 1), +, \cdot) \cong (\mathbb{R}^2, +, \cdot)$ je tvaru $a + bx \mapsto (a, b)$.

Veta 8.16. *Zobrazenie $\iota\colon a \mapsto a + (f)$ je prostý morfizmus $(R, +, \cdot)$ do $(R[x]/(f), +, \cdot)$.*

Dôkaz. $\iota(a + b) = (a + b) + (f) = a + (f) + b + (f) = \iota(a) + \iota(b)$ a tiež $\iota(1) = 1 + (f)$. □

Dôsledok 8.17. *Nech $n = st(f)$ v $(R[x]/(f), +, \cdot)$. Polynóm $a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} \in R[x]$ je morfizmom ι zobrazený na polynóm $(a_0 + (f)) + (a_1 + (f))y + \cdots + (a_{n-1} + (f))y^{n-1}$, kde $y = ((f), 1 + (f), (f), \ldots)$. Dosadením $x + (f)$ do y dostaneme nulu, teda (f).*

Veta 8.18. *Nech $(R,+,\cdot)$ je teleso, $f,g \in R[x]$. Potom $g+(f) \neq 0=(f)$ má inverziu, práve keď $(g,f)=1$.*

Dôkaz. „$\Longrightarrow$“: Ak $g+(f)$ má inverziu, tak $\exists h \in R[x]\colon (g+(f))\cdot(h+(f))=1+(f)$, teda $gh+(f)=1+(f)$, teda $f \mid (gh-1)$, teda $fk=gh-1$. Keby $(g,f)=e>1$, tak by $e \mid f,g$, teda $e \mid 1$ ※. Teda $(g,f)=1$.

„$\Longleftarrow$“: Podľa Bezouta $\exists u,v \in R[x]\colon ug+vf=1$. Potom $(u+(f))\cdot(g+(f))=1-vf+(f)$, teda $ug+(f)=(f)$, kde $u+(f)$ je inverziou $g+(f)$. □

Dôsledok 8.19. *Nech $(R,+,\cdot)$ je teleso, $f \in R[x]$ je nekonštantný polynóm. Potom $(R[x]/(f),+,\cdot)$ je teleso, práve keď f je ireducibilný nad R.*

8.3 Rozšírenia telies

Definícia 8.20. Nech T je teleso a R podokruh v T taký, že $a^{-1} \in R$ pre každé nenulové $a \in R$. Potom R je *podteleso* v T, resp. T je *rozšírením* R.

Poznámka. Ak je R podtelesom v T, tak R je teleso.

Definícia 8.21. Nech T je rozšírením telesa R. Prvok $a \in T$ nazývame *algebraický* nad R, ak existuje nenulový polynóm $f \in R[x]$ tak, že a je jeho koreňom. V opačnom prípade hovoríme, že a je *transcendentný* nad R.

Poznámka. Ak explicitne neuvedieme dané telesá, pod pojmom algebraický myslíme prvok $a \in \mathbb{C}$ nad $\mathbb{Q}$.

Príklad 8.22. Je $a=\sqrt{2}+\sqrt{3}$ algebraické číslo? Áno, pretože $a^2=5+2\sqrt{6}$, teda $24=a^2-10a+25$, teda a je koreňom polynómu $x^2-10x+1 \in \mathbb{Q}[x]$.

Veta 8.23. *Nech $(T,+,\cdot)$ je rozšírením telesa $(R,+,\cdot)$, $a \in T$ je algebraický nad R. Potom a je koreňom práve jedného normovaného ireducibilného polynómu $f \in R[x]$. Navyše platí, že a je koreňom polynómu $h \in R[x]$, práve keď $f \mid h$.*

Dôkaz. Nech f je polynóm najmenšieho stupňa medzi všetkými normovanými polynómami z $R[x]$, ktoré majú a za koreň. Ukážeme, že f je ireducibilný nad R.

Existencia f: Zrejme f nie je konštantný – normovaný konštantný polynóm je 1 a ten nemá a za koreň. Nech $f=gh$, kde $g,h \in R[x]$. Potom $0=f(a)=g(a)h(a)$. Keďže T je teleso, tak buď $g(a)=0$, alebo $h(a)=0$. Teda buď $\mathrm{st}(g)=\mathrm{st}(f)$, alebo $\mathrm{st}(h)=\mathrm{st}(f)$, takže jeden z polynómov g,h je konštantný. (BUNV $\mathrm{st}(f)\leq\mathrm{st}(g)\wedge\ \mathrm{st}(f)\geq\mathrm{st}(g) \implies f=g$, potom h je konštantný.)

$f \mid h$: Nech $h \in R[x]$, $h(a)=0$. Potom $\exists q,r \in R[x]$ také, že $\mathrm{st}(r)<\mathrm{st}(f)$ a $h=qf+r$. Keďže $r(a)=h(a)-q(a)f(a)=0$ a f má najmenší stupeň medzi nenulovými polynómami s koreňom a, platí $r=0$. Teda $f \mid h$.

Jednoznačnosť f: Nech $f' \in R[x]$ je taký normovaný polynóm, že $\forall h \in R[x]$ platí: $h(a)=0 \iff f' \mid h$. Potom $f' \mid f$ a $f \mid f'$, takže $f=f'$, lebo oba sú normované. □

Definícia 8.24. Polynóm f z predošlej Vety sa nazýva *minimálny polynóm* prvku a nad R.

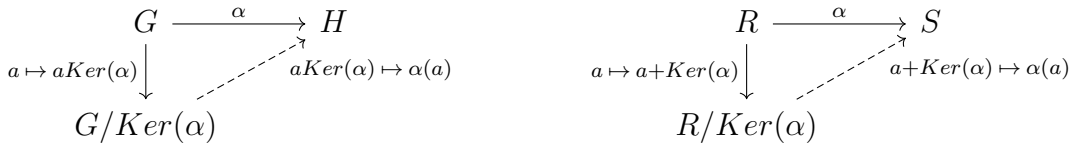
Príklad 8.25. Nad $\mathbb{C}$: $\epsilon n=\cos\frac{2\pi}{n}+i\cdot\sin\frac{2\pi}{n}$ je koreňom polynómu x^n-1 (hľadanie $\sqrt[n]{x}$).

Veta 8.26 (Delo II). *Pripomeňme Vetu Delo (4.68) pre grupy (multiplikatívna):*

- *Nech zobrazenie* $\alpha\colon (G,\cdot) \to (H,\cdot)$ *je surjektívny homomorfizmus grúp.*
- *Potom* $Ker(\alpha) = \{a \in G \mid \alpha(a) = 1\}$ *je normálna podgrupa v* $(G,\cdot)$.
- *Ďalej* $\beta\colon aKer(\alpha) \mapsto \alpha(a)$ *je surjektívny morfizmus* $(G,\cdot)/Ker(\alpha)$ *na* $(H,\cdot)$.

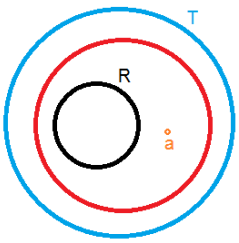
Pre okruhy je Veta Delo aditívna:

- *Nech zobrazenie* $\alpha\colon (R,+,\cdot) \to (S,+,\cdot)$ *je surjektívny homomorfizmus okruhov.*
- *Potom* $Ker(\alpha) = \{a \in R \mid \alpha(a) = 0\}$ *je podokruh v* $(R,+,\cdot)$.
- *Ďalej* $\beta\colon a + Ker(\alpha) \mapsto \alpha(a)$ *je surjektívny morfizmus* $(R,+,\cdot)/Ker(\alpha)$ *na* $(S,+,\cdot)$.



Definícia 8.27. Nech $(R,+,\cdot)$ je podtelesom telesa $(T,+,\cdot)$, $a \in T$. Potom:

- $R[a]$:= najmenší *podokruh* telesa T obsahujúci (= generovaný) množin(o)u $R \cup \{a\}$; $R[a] = \{f(a) \mid f \in R[x]\}$.
- $R(a)$:= najmenšie *podteleso* telesa T obsahujúce (= generované) množin(o)u $R \cup \{a\}$; $R(a) = \{\frac{f(a)}{g(a)} \mid f, g \in R[x], g \neq 0\}$.



Definícia 8.28. Rozšírenie T telesa R sa nazýva *jednoduché*, ak existuje prvok $a \in T$ algebraický nad R taký, že $T = R(a)$.

Veta 8.29. *Nech R je teleso. Potom T je jednoduché rozšírenie R, práve keď $T \cong R[x]/(f)$, kde $f \in R[x]$ je ireducibilný* [2, II.11.12].
Ďalej $1, a, \ldots, a^{n-1}$, kde $n \leq st(f)$ je báza T/R.

Dôkaz. „$\Longrightarrow$“: Použijeme Vetu Delo pre okruhy (8.26). Idea:

- Uvažujeme surjektívny homomorfizmus $\alpha\colon R[x] \to T = R[a]$, kde $g \mapsto g(a)$.

- $Ker(\alpha) = \{g \in R[x] \mid \alpha(g) = 0\} = (f)$, kde f je minimálny polynóm prvku a nad R.
- Ďalej $\beta\colon a + (f) \mapsto \alpha(a)$ je surjektívny morfizmus $R[x]/(f)$ na $R[a]$. Ukážeme, že sa jedná o izomorfizmus telies.

Nech T je jednoduché rozšírenie telesa R, ktoré vzniklo pridaním algebraického prvku $a \in T$. Existuje $f = k_n x^n + \cdots + k_1 x + k_0 \in R[x]$ tak, že $0 = f(a) = k_n a^n + \cdots + k_1 a + k_0$. Z toho $k_n a^n = -k_{n-1}a^{n-1} - \ldots - k_1 a - k_0$, teda

$$a^n = -\frac{k_{n-1}}{k_n}a^{n-1} - \ldots - \frac{k_1}{k_n}a - \frac{k_0}{k_n}. \qquad (*)$$

Potom a^n je lineárnou kombináciou báze $1, a, \ldots, a^{n-1}$. Nezávislosť báze: nech $a_0 + \cdots + k_{n-1}a^{n-1} = 0$, niektoré $k_i \neq 0$. Potom a je koreňom polynómu stupňa $\leq n-1$.

„ $\Longleftarrow$ “: Ak je $f \in R[x]$ ireducibilný nad R, tak z 8.14 vieme, že $T = R[x]/(f)$ je rozšírenie telesa R a že platí $T = R[a]$. Keďže $R[a] \subseteq R(a)$, tak $T = R(a)$, takže T je jednoduché rozšírenie telesa R. □

Dôsledok 8.30. *Ak T je rozšírenie telesa R a prvok $a \in T$ je algebraický nad R, tak $R(a) = R[a] \cong R[x]/(f)$.*

Príklad 8.31. Ak T je rozšírenie telesa R, tak $(T, +, \cdot)$ je vektorový priestor nad $(R, +, \cdot)$. $(T, +)$ je komutatívna grupa a násobenie vektoru skalárom je dané zobrazením $\cdot\colon R \times T \to T$, $(\alpha, a) \mapsto \alpha a$.

Ďalej $\dim T/R < \infty$, práve keď T/R je konečné rozšírenie (to neplatí napr. pri $\mathbb{C}/\mathbb{Q}$). Ak $T = R[\alpha]$, tak $1, \alpha, \ldots, \alpha^{n-1}$ je bázou vektorového priestoru T.

8.4 Lemmy o rozšírení telies

Lemma 1. *Ak T je rozšírením R a $f \in R[x]$ je ireducibilný nad R, tak f má v T koreň.*

Lemma 2. *Nech $(R, +, \cdot)$ je teleso, $f \in R[x]$ nekonštantný. Potom existuje rozšírenie T telesa R také, že f je ako polynóm nad T súčin lineárnych polynómov z $T[x]$.*

Dôkaz. Indukciou k $n = \mathrm{st}(f)$. Báza: $n = 1$, položíme $T = R$. IP: veta platí pre ľubovoľné R, f, kde $\mathrm{st}(f) < n$. IK: nech f je polynóm nad R stupňa n. Potom sa dá rozložiť na súčin normovaných ireducibilných polynómov, $f = ap_1 \ldots p_k$, kde $a \in R$. Potom existuje rozšírenie $W := R[x]/(p_k)$ telesa T také, že c je koreň f_k v W. Teda $\exists q \in W[x]\colon p_k = (x - c)q$. Potom $f = ap_1 \ldots p_{k-1}(x - c)q$.

Položme $g = aqp_1 \ldots p_{k-1}$. Keďže $\mathrm{st}(g) = n - 1$, podľa IP existuje rozšírenie T telesa W také, že $g = a(x - c_1)\ldots(x - c_{n-1})$ je súčin lineárnych polynómov nad T. Teda T je rozšírením telesa R a $f = a(x - c)(x - c_1)\ldots(x - c_{n-1})$ je súčin lineárnych poly. z $T[x]$. □

Definícia 8.32. Rozšírenie T/R je *algebraické*, ak každý $a \in T$ je algebraický nad R.

Definícia 8.33. Dimenziu rozšírenia T/R nazývame *stupeň* ($\dim T/R = \mathrm{st}\ T/R$).

Lemma 3. *Ak je rozšírenie T/R jednoduché, tak je konečné.*

Lemma 4. *Ak je rozšírenie T/R konečné, tak je algebraické.*

Dôkaz. Máme st $T/R = n \in \mathbb{N}$. Pre $a \in T$ sú $1, a, \ldots, a^n$ lineárne závislé. Existuje $b_0, \ldots, b_n \in R$ (niektoré nenulové) tak, že $b_0 + b_1 a + \cdots + b_n a^n = 0$, teda a je algebraické. □

Lemma 5. *Ak sú T/S, S/R konečné, tak T/R je konečné.*

Dôkaz. Máme st $T/S = m \in \mathbb{N}$, st $S/R = n \in \mathbb{N}$. Nech množina $\{b_1, \ldots, b_m \mid b_i \in S\}$ je bázou T/S a $\{a_1, \ldots, a_n \mid a_i \in R\}$ je bázou S/R. Potom množina $\{a_i b_j \mid i = 1, \ldots, m, j = 1, \ldots, n\}$ všetkých lineárnych kombinácií bázových prvkov $T/S, S/R$ je bázou T/R. □

Lemma 6. *Ak sú T/S, S/R algebraické, tak T/R je algebraické.*

Dôkaz. Nech $a \in T$ je algebraický. Potom $\exists 0 \neq f \in S[x]\colon f(a) = 0$. Nech $f = b_n x^n + \cdots + b_1 x + b_0$, kde $b_i \in S, b_n \neq 0$. Potom postupným pridávaním algebraických prvkov do štruktúry T/R dostávame $(\ldots((R(b_0))(b_1)\ldots(b_n)))(a)$. □

Lemma 7. *Ak $a, b \in T$ sú algebraické nad R, tak $a+b, a \cdot b, a^{-1}$ (pre $a \neq 0$) sú algebraické. Inak povedané, sčítanie a násobenie algebraických čísel dá algebraické číslo.*

Dôkaz. $R(a)/R$ je konečné podľa Lemmy 3. Takisto $(R(a))(b)/R(a)$. Ďalej $R(a, b)/R$ je konečné podľa Lemmy 5. Výsledok z Lemmy 4. □

Lemma 8. *Pre teleso R existuje také jeho rozšírenie T, kde má koreň ľubovoľný nekonštantný polynóm.*

Lemma 9. *Existuje algebraicky uzavrené rozšírenie T telesa R.*

Dôkaz. Existuje postupnosť $R = R_0 \subseteq R_1 \subseteq R_2 \subseteq \ldots$, kde R_{n+1} je také rozšírenie R, že každý nekonštantný polynóm nad R_n má koreň v R_{n+1}. Potom $T := \bigcup_{n=0}^{\infty}$. □

Lemma 10. *Existuje algebraicky uzavrené rozšírenie T telesa R, ktoré je algebraické.*

Dôkaz. Nech $\overline{R}$ je štruktúra všetkých algebraických prvkov nad R. Vezmime nejaký nekonštantný polynóm $f = a_n x^n + \cdots + a_0 \in \overline{R}[x]$ a nejaký prvok $a \in T$. Ak bude koreňom nejakého f, tak je algebraický nad R. To platí, lebo $R(a_0, \ldots, a_n, a)/T$ je algebraické. □

Príklad 8.34. Napr. $\mathbb{C}/\mathbb{R}$: k $\mathbb{R}$ sme pridali i a všetky prvky boli zrazu algebraické (každý polynóm mal koreň).

8.5 Konečné telesá

Nasledujúce vety sú z [2, II.12].

Veta 8.35. *Každé konečné teleso charakteristiky p je jednoduchým rozšírením telesa $\mathbb{Z}_p$.*

Veta 8.36. *Každé konečné teleso charakteristiky p má počet prvkov mocninu prvočísla p.*

Veta 8.37. *Nech p je prvočíslo, $n \in \mathbb{N}$. Potom existuje teleso R o p^n prvkoch.*

Dôsledok 8.38. *$R \cong \mathbb{Z}_p[x]/(f)$, kde $f \in \mathbb{Z}_p[x]$ je ireducibilné v $\mathbb{Z}_p$ a $st(f) = n$.*

Dôsledok 8.39. *V $\mathbb{Z}_p[x]$ existujú ireducibilné polynómy ľubovoľného stupňa.*

Veta 8.40. *Ľubovoľné dve konečné telesá o rovnakom počte prvkov sú izomorfné.*

8.6 Cvičenia

1. Nájdite inverziu prvku $g+(f)$ v okruhu $\mathbb{Q}[x]/(f)$, kde $g=x^3+1$.
2. Nech α je koreňom polynómu $f=x^3+2x^2+2$. Vyjadrite $\frac{1}{\alpha^2+\alpha+1}$ bez α v menovateli.
3. Nájdite minimálny polynóm čísla $\sqrt{2+\sqrt[3]{2}}$.
4. Nájdite minimálny polynóm čísla $\zeta(6)=\sqrt[6]{1}$.
5. Nájdite minimálny polynóm čísla $\zeta(p)=\sqrt[p]{1}$, kde p je prvočíslo.
6. Určite stupeň rozšírenia $\mathbb{C}(a)$ (= stupeň min. polynómu) nad $\mathbb{R}$.
7. Nájdite rozkladové teleso polynómu x^3-2 nad $\mathbb{Q}$ a určite jeho st. rozšírenia nad $\mathbb{Q}$.

8.7 Návody k riešeniu cvičení

1. $(f)=\{gf \mid g\in\mathbb{Q}[x]\}$. Potom $g+(f)=h+(f)$, práve keď g,h majú rovnaký zvyšok po delení f, t. j. keď $f \mid g-h$.

   $gh+(f)=(g+(f))(h+(f))=1+(f)$, teda $h=\frac{x^3+x^2+x-1}{-2}+(f)$.

2. Keďže f je ireducibilný nad $\mathbb{Q}$ (Eisensteinovo kritérium), tak $\mathbb{Q}[x]/(f)\cong$ telesu $\mathbb{Q}(\alpha)=\{a\alpha^2+b\alpha+c \mid a,b,c\in\mathbb{Q}\}$ ($\mathrm{st}(f)-1$). Izomorfizmus je daný $x+(x^3+2x^2+2)\mapsto\alpha$, kde $(x^2+x+1+(f))^{-1}\in\mathbb{Q}[x]/(f)$.

   Bezout: $1=f(\frac{1}{2}x+\frac{3}{4})+(x^2+x+1)(-\frac{1}{2}x^2-\frac{5}{4}x+\frac{1}{4})$.

   Potom $(x^2+x+1+(f))^{-1}=-\frac{2}{7}x^2-\frac{5}{7}x+\frac{1}{7}+(f)\in\mathbb{Q}[x]/(f)$.

   Teda $\frac{1}{\alpha^2+\alpha+1}=-\frac{2}{7}\alpha^2-\frac{5}{7}\alpha+\frac{1}{7}$.

3. $x=\sqrt{2+\sqrt[3]{2}}$, teda $(x^2-2)^3=2$, teda $x^6-6x^4+12x^2-10=0$. Tento polynóm má daný koreň a je ireducibilný nad $\mathbb{Q}$ (Eisenstein), teda je minimálny.

4. $x^6=1$, teda $x^6-1=0$, nie je ireduc. Potom $\zeta_6=e^{\frac{\pi}{3}i}=\frac{1}{2}+\frac{\sqrt{3}}{2}i$; $\overline{\zeta_6}=\frac{1}{2}-\frac{\sqrt{3}}{2}i$; $\zeta_6+\overline{\zeta_6}=1$. $(x-\zeta_6)(x-\overline{\zeta_6})=(x^2-x+\frac{1}{4}+\frac{3}{4})=x^2-x+1$.

5. $x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+x+1)$. Musíme dokázať, že polynóm $\Phi_p(x)=\frac{x^p-1}{x-1}=x^{p-1}+x^{p-2}+\cdots+x+1$ je ireducibilný nad $\mathbb{Q}[x]$ pre všetky prvočísla p.

   Platí, že $f(x)$ je ireducibilný, práve keď $f(x+k)$ je ireducibilný ($k\in\mathbb{Q}$).

$$\begin{aligned}\Phi_p(x+1)&=\frac{(x+1)^p-1}{x+1-1}\\&=\frac{(\sum_{k=0}^{p}\binom{p}{k}x^{p-k})-1}{x}\\&=\frac{\binom{p}{0}x^p+\binom{p}{1}x^{p-1}+\binom{p}{2}x^{p-2}+\ldots+\binom{p}{p-2}x^2+\binom{p}{p-1}x+\binom{p}{p}-1}{x}\\&=x^{p-1}+px^{p-2}+\binom{p}{2}x^{p-3}+\ldots+\binom{p}{p-2}x+p.\end{aligned}$$

Tento polynom spĺňa Eisensteinovo kritérium pre p.

Nazýva sa cyklotomický, delí $x^p - 1$ a jeho korene sú p-te odmocniny z 1.

Pre ľubovoľné ζ_n je stupeň min. polynómu $\varphi(n)$.

6. $\mathbb{C}$ má rozšírenie stupňa 2 nad $\mathbb{R}$; min. polynóm i je $x^2 - 1$.

7. $\mathbb{Q}[x]/(f) \cong \mathbb{Q}(\alpha)$, kde α je koreňom f, je rozkladové teleso, ktoré vznikne pridaním všetkých koreňov polynómu f. Korene $x^3 - 2$ sú $\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta_3, \sqrt[3]{2} \cdot \zeta_3^2$.

   Potom stupeň rozšírenia $\mathbb{Q}(a) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta_3, \sqrt[3]{2} \cdot \zeta_3^2) = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2} \cdot \zeta_3) = \mathbb{Q}(\sqrt[3]{2})(\zeta_3)$.

	1	0	0	-2
$\sqrt[3]{2}$	1	$\sqrt[3]{2}$	$\sqrt[3]{4}$	0

   $x^2 + \sqrt[3]{2}x + \sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$ má koreň $\sqrt[3]{2} \cdot \zeta_3$.

   $x^3 - 1 = (x-1)(x^2 + x + 1)$ je min. polynóm ζ_3 nad $\mathbb{Q}$.

Kapitola 9: Syntaktický monoid

9.1 Teória jazykov

Definícia 9.1. Nech A je neprázdna konečná množina (tzv. *abeceda*). Potom $A^* = \{(a_1, \ldots, a_n) \mid n \in \mathbb{N}_0, a_1, \ldots, a_n \in A\}$ je množina *slov* nad A.

Poznámka. Píšeme stručne $a_1 \ldots a_n$ namiesto $(a_1, \ldots, a_n)$. Slovo pre $n = 0$ značíme λ a hovoríme mu *prázdne* (v automatoch ε).

Veta 9.2. *Na množine A^* definujeme operáciu $\cdot$ (zreťazenie) vzťahom $a_1 \ldots a_n \cdot b_1 \ldots b_m = a_1 \ldots a_n b_1 \ldots b_m$ pre $a_1, \ldots, a_n, b_1, \ldots, b_m$. Potom $(A^*, \cdot, \lambda)$ je monoid (tzv. voľný nad A).*

Dôkaz. Uzavretosť, asociativita je zrejmá; λ je neutrálny prvok. □

Definícia 9.3. *Jazyk* nad abecedou A je ľubovoľná podmnožina množiny A^*.

Definícia 9.4. *Súčin* jazykov U, V je $U \cdot V = \{u \cdot v \mid u \in U, v \in V\}$.

Definícia 9.5. *Iterácia* jazyka U je $U^* = \{u_1 \ldots u_n \mid n \in \mathbb{N}_0, u_1, \ldots, u_n \in U\}$.

Poznámka. Jazyk pre $n = 0$ značíme $\emptyset$ a hovoríme mu *prázdny*. Platí, že $\emptyset^* = \{\lambda\}$.

Definícia 9.6. Jazyk $L \subseteq A^*$ sa nazýva *regulárny*, ak vznikol z $\emptyset$ a prvkov množiny A použitím konečne mnoho aplikácií operácií $^*, \cdot, \cup$ (binárne zjednotenie).

9.2 Automaty

Definícia 9.7. *Deterministický konečný automat* M je pätica $(Q, A, \cdot, q_0, F)$, kde:

- Q je neprázdna konečná množina stavov,
- A je neprázdna konečná množina vstupných symbolov (vstupná abeceda),
- $\cdot\colon Q \times A \to Q$ je parciálna prechodová funkcia, kde $(q, a) \mapsto q \cdot a$,
- $q_0 \in Q$ je počiatočný stav,
- $F \subseteq Q$ je množina koncových (akceptujúcich) stavov.

Definícia 9.8. Každé slovo $u \in A^*$ definuje transformáciu $[u]\colon Q \to Q$, kde $q \mapsto q \cdot u$.

- Zobrazenie $[a]$ pre $a \in A$ je už definované,
- $q \cdot \lambda = q$,
- $q \cdot (ua) = (q \cdot u) \cdot a \quad$ pre $q \in Q, u \in A^*, a \in A$.

Definícia 9.9. Monoid $(\{[u] \mid u \in A^*\}, \cdot)$, kde $[u] \cdot [v] = [uv]$ sa nazýva *transformačný monoid* automatu M.

Definícia 9.10. $L(M) = \{u \in A^* \mid q_0 \cdot u \in F\}$ je jazyk *prijímaný* automatom M.

Definícia 9.11. Automat je *minimálny*, ak platí:

(i) $\{q_0 \cdot u \mid u \in A^*\} = Q$ (z počiatočného stavu sa viem dostať do všetkých ďalších);

(ii) $\forall p, q \in Q\colon \forall u \in A^*\colon (pu \in F \iff qu \in F) \implies p = q$ (ak sa zo stavov p, q dostanem do koncového, nebudem medzi nimi rozlišovať).

9.3 Kongruencie na pologrupách

Definícia 9.12. *Kongruencia pologrupy* $(S, \cdot)$ je relácia ekvivalencie $\sim$ na množine S, ktorá spĺňa: $\forall a, b, c, d \in S\colon a \sim b, c \sim d \implies ac \sim bd$. (Definícia je vhodná pre dôkazy.)

Lemma 9.13. *Namiesto podmienky vyššie stačí:* $\forall a, b, c \in S\colon a \sim b, \implies ac \sim bc, ca \sim cb$. *(Vhodnejšie pre výpočty – máme menej premenných.)*

Dôkaz. „$\implies$“: Stačí $d := c$ a potom $a := c, b := c, c := a, d := b$.
„$\impliedby$“: Z $ac \sim bc, bc \sim bd$ tranzitívne $ac \sim bd$. □

Príklad 9.14. Príklad kongruencie na grupe $(\mathbb{Z}, +)$: $a \equiv b \pmod{n}$.

Príklad 9.15. Príklad kongruencie na monoide $(\mathbb{Z}, \cdot)$: $a \equiv b \pmod{n}$.

Veta 9.16. *Nech* $a\sim := \{b \in S \mid b \sim a\}$ *pre* $a \in S$ *a nech* $S/\sim := \{a\sim \mid a \in S\}$ *je rozklad na* S. *Na množine* $S/\sim$ *definujeme operáciu* $\cdot$ *vzťahom* $a\sim \cdot b\sim = (a \cdot b)\sim$. *Potom* $(S, \cdot)/\sim$ *je pologrupa (tzv. faktorová).*

Dôkaz. Uzavretosť, asociativita je zrejmá.
Ak $(S, \cdot, e)$ je monoid, tak $e\sim$ je neutrálny prvok v $(S, \cdot, e)/\sim$. □

9.4 Syntaktické štruktúry

Definícia 9.17. Jazyk $L \subseteq A^*$ definuje na množine A^* reláciu $\sim_L$ vzťahom

$$u \sim_L v, \text{ práve keď } \forall s,t \in A^*\colon sut \in L \iff svt \in L.$$

Reláciu $\sim_L$ nazývame *syntaktická kongruencia*.

Lemma 9.18. *Syntaktická kongruencia je relácia ekvivalencie a je to kongruencia.*

Dôkaz. Reflexivita: $u \sim_L u$. Symetria: $u \sim_L v \implies v \sim_L u$. Tranzitivita: $u \sim_L v, v \sim_L w \implies u \sim_L w$.

Kongruencia: Ak $u,v,w \in A^*$, tak chceme, aby $u \sim_L v$ dalo $uw \sim_L vw$; podobne $wu \sim_L wv$. Nech $s,t \in A^*$. Potom $suwt \in L \iff svwt \in L$. □

Definícia 9.19. Relácia $\sim_L$ je kongruencia monoidu $(A^*,\cdot)$. Príslušný faktorový monoid nazývame *syntaktický monoid* jazyka L a značíme ho $(O(L),\cdot) := A^*/\sim_L$.

Poznámka. $O(L)$ znamená "ordered".

Definícia 9.20. Na množine $O(L)$ definujeme reláciu usporiadania $\leq_L$ vzťahom

$$u{\sim_L} \leq_L v{\sim_L}, \text{ práve keď } \forall s,t \in A^*\colon svt \in L \implies sut \in L.$$

Veta 9.21. *Nech minimálny automat $M = (Q,A,\cdot,q_0,F)$ prijíma jazyk $L = L(M)$. Syntaktický monoid jazyka L je izomorfný s transformačným monoidom automatu M.*

Dôkaz. Definujme zobrazenie φ medzi syntaktickým monoidom $O(L)$ a transformačným monoidom $T(M)$ nasledovne: $\varphi\colon O(L) \to T(M)$, kde $u{\sim_L} \mapsto [u]$. (Pre jednoduchosť budeme namiesto $u{\sim_L}$ písať len $u{\sim}$.)

- Homomorfizmus: $\varphi(u{\sim}\cdot v{\sim}) = \varphi(uv{\sim}) = [uv]$, a aj $\varphi(u{\sim})\cdot\varphi(v{\sim}) = [u]\cdot[v]$.
- Surjektivita: mám zadaný obraz $[u]$ a chcem nájsť jeho vzor – to je $u{\sim}$.
- Injektivita a korektnosť vyplynú z dôkazu tvrdenia: $\forall u,v \in A^*\colon u \sim v \iff [u] = [v]$.

  Korektnosť (v smere $\implies$) znamená, že ak $u \sim v$, teda $u{\sim} = v{\sim}$, teda jeden prvok je zapísaný dvoma spôsobmi, tak potom dostanem rovnaký obraz $[u] = [v]$.

  Injektivita vyplynie v smere $\impliedby$.

  Dokážme teda ekvivalenciu vyššie. Ľavá strana $u \sim v$ je ekvivalentná tvrdeniu $\forall p,q \in A^*\colon puq \in L \iff pvq \in L$.

$$\begin{aligned}
&\forall p,q \in A^*\colon puq \in L \iff pvq \in L, && \text{t. j.}\\
&\forall p,q \in A^*\colon q_0\cdot puq \in F \iff q_0\cdot pvq \in F, && \text{t. j. podľa (ii) z Def. 9.11}\\
&\forall p \in A^*\colon q_0\cdot pu = q_0\cdot pv, && \text{t. j. } u,v \text{ transformujú rovnako}\\
&\forall p \in A^*\colon (q_0p)[u] = (q_0p)[p], && \text{t. j. podľa (i) z Def. 9.11}\\
&\forall q \in Q\colon q[u] = q[v], && \text{t. j.}\\
&\qquad [u] = [v].
\end{aligned}$$

□

Veta 9.22. *Pre jazyk $L \subseteq A^*$ je ekvivalentné:*

1. *L je regulárny;*
2. *L je prijímaný konečným automatom;*
3. *$O(L)$ je konečná množina.*

Dôkaz. 2. $\Longrightarrow$ 3.: Daný automat je konečná množina. Minimalizujeme ho. Transformáciou konečnej množiny vznikne konečná množina $O(L)$.

3. $\Longrightarrow$ 2.: Definujme zobrazenie $\sigma\colon A^* \to O(L)$ tak, že $\sigma\colon u \mapsto u\sim$. Potom σ je surjektívny homomorfizmus: $\sigma(uv) = (uv)\sim$, $\sigma(u)\cdot\sigma(v) = u\sim \cdot\, v\sim$.

Zostrojíme automat $M = (Q, A, \cdot, q_0, F)$ prijímajúci jazyk L:

- $Q := O(L)$,
- $A := A$,
- Pre $q \in Q, a \in A$ je $q \cdot a = q \cdot \sigma(a)$,
- $q_0 := 1$,
- $q \in F \iff q \in \sigma(L)$.

Potom $u \in L(M) \iff 1 \cdot u \in T$, t. j. $1 \cdot \sigma(u) \in \sigma(L)$, t. j. $\sigma(u) \in \sigma(L)$, t. j. $u \in L$.

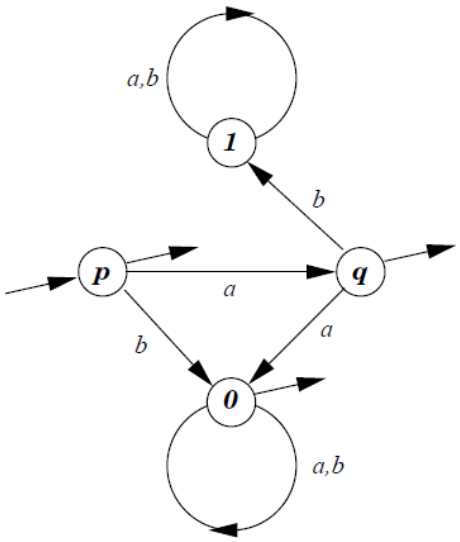
Ukážeme, že v rámci A^* neexistuje trieda slov, kde niečo $\in L$ a niečo $\notin L$.

L je zjednotením $\sim$-tried. Potom $u \sim v$, $v \in L$ dá $u \in L$. Vezmi $p = q = 1$. □

Dôsledok 9.23. *Pre regulárne jazyky nad množinou A nám Veta 9.21 dáva algoritmus pre výpočet syntaktických monoidov. Uvažujeme postupne transformácie množiny Q dané slovami v poradí ich dĺžok, pričom slová rovnakej dĺžky preberáme v lexikografickom usporiadaní. Dostávame tak prezentáciu syntaktického monoidu.*

Príklad 9.24. Lexikografické usporiadanie pre $A = \{a, b\}$ je $\lambda, a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, aaaa, aaab, \ldots$

Príklad 9.25. Transformačný monoid minimálneho automatu



má prvky

u	p	q	0	1
1	p	q	0	1
a	q	0	0	1
b	0	1	0	1
a^2	0	0	0	1
ab	1	0	0	1

Postupne si vypisujem riadky vo vojenskom usporiadaní $(1, a, b, aa, ab, \dots)$ a dívam sa, či sa neopakujú. Napr. $b = ba = bb$ alebo $aa = aaa = aab$.

Keď máme tabuľku, zistíme, že hrozné slovo ako *abbaabab* transformuje rovnako ako *ab*.

Ďalej syntaktický monoid jazyka prijímaného týmto automatom má prezentáciu

$$O(L) = \langle a, b \mid ba = b, b^2 = b, a^3 = a^2, a^2b = a^2 \rangle.$$

(Iné už netreba, napr. *aba* je zbytočné, lebo $ba = b$, teda $aba = ab$ a to už mám.)

9.5 Regulárne výrazy

Definícia 9.26. Množina $RE(A)$ *regulárnych výrazov* nad abecedou A je definovaná:

1. $\emptyset = 0, \varepsilon = 1, a$ pre každé $a \in A$ sú (základné) regulárne výrazy nad A.
2. Ak $E, F \in RE(A)$, sú aj $(E \cdot F), (E + F)$ a (E^*) regulárne výrazy nad A. Zátvorky je možné vypustiť s tým, že najväčšiu prioritu má *, potom $\cdot$ a potom $+$.
3. Každý regulárny výraz vznikne po konečnom počte aplikácií krokov 1 a 2.

Poznámka. Regulárny výraz je teda množina $\{0, 1, a \in A\}$ uzavretá na operácie $*, \cdot, +$.

Definícia 9.27. Každý $E \in RE(A)$ popisuje jazyk $L(E)$ nad A podľa pravidiel:

- $L(\varepsilon) = \{\varepsilon\}$,
- $L(\emptyset) = \emptyset$,
- $L(a) = \{a\}$ pre každé $a \in A$,
- $L(E \cdot F) = L(E) \cdot L(F)$,
- $L(E + F) = L(E) \cup L(F)$,
- $L(E^*) = L(E)^*$.

Definícia 9.28. *Zovšeobecnený* RV je množina $\{0, 1, a \in A\}$ uzavretá na operácie $\cdot, +, \cap, '$. Túto množinu nad abecedou A značíme $GRE(A)$.

Definícia 9.29. Nech $E \in GRE(A)$ je zovšeobecnený RE. Jazyk $L(E)$ nazývame *star-free*.

Príklad 9.30. Máme abecedu $A = \{a, b\}$. Jazyk $L = (ab)^*$ je *star-free*, pretože je možné ho zadať zovšeobecneným RV (bez operácie $*$) nasledovne:

$$L = 1 + ((bA^*)' \cap (A^*a)' \cap (A^*aaA^*)' \cap (A^*bbA^*)'),$$

kde $A^* = 0'$. (Slovo z L nesmie začínať b-čkom, nesmie končiť a-čkom a nesmie mať dve rovnaké písmená bezprostredne za sebou.)

9.6 Vlastnosti jazykov

Definícia 9.31. Podslovo je ľubovoľná podčasť (nie nutne postupnosť) iného slova.

Príklad 9.32. Slovo *cd* je podslovom slova *cxydz*.

Veta 9.33 (Higman, Conway, Nash-Williams)**.** *Ľubovoľná nekonečná množina slov nad konečnou abecedou A obsahuje dve rôzne slová u, v tak, že $u \leq v$ je podslovo.*

Dôkaz. Bonus... □

Definícia 9.34. Jazyk $L \subseteq A^*$ sa nazýva „$\frac{1}{2}$“, keď je konečným zjednotením konečných prienikov jazykov tvaru $A^*a_1A^* \dots A^*a_kA^*$, kde $k \in \mathbb{N}_0$ behá. Do zadaných jazykov patrí práve to, čo má za podslovo $a_1a_2 \dots a_k$.

Definícia 9.35. Jazyk $L \subseteq A^*$ sa nazýva „level 1“, keď je konečným zjednotením konečných prienikov jazykov tvaru $A^*a_1A^* \dots A^*a_kA^*$ a ich komplementov, kde $k \in \mathbb{N}_0$ behá.

Veta 9.36. *Jazyk $L \subseteq A^*$ je „$\frac{1}{2}$“, práve keď je neutrálny prvok jeho syntaktického monoidu najväčším prvkom usporiadanej množiny $(O(L), \leq)$.*

Dôkaz. „$\implies$“: Vezmime $L = A^*a_1A^* \dots A^*a_kA^*$ (pozor na to, že $a_1, \dots, a_k$ nemusia byť nutne po dvoch rôzne). Platí, že pre $p, q, u \in A^*$: $pq \in L \implies puq \in L$, t. j. $\forall u \in A^*$: $u\sim = 1\sim$. Táto podmienka platí pre naše jazyky tvaru L, ale musí aj pre ich konečné prieniky a zjednotenia. Ale zjednotenia jazykov nášho typu budú zjavne opäť jazyky nášho typu. Pre prieniky stačí prepísať jazyk s použitím zjednotení (pozri Príklad 9.38).

„$\impliedby$“: Nech $p, q, u \in A^*$. Potom $pq \in L \implies puq \in L$. Nech $M = \{u_1, \dots, u_k\}$ je množina všetkých min. prvkov z L vzhľadom k usporiadaniu $\leq$ („byť podslovom“). Podľa 9.33: $u_i = a_{i1} \dots a_{il_1}$, kde $i = 1, \dots, k$. Potom $L = A^*a_{11}A^* \dots a_{1l_1}A^* \cup \dots \cup A^*a_{k_1}A^* \dots a_{il_k}A^*$. □

Definícia 9.37. The *shuffle* of two words is a finite set of words obtainable from merging the words x and y from left to right, but choosing the next symbol arbitrarily from x or y.

Príklad 9.38. $A = \{a, b\}$, $L = A^*aA^*aA^*bA^* \cap A^*bA^*aA^*$. Ako L vyjadriť v tvare „$\frac{1}{2}$“? Vezmi z prvého $x = \overline{aab}$ a z druhého $y = \underline{ba}$. Shuffle je množina $\{\overline{aa}\underline{ba}, \overline{a}\underline{b}\overline{ab}\underline{a}, \overline{a}\underline{b}\overline{a}\underline{a}\overline{b}, \overline{a}\underline{b}\overline{ab}, \underline{b}\overline{aab}\underline{a}, \underline{b}\overline{aa}\underline{a}\overline{b}, \underline{b}\overline{aab}\}$ slov, ktoré sú podslovom v prvej aj druhej časti jazyka L. Unikátne sú ale len 1., 4. a 7. slovo, pretože 2. a 5. implikuje 1., 3. implikuje 4. a 6. implikuje 7.

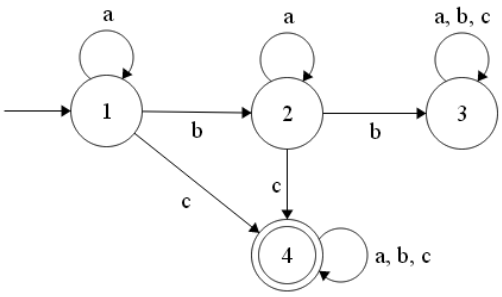
Výsledok: $L = A^*aA^*aA^*bA^*aA^* \cup A^*aA^*bA^*aA^*bA^* \cup A^*bA^*aA^*aA^*bA^*$.

Veta 9.39 (Simon)**.** *Jazyk $L \subseteq A^*$ je „level 1“, práve keď je jeho syntaktický monoid $\mathcal{J}$-triviálny, t. j. keď platí $u\mathcal{J}v \implies u = v$.*

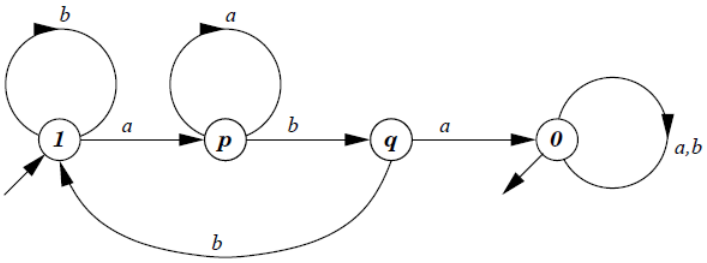
Veta 9.40 (Schützenberger)**.** *Jazyk $L \subseteq A^*$ je star-free, práve keď jeho syntaktický monoid obsahuje len triviálne podgrupy.*

9.7 Cvičenia

1. Určte syntaktický monoid jazyka prijímaného nasledujúcim automatom:



2. Určte syntaktický monoid jazyka prijímaného nasledujúcim automatom:



9.8 Návody k riešeniu cvičení

1. Príslušný regulárny výraz je $a^* \cdot (c + ba^*c) \cdot (a + b + c)^*$.

Transformačný monoid:

	1	2	3	4
λ	1	2	3	4
b	2	3	4	4
c	4	4	3	4
bb	3	3	3	4
cc	4	3	3	4

Vznikne tak 5-prvkový monoid, kde platia relácie: $a = \lambda$, $cb = c$, $cc = c$, $bbb = bb$, $bbc = bb$.
Zadanie syntaktického monoidu tabuľkou:

	λ	b	c	bb	bc
λ	λ	b	c	bb	bc
b	b	bb	bc	bb	bb
c	c	c	c	c	c
bb	bb	bb	bb	bb	bb
bc	bc	bc	bc	bc	bc

Green: $\mathcal{L} = \{\{1\}, \{b\}, \{c, bb, bc\}\} = \mathcal{J} = \mathcal{D}$, $\mathcal{R} = \{\{1\}, \{b\}, \{c\}, \{bb\}, \{bc\}\} = \mathcal{H}$.

2.

	1	2	3	4
ε	1	2	3	4
a	3	4	4	4
b	1	1	2	4
aa	4	4	4	4
ab	2	4	4	4
ba	3	3	4	4
bb	1	1	1	4
~~a^3~~	4	4	4	4
~~a^2b~~	4	4	4	4
~~aba~~	4	4	4	4
ab^2	1	4	4	4
~~ba^2~~	4	4	4	4
bab	2	2	4	4
b^2a	3	3	3	4
~~b^3~~	1	1	1	4
~~ab^2a~~	3	4	4	4
bab^2	1	1	4	4
b^2ab	2	2	2	4
~~b^2ab^2~~	1	1	1	4

Vznikne tak 12-prvkový monoid, kde platia relácie:

- $a^3 = a^2$,
- $a^2b = a^2$,
- $aba = a^2$,
- $ba^2 = a^2$,
- $b^3 = b^2$,
- $ab^2a = a$,
- $b^2ab^2 = b^2$.

Aplikácia transformácií je sprava, napr. $t_{ab} = t_a \circ t_b$. Teda napr. $b^2ab \circ a = b^2aba = b^2a^2 = ba^2 = a^2$.

Zadanie monoidu tabuľkou:

	ε	a	b	a^2	ab	ba	bb	$\ldots$	b^2ab
ε									
a									
b									
$\vdots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
b^2ab	b^2ab	a^2	b^2	a^2	a^2	b^2a	b^2	$\ldots$	b^2ab

(Za kompletnú tabuľku je len o pár bodov viac ako keď vyplníš pár riadkov.)

Tým, že stav 4 je peklo sa pre aa dá pridať pravidlo $a^2 = 0$. Potom všetko, čo obsahuje a^2 tiež skončí v pekle. Tento zápis s 0 ušetrí nejaké relácie. Počet prvkov monoidu sa nezmení, len namiesto a^2 budeme písať 0.

Literatúra

[1] *Creative Commons: Uveďte autora-Neužívejte dílo komerčně-Zachovejte licenci 4.0 Mezinárodní*. Dostupné na URL: http://creativecommons.org/licenses/by-nc-sa/4.0/deed.cs

[2] ROSICKÝ, Jiří. *Algebra*. Vyd 4., přeprac. Brno: Masarykova univerzita, 2007. 133 s. ISBN 978-80-210-2964-4.

[3] Poznámky od doc. Poláka: https://is.muni.cz/auth/of/1433/MV008/podzim2013/algebra_OD_POLAKA.pdf + všetky prednášky.

[4] Vzorové písomky: https://is.muni.cz/auth/el/1433/podzim2010/MB008/um/

[5] WISSAM, Raji. *An Introductory Course in Elementary Number Theory*. 2013. 171 s. Dostupné z URL: http://www.saylor.org/site/wp-content/uploads/2013/05/An-Introductory-in-Elementary-Number-Theory.pdf.

[6] CLARK, Allan. *Elements of Abstract Algebra*. Dover, 1970. ISBN 0-486-64725-0.

[7] http://www.liafa.jussieu.fr/~jep/PDF/Exposes/StAndrews.pdf