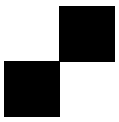


Zápisky z Algebry

Tomáš Hejda

Obsah

Několik poznámek

(1) Dokument vznikl jako přepis přednášek p. Doc. Mareše z předmětu Algebra na katedře matematiky FJFI v zimním semestru 2008/2009.

(2) Všechna tvrzení v přednášce označovaná jako pozorování, lemmata, tvrzení a věty budeme nazývat pouze lemmaty a větami.

(3) Přestože jsou veškeré výroky zapisovány tak, že kvantifikátory nemají závorky, pro přehlednost psaného textu a už ze zvyku závorky psát budeme.

(4) Používáme symbol $\Subset$ místo $\subset\subset$, důvodem je zejména přehlednost tištěného textu.

(5) Součástí publikace je i rejstřík, který by měl pomoci s orientací v textu.

1. Teorie množin

1.1. Naivní teorie množin

(1) Cantor, 19. století

(2) Vychází z představy, že každý objekt je množina.

V naivní teorii množin se brzy došlo k tzv. paradoxům. Ve skutečnosti to nejsou paradoxy, neboť paradox je „neuvěřitelné, leč pravdivé tvrzení“, ale zde jde skutečně o spory v pravém slova smyslu

▶ 1.1.1. Příklad (Cantorův paradox). Nechť $\mathcal{U}$ je množina všech množin a $\mathcal{P}(\mathcal{U}) = \{x \mid x \subset \mathcal{U}\}$ její potenční množina (množina všech jejích podmnožin. Potom neboť $\mathcal{P}(\mathcal{U}) \subseteq \mathcal{U}$, je $|\mathcal{U}| \leq |\mathcal{P}(\mathcal{U})|$ (exaktní definice velkosti množiny je dále). Současně však $\forall M(|\mathcal{P}(M)| > |M|)$, tedy i $|\mathcal{U}| \leq |\mathcal{P}(\mathcal{U})|$, což je spor.

▶ 1.1.2. Příklad (Russelův paradox). 2 předpoklady:

(1) každý výrok $V(x)$ definuje množinu;

(2) o každém prvku lze rozhodnout, zda do množiny patří, či nikoli.

Potom definujme $x := \{y \mid y \notin y\}$. Dále $x \in x \Rightarrow x \notin x$ a zároveň $x \notin x \Rightarrow x \in x$, což je spor.

▶ 1.1.3. Příklad (sémantické paradoxy). Např. paradox Kréťana: „Všichni Kréťani jsou lháři.“ V této podobě však nefunguje a je třeba jej poupravit: „Teď lžu.“

1.2. Axiomatická teorie množin

Teorie množin má 2 axiomatiky, které jsou však ekvivalentní:

(1) Zermelova-Fraenkelova axiomatika (označovaná ZF)

(2) Gődelova-Bernaysova axiomatika;

My budeme pracovat s Zermelovou-Fraenkelovou axiomatikou, jež vznikla v roce 1908.

▶ 1.2.1. Axiom (A0. Axiomy rovnosti).

(1) $\forall x(x = x)$;

(2) $\forall x \forall y(x = y \Rightarrow y = x)$;

(3) $\forall x \forall y \forall z((x = y \wedge y = z) \Rightarrow x = z)$;

(4) $\forall x \forall y \Big(x = y \Rightarrow \big((\forall u(u \in x \Leftrightarrow u \in y)) \wedge \forall u(x \in u \Leftrightarrow y \in u)\big)\Big)$.

▶ 1.2.2. Axiom (A1. Axiom existence). $\exists x(x = x)$.

▶ 1.2.3. Axiom (A2. Axiom extenzionality). $\forall x \forall y \big(x = y \Leftrightarrow \forall u (u \in x \Leftrightarrow u \in y)\big)$.

▶ 1.2.4. Axiom (A3. Axiom dvojice). $\forall x \forall y \exists z \forall u \big(u \in z \Leftrightarrow (u = x \vee u = y)\big)$.

▶ 1.2.5. Definice. Uspořádaná dvojice $\langle x, y \rangle := \{\{x\}, \{x, y\}\}$.
Uspořádaná n-tice $\langle x_1, \ldots, x_n \rangle := \langle x_1, \langle x_2, \ldots, x_n \rangle \rangle$.

▶ 1.2.6. Axiom (A4. Axiom sjednocení (sumy).) $\forall x \exists z \forall u \big(u \in z \Leftrightarrow \exists y (u \in y \wedge u \in x)\big)$.

▶ 1.2.7. Definice. Sumu systému x značíme $z = \bigcup x$.

▶ 1.2.8. Axiom (A5. Schema axiomů vydělení). Nechť $F[u]$ je formule s volnou proměnnou u, jež neobsahuje z. Potom axiomem je $\forall x \exists z \forall u \big(u \in z \Leftrightarrow (u \in x \wedge F[u])\big)$.

▶ 1.2.9. Příklad.

(1) $F = \ulcorner u \in y \urcorner \to$ průnik $z =: x \cap y$.

(2) $F = \ulcorner u \notin y \urcorner \to$ rozdíl $z =: x \setminus y$.

(3) $F = \ulcorner u \neq u \urcorner \to$ existence prázdné množiny $z =: \emptyset$.

▶ 1.2.10. Axiom (A6. Axiom potence). $\forall x \exists z \forall u (u \in z \Leftrightarrow u \subseteq x)$.

▶ 1.2.11. Definice. Potenční množinu množiny x značíme $z = \mathcal{P}(x)$.

▶ 1.2.12. Axiom (A7. Axiom nekonečna). $\exists z \big(\emptyset \in z \wedge \forall x (x \in z \Rightarrow x \cup \{x\} \in z)\big)$.

▶ 1.2.13. Příklad. $\mathcal{P}(\emptyset) = \{\emptyset\}$. $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$. $\mathcal{P}(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$.
Tato posloupnost množin umožňuje definovat přirozená čísla (s nulou) jako množiny.

▶ 1.2.14. Axiom (A8. Axiom fundovanosti). $\forall x \big(x \neq \emptyset \Rightarrow \exists z (z \in x \wedge z \cap x = \emptyset)\big)$.

▶ 1.2.15. Důsledek. $\forall y (y \notin y)$.

▶ 1.2.16. Axiom (A9. Axiom výběru). Nezařazuje se do ZF axiomatiky, pokud jej zahrneme, používáme označení ZFC („C“ označuje „axiom of Choice“).

▶ 1.2.17. Definice (třídy v Z-F axiomatice).

(1) Každá formule $F[u]$ definuje třídu $Z = \{u \mid F[u]\}$.

(2) Třídy značíme velkými písmeny.

(3) Každá monžina je třída $x = \{u \mid u \in x\}$.

(4) Třída, která není množinou, se nazývá vlastní třída.

(5) $\mathcal{U} := \{u \mid u = u\}$ nazýváme universum a je to vlastní třída.

▶ 1.2.18. Poznámka (Gődelova-Bernaysova axiomatika).

(1) Prvotním pojmem je třída.

(2) Množina je taková třída, která je prvkem jiné třídy.

(3) Třída, který není množinou, je vlastní třída.

(4) Obě teorie jsou ekvivalentní.

1.3. Kartézský součin

▶ 1.3.1. Definice. Mějme 2 třídy X, Y. Třídu

$$X \times Y := \{\langle u, v\rangle \mid u \in X \wedge v \in y\} = \{z \mid \exists u \exists v (z = \langle u, v\rangle \wedge u \in X \wedge v \in Y)\}$$

nazveme kartézský součin X a Y.

▶ 1.3.2. Lemma. Jsou-li x a y množiny, pak i kartézský součin $x \times y$ je množina.

○ *Důkaz.* $u \in x \wedge v \in y \implies u, v \in X \cup Y \implies \{u\}, \{u, v\} \in \mathcal{P}(x \cup y) \implies z \in \mathcal{P}(\mathcal{P}(x \cup y)) \implies x \times y = \{z \in \mathcal{P}(\mathcal{P}(x \cup y)) \mid \exists u \exists v (z = \langle u, v\rangle \wedge u \in x \wedge v \in y)\}$, tedy podle schematu axiomu vydělení je $x \times y$ množina. □

---

2. Relace

▶ 2.0.1. Definice. Nechť $M_1, \ldots, M_n$ jsou libovolné množiny Potom libovolné $\rho \subseteq M_1 \times \cdots \times M_n$ nazveme n-ární relací na $M_1 \times \cdots \times M_n$ a číslo n aritou relace ρ.

▶ 2.0.2. Definice.

(1) Každé $R \subseteq M^2$ nazýváme binární relace na M^2.

(2) $R^{-1} := \{\langle a, b\rangle \mid \langle b, a\rangle \in R\}$ je inverzní relace k R.

(3) $R \circ S = RS := \{\langle a, c\rangle \mid \exists b \in M(\langle a, b\rangle \in R \wedge \langle b, c\rangle \in S)\}$ je součin relací.

(4) $D_M = \{\langle a, a\rangle \mid a \in M\}$ je diagonála.

▶ 2.0.3. Definice. Definujeme obecné vlastnosti, předpokládáme platnost výroků pro všechna $a, b, c \in M$. Relace je:

(1) reflexivní $\iff \langle a, a\rangle \in R \iff D_M \subseteq R$;

(2) transitivní $\iff \langle a, b\rangle \in R \wedge \langle b, c\rangle \in R \Rightarrow \langle a, c\rangle \in R \iff RR \subseteq R$;

(3) symetrická $\iff \langle a, b\rangle \in R \Leftrightarrow \langle b, a\rangle \in R \iff R^{-1} = R$;

(4) slabě antisymetrická $\iff \langle a, b\rangle \in R \wedge \langle b, a\rangle \in R \Rightarrow a = b \iff R^{-1} \cap R \subseteq D_M$;

(5) silně antisymetrická $\iff \langle a, b\rangle \in R \Rightarrow \langle b, c\rangle \notin R \iff R^{-1} \cap R = \emptyset$;

(6) trichotonická $\iff \langle a, b\rangle \notin R \Rightarrow (\langle b, a\rangle \in R \vee a = b) \iff R^{-1} \cup R \cup D_M = M^2$;

▶ 2.0.4. Definice. Rozlišujeme následující typy relací:

(1) ekvivalence (zn. $\equiv$) je reflexivní, transitivní a symetrická. Ekvivalence rozděluje množinu na třídy ekvivalence. Množina $M_{/\equiv}$ všech tříd ekvivalence se nazývá faktorová množina nebo též faktor-množina M podle $\equiv$.

(2) uspořádání (zn. $\leq$) je relace reflexivní, transitivní a slabě antisymetrická.

(3) ostré uspořádání (zn. $<$) je relace transitivní a silně antisymetrická. Platí:

$$a \leq b \Leftrightarrow a = b \vee a < b,$$

$$a < b \Leftrightarrow a \neq b \wedge a \leq b.$$

(4) úplné uspořádání (lineární uspořádání) je relace trichotonická (každé dva prvky jsou srovnatelné), slabě antisymetrická, transitivní a reflexivní.

---

3. Uspořádané množiny

3.1. Uspořádané množiny. Řetězce

▶ 3.1.1. Definice.

(1) Množina M s uspořádáním $\leq$ se nazývá uspořádaná množina $(M, \leq)$.

(2) Přirozeným způsobem jsou na M definovány operace $\geq$, $<$, $>$.

(3) Nechť $R \subseteq M$ je úplně uspořádaná, pak ji nazveme řetězcem.

▶ 3.1.2. Definice. Nechť $(M, \leq)$ je uspořádaná množina, $a \in M$. Pak a je:

(1) největší prvek (poslední prvek) $\iff (\forall x \in M)(x \leq a)$;

(2) nejmenší prvek (první prvek) $\iff (\forall x \in M)(x \geq a)$;

(3) maximální prvek $\iff (\forall x \in M)(x \geq a \Rightarrow x = a)$;

(4) minimální prvek $\iff (\forall x \in M)(x \leq a \Rightarrow x = a)$.

▶ 3.1.3. Lemma.

(1) Je-li $a \in M$ poslední, je maximální.

(2) Je-li $a \in M$ první, je minimální.

▶ 3.1.4. Příklad.

(1) $(\mathbb{N}, \mid)$. Relace „dělí“: $a \mid b \Leftrightarrow (\exists c \in \mathbb{Z})(b = ac)$. První prvek je 1, poslední není.

(2) $(\mathbb{N}_0, \mid)$. Prvním prvkem zůstává 1, ale posledním je 0, neboť $n \mid 0$ pro všechna celá čísla.

(3) $(\mathbb{N} \setminus \{1\}, \mid)$. Nemá nejmenší, ale má minimální – jsou to všechna prvočísla.

▶ 3.1.5. Definice. Nechť $(M, \leq)$ je uspořádaná množina, $N \subseteq M$. Pak:

(1) $z \in M$ je horní závora podmnožiny $N \iff (\forall x \in N)(x \leq z)$.

(2) $z \in M$ je dolní závora podmnožiny $N \iff (\forall x \in N)(x \geq z)$.

(3) N je shora omezená $\iff$ existuje horní závora N.

(4) N je zdola omezená $\iff$ existuje dolní závora N.

▶ 3.1.6. Definice. Nechť $(A, \leq)$ a $(B, \leq)$ jsou 2 uspořádané množiny, $f : A \to B$. Pak řekneme, že f je izotonní (izotonie) $\iff (\forall x, y \in A)\big(x \leq y \Rightarrow f(x) \leq f(y)\big)$.

▶ 3.1.7. Definice. Nechť $(A, \leq)$ a $(B, \leq)$ jsou 2 uspořádané množiny. Pak:

(1) $f : a \to b$ je izomorfizmus, pokud je bijektivní a f i f^{-1} jsou izotonní, tj.

$$(\forall x, y \in A)\big(x \leq y \Leftrightarrow f(x) \leq f(y)\big).$$

(2) A a B jsou izomorfní (značíme $A \cong B$), pokud existuje izomorfismus $A \to B$.

• 3.2. Ekvivalence, subvalence množin

▶ 3.2.1. Definice.

(1) Řekneme, že M a N jsou ekvivalentní (ekvipotenční) $\iff$ existuje bijekce M na N. Značíme $M \approx N$.

(2) Řekneme, že M je subvalentní $N \iff$ existuje injekce (prosté zobrazení) M do N. Značíme $M \preccurlyeq N$.

(3) Řekneme, že M je ostře subvalentní $N \iff M \preccurlyeq N \wedge M \not\approx N$. Značíme $M \precnsim N$ nebo $M \prec N$.

▶ 3.2.2. Poznámka.

(1) $\approx$ je ekvivalence.

(2) Třídám ekvivalence $\mathcal{U}_{/\approx}$ přiřazujeme kardinální číslo.

(3) $\preccurlyeq$ není uspořádání, neboť $A \preccurlyeq B \wedge B \preccurlyeq A \Rightarrow A \approx B$, nikoli $A = B$. Lze tedy uspořádat kardinální čísla.

▶ 3.2.3. Věta (Cantor, Bernstein). Nechť M a N jsou libovolné množiny. Pak

$$M \preccurlyeq N \ \wedge \ N \preccurlyeq M \quad \Rightarrow \quad M \approx N.$$

◦ *Důkaz.* Víme, že existují injekce $f : M \to N$ a $g : M \to N$. Označme $N_1 := f(M)$, $M_1 := g(N)$, $N_1' := N \setminus N_1$, $M_1' := M \setminus M_1$. Pak $f : M \xrightarrow{\text{bij.}} N_1$ a $g : N \xrightarrow{\text{bij.}} M_1$.

Definujme posloupnost x_n následovně:

(1) $x_1 \in M$;

(2) pokud $x_1 \in M_1$, definuji $x_2 := g^{-1}x_1$, jinak je x_1 poslední v posloupnosti;

(3) pokud $x_2 \in N_1$, definuji $x_3 := f^{-1}x_2$, jinak je x_2 poslední v posloupnosti;

(4) ...

Posloupnost je jednoduše rekurentní (každý prvek závisí pouze na nejbližším předchozím), tedy se množina M direktně rozkládá na 3 podmnožiny:

(1) $x \in M_M \subseteq M$, pokud poslední člen posloupnosti obsahující x je v M;

(2) $x \in M_N \subseteq M$, pokud poslední člen posloupnosti obsahující x je v N;

(3) $x \in M_\infty \subseteq M$, pokud je posloupnost obsahující x nekonečná.

Obdobně definujeme N_M, N_N a N_∞.

Potom nutně $N_1' \subseteq N_N$ a tedy platí, že $f_{/M_M} : M_M \to N_M$ je prosté, protože f je prosté, a na, protože $N_M \subseteq f(M)$. Obdobně $g_{/N_N} : N_N \xrightarrow{\text{bij.}} M_N$ a konečně $f_{/M_\infty} : M_\infty \xrightarrow{\text{bij.}} N_\infty$. Tedy $M_M \approx N_M$; $M_N \approx N_N$ a $M_\infty \approx N_\infty$, z čehož díky disjunktnosti rozkladů plyne $M \approx N$. □

► 3.2.4. Věta (Cantor).

$$M \precnsim \mathcal{P}(M).$$

◦ *Důkaz.*

$(M \preccurlyeq \mathcal{P}(M))$ Položme $f(x) := \{x\}$.

$(M \not\approx \mathcal{P}(M))$ Důkaz sporem. Předpokládejme, že $M \approx \mathcal{P}(M)$.

Pak $(\exists g : M \xrightarrow{\text{bij.}} \mathcal{P}(M))$. Označme $D := \{x \in M \mid x \notin g(x)\}$, $d = g^{-1}(D)$. Pak

- $d \in D \Rightarrow d \notin g(d) = D$;
- $d \notin D \Rightarrow d \in g(d) = D$,

což je spor. (Tento typ důkazu se nazývá Cantorův diagonální argument.)

□

• **3.3.** Úplně uspořádané množiny

► 3.3.1. Definice. Nechť $(A, \leq)$, $(B, \leq)$ jsou 2 úplně uspořádané množiny a nechť A je izomorfní s B. Potom řekneme, že A je podobná B (relace podobnost; značíme $A \cong B$), pokud existuje zobrazení $f : A \to B$ nazývané podobnost, které je bijektivní a izotonní.

► 3.3.2. Lemma. Podobnost je ekvivalence na třídě všech úplně uspořádaných množin.

◦ *Důkaz.*

(reflexivita) Podobností je identita.

(symetrie) Podobností $g : B \to A$ je inverzní zobrazení k podobnosti $f : A \to B$.

(transitivita) existence podobností $f : A \to B$ a $g : B \to C$ zajišťuje existenci podobnosti $h : A \to C$, $h = g \circ f$.

□

▶ 3.3.3. Definice. Ordinální typ je charakteristická vlastnost tříd ekvivalence na všech úplně uspořádaných množinách podle $\cong$. Značí se $\operatorname{ord} A$.

▶ 3.3.4. Příklad.

(1) $\operatorname{ord} \emptyset =: 0$.

(2) Nechť K je úplně uspořádaná a $|K| = k \in \mathbb{N}$. Pak $\operatorname{ord} K =: k$. (Jednoznačnost lze ukázat matematickou indukcí, každá má první prvek)

(3) $\operatorname{ord} (\mathbb{N}, \leq) =: \omega$.

▶ 3.3.5. Věta. Nechť A a B jsou podobné množiny. Pak má-li A první prvek, má jej i B.

◦ *Důkaz.* Nechť p je první v A a $f : A \to B$ je podobnost. Ukážeme, že $f(p)$ je první v B, tj. $(\forall y \in B)(\exists x \in A)(y = f(x))$. Ale p je první v A, tedy $x \geq p \Rightarrow y = f(x) \geq f(p)$. □

▶ 3.3.6. Příklad.

(1) $S = \{2n \mid n \in \mathbb{N}\} \cong \mathbb{N}$, $f : S \to \mathbb{N}$, $f(x) = x/2$.

(2) $\mathbb{N}_0 \cong \mathbb{N}$, $f(x) = x + 1$.

(3) $(\mathbb{Z}, \leq) \ncong (\mathbb{N}, \leq)$, neboť $\mathbb{N}$ má první a $\mathbb{Z}$ nikoliv, ale $\mathbb{Z} \approx \mathbb{N}$.

▶ 3.3.7. Definice. Řekneme, že úplné uspořádání $(M, \leq)$ je husté, právě když:

$$(\forall x, y \in M, x < y)(\exists z \in M)(x < z < y).$$

▶ 3.3.8. Příklad.

(1) $(\mathbb{Z}, \leq)$ není husté uspořádání.

(2) $(\mathbb{Q}, \leq)$ je husté uspořádání.

▶ 3.3.9. Věta. Libovolná spočetná hustě uspořádaná množina, která nemá ani první, ani poslední prvek, je podobná $(\mathbb{Q}, \leq)$.

▶ 3.3.10. Definice. Nechť A je úplně uspořádaná množina, $a \in A$. Pak úsekem množiny A určeným prvkem a rozumíme $A_a := \{x \in A \mid x < a\}$.

▶ 3.3.11. Věta.

(1) Je-li a první v A, pak $A_a = \emptyset$.

(2) Je-li a poslední v A, pak $A_a = A \setminus \{a\}$.

(3) Ze 2 různých úseků množiny A je jeden úsekem druhého.

(4) $a \leq b \iff A_a \subseteq A_b$.

(5) $(\{A_a \mid a \in A\}, \subseteq)$ je úplně uspořádaná množina.

(6) $(\{A_a \mid a \in A\}, \subseteq) \cong (A, \leq)$.

• 3.4. Dobré uspořádání

▶ 3.4.1. Definice. Řekneme, že množina M je dobře uspořádaná, má-li libovolná neprázdná podmnožina M první prvek.

▶ 3.4.2. Věta. Dobré uspořádání je úplné.

◦ *Důkaz.* Mějme libovolné $a, b \in M$, $a \neq b$. Pak množina $\{a, b\} \subseteq M$ má první prvek, a tedy $a < b$ nebo $b < a$. □

▶ 3.4.3. Věta.

(1) Neprázdná dobře uspořádaná množina má první prvek.

(2) Libovolná podmnožina dobře uspořádané množiny je dobře uspořádaná.

(3) Množina podobná dobře uspořádané množině je dobře uspořádaná. (Dobře uspořádané množiny mají tedy vlastní třídy ekvivalence podle $\cong$ a jejich ordinální typ nazýváme ordinální číslo.)

(4) Libovolný prvek dobře uspořádané množiny M, který není poslední (poslední však nemusí existovat), má následníka, tj.

$$(\forall x \in M, x \text{ není poslední})(\exists y \in M)(\forall z \in M)(z \leq x \vee z \geq y).$$

▶ 3.4.4. Příklad. Mějme $(\mathbb{Z}, \preccurlyeq)$ s uspořádáním definovaným následovně:

(1) $x, y \geq 0 \quad x \prec y \Leftrightarrow x < y$;

(2) $x, y < 0 \quad x \prec y \Leftrightarrow -x < -y$;

(3) $x < 0 \leq y \quad y \prec x$.

Pak $\operatorname{ord}(\mathbb{Z}, \preccurlyeq) = \omega + \omega \neq \omega$.

▶ 3.4.5. Axiom (A9. Axiom výběru). Na libovolném $M \neq \emptyset$ existuje selektor (výběrová funkce) $\phi : \mathcal{P}(M) \setminus \{\emptyset\} \to M$ a platí: $(\forall A \subseteq M, A \neq \emptyset)(\phi(A) \in A)$.

▶ 3.4.6. Definice. Zermelova-Frankelova axiomatika s axiomem výběru se označuje ZFC.

▶ 3.4.7. Věta (Zermelo, v ZFC). Na libovolné množině existuje binární relace, která je jejím dobrým uspořádáním.

▶ 3.4.8. Věta (v ZFC). Nechť M je úplně uspořádaná množina. Pak následující výroky jsou ekvivalentní:

(1) M je dobře uspořádaná;

(2) na M platí indukční podmínka:

$$\big(\forall N \subseteq M\big)\Big(\forall x \in M\big(\forall y \in M(y < x \Rightarrow y \in N) \Rightarrow x \in N\big) \Rightarrow N = M\Big);$$

(3) na M platí podmínka konečnosti klesajících řetězců (každý ostře klesající řetězec má konečnou délku).

◦ *Důkaz.* Pro $M = \emptyset$ je důkaz triviální. Tedy nechť $M \neq \emptyset$.

$(1 \Rightarrow 2)$ Důkaz sporem. Nechť $(\exists N \subseteq M)(\forall x \in M(\forall y \in M(y < x \Rightarrow y \in N) \Rightarrow x \in N) \wedge N \subsetneq M)$. M je dobře uspořádaná, tedy má první prvek p a podle předpokladu (neexistuje $y < p$) je $p \in N$, tedy $N \neq \emptyset$. Dále $M \setminus N \neq \emptyset$ (N je vlastní podmnožina), tedy existuje první prvek $q \in M \setminus N$. Potom $(\forall y < q)(y \in N) \Rightarrow q \in N$, což je spor s $q \in M \setminus N$.

$(2 \Rightarrow 3)$ Nechť N je množina všech $z \in M$, pro které neexistuje nekonečný ostře klesající řetězec začínající v z.

$(3 \Rightarrow 1)$ Dokážeme sporem. Nechť M není dobře uspořádaná, tedy nechť existuje neprázdná $N \subseteq M$, která nemá první prvek. Pak pro libovolné $a \in N$ je úsek N_a neprázdný (jinak by a byl první prvek) a podle axiomu výběru $(\exists \phi : \mathcal{P}(N) \setminus \{\emptyset\} \to N)(\phi(x) \in x)$. Definujme posloupnost $(a_k)_1^\infty$ následovně: $a_1 := \phi(N)$; $a_{k+1} := \phi(N_{a_k})$. Protože N_a je neprázdná pro všechna a a $a_{k+1} < a_k$ (vlastnost úseku), je (a_k) nekonečný ostře klesající řetětec, což je spor.

□

▶ 3.4.9. Věta. Upořádaná množina $(\mathbb{N}, \leq)$ je uspořádaná dobře.

▶ 3.4.10. Věta. Nechť A je dobře uspořádaná množina, $B \subseteq A$, $B \cong A$, $f : A \to B$ je podobnost. Pak $(\forall x \in A)(f(x) \geq x)$.

◦ *Důkaz.* Označme $M := \{x \in A \mid f(x) < x\}$. Ukážeme sporem, že M je prázdná.
Nechť $M \neq \emptyset$. Pak $M \subseteq A$, tedy má první prvek p. Platí $f(p) < p$, tedy z izotonie f je $f(f(p)) < f(p)$ a tedy $f(p)$ je prvek M menší než p, což je spor. □

▶ 3.4.11. Věta. Ze 2 dobře uspořádaných množin je vždy jedna podobná druhé nebo jejímu úseku.

▶ 3.4.12. Věta (princip maximality, Zornovo lemma, Kuratowského lemma). Nechť $(M, \leq)$ je uspořádaná množina. Pak má-li libovolný řetězec z M horní závoru v M, pak libovolný prvek $a \in M$ je srovnatelný s nějakým maximálním prvkem v M. (A tedy existuje alespoň jeden maximální prvek v M.)

▶ 3.4.13. Věta (speciální případ Zornova lemmatu). Nechť $(\mathcal{S}, \subseteq)$ je systém množin uspořádaný inkluzí. Pokud pro každý řetězec R z $\mathcal{S}$ je $\bigcup R \in \mathcal{S}$, pak $(\forall A \in \mathcal{S})(\exists B \in \mathcal{S}, B \text{ maximální})(A \subseteq B)$.

▶ 3.4.14. Věta. Subvalence je trichotonická na třídě všech množin (tj. libovolné 2 prvky jsou srovnatelné).

◦ *Důkaz.* Mějme 2 neprázdné množiny $A, B \in \mathcal{U}$. Označme M množinu všech prostých zobrazení z A do B, tedy $M = \left\{ f \;\middle|\; f : (A) \xrightarrow{\text{inj.}} B \right\}$. Každé f je speciální podmnožina $A \times B$, tedy $(M, \subseteq)$ je uspořádání. Nechť $R \subseteq M$ je řetězec. Označme $g := \bigcup R$ Ukážeme, že $g \in M$. □

(g je zobrazení) Nechť $\langle a, b_1\rangle, \langle a, b_2\rangle \in g$. Pak $(\exists f_1, f_2 \in R)\big(\langle a, b_1\rangle \in f_1, \langle a, b_2\rangle \in f_2\big)$. Bez újmy na obecnosti je $f_1 \subseteq f_2$ a tedy $\langle a, b_1\rangle, \langle a, b_2\rangle \in f_2$, tedy (neboť f_2 je zobrazení) $b_1 = b_2$.

(g je injekce) Vezmeme $\langle a_1, b\rangle, \langle a_2, b\rangle \in g$. Stejným postupem dostaneme $a_1 = a_2$.

Tedy v M existuje maximální prvek f. Ukážeme, že je buďto $\operatorname{def} f = A$ nebo $f(A) = B$. Nechť $(\exists a \in A)(a \notin \operatorname{def} f)$ a $(\exists b \in B)(f^{-1}(\{b\}) = \emptyset)$. Pak $f' := f \cup \langle a, b\rangle$ je bijekce z A do B a $f \preccurlyeq f'$, což je spor s maximalitou f.

▶ 3.4.15. Věta. Libovolný netriviální vektorový prostor V má (konečnou nebo Hammelovu) bázi.

◦ *Důkaz.* Označme $\mathcal{S}$ systém všech lineárně nezávislých podmnožin V uspořádaný inkluzí. Ukážeme, že pro libovolný řetězec $R = \{A_i \mid i = 1, \ldots, n, \infty\} \subseteq \mathcal{S}$ je $A := \bigcup R \in \mathcal{S}$. Mějmě konečnou lineární kombinaci $\sum_{j=1}^{k} \alpha_j a_j$ prvků z A. Pro každé a_j existuje A_{i_j} takové, že $a_j \in A_{i_j}$. Označme $i_m = \max_{j \in \widehat{k}} i_j$. Pak $(\forall j \in \widehat{k})(a_j \in A_{i_m} \in \mathcal{S})$, tedy $\sum_{j=1}^{k} \alpha_j a_j = 0 \Leftrightarrow (\forall j)(\alpha_j = 0)$, což znamená, že $A \in \mathcal{S}$. Tedy podle Zornova lemmatu existuje maximální prvek $B \in \mathcal{S}$.

Ukážeme, že $B_\lambda = V$. Zjevně $B_\lambda \subseteq V$, tedy zbývá ukázat, že generuje: Vezměme $v \in V \setminus B$. Pak $B \cup \{v\} \supsetneq B$ je lineárně závislá (jinak by B nebyla maximální v $\mathcal{S}$). Tedy existuje konečná lineární kombinace z $B \cup \{v\}$ a nutně je koeficient u v nenulový (jinak by kombinace byla nulová a z B, ale B je lineárně nezávislá). Tedy $v \in B_\lambda$. □

▶ 3.4.16. Věta (Hausdorffův princip, v ZFC). V libovolné uspořádané množině je každý řetězec částí nějakého maximálního řetězce (ve smyslu inkluze).

▶ 3.4.17. Věta. V ZF axiomatice jsou následující výroky ekvivalentní:

(1) axiom výběru;

(2) princip dobrého uspořádání (Zermelova věta);

(3) princip maximality (Zornovo lemma);

(4) Hausdorffův princip.

• 3.5. Uspořádání kartézského součinu

▶ 3.5.1. Definice. Nechť $(A, \leq)$, $(B, \leq)$, $A \times B = \{\langle a, b\rangle \mid a \in A, b \in B\}$.
Pak definuji lexikografické uspořádání:

$$\langle a, b\rangle \leq \langle c, d\rangle \iff (a < c \ \vee \ (a = c \wedge b \leq d)).$$

▶ 3.5.2. Lemma. Jsou-li A, B dobře uspořádané, pak i lexikografické uspořádání na $A \times B$ je dobré.

◦ *Důkaz.* Nechť $\emptyset \neq M \subseteq A \times B$. Položme $M_A := \{a \in A \mid (\exists b \in B)(\langle a, b\rangle \in M)\}$. $\emptyset \neq M_A \subseteq A$, tedy má první prvek p. Položme $M_B := \{b \in B \mid \langle p, b\rangle \in M\}$. $\emptyset \neq M_B \subseteq B$, tedy má první prvek q.

Ukážeme, že $(\forall \langle a, b\rangle \in M)(\langle p, q\rangle \leq \langle a, b\rangle)$. Z definice M_A je $p \leq a$ a pokud $p = a$, je z definice M_B $q \leq b$. □

▶ 3.5.3. Definice. Nechť A, B jsou dobře uspořádané množiny, $\alpha = \operatorname{ord} A$, $\beta = \operatorname{ord} B$. Definujeme součin ordinálních čísel:

$$\alpha \cdot \beta := \operatorname{ord}(B \times A).$$

▶ 3.5.4. Příklad.

(1) $\operatorname{ord} \mathbb{N} = \omega$.

(2) $\omega \cdot \omega = \operatorname{ord}(\mathbb{N} \times \mathbb{N}) =: \omega^2$.

(3) $\omega \cdot 2 = \operatorname{ord}(\{a, b; a < b\} \times \mathbb{N}) = \omega + \omega \neq \omega$.

(4) $2 \cdot \omega = \operatorname{ord}(\mathbb{N} \times \{a, b\}) = \operatorname{ord} \mathbb{N} = \omega$. Tedy $\omega \cdot 2 \neq 2 \cdot \omega$.

▶ 3.5.5. Definice. Nechť $\mathcal{S} = \{A_i \mid i \in I\}$ je systém po dvou disjunktních množin (disjunktnost lze zaručit položením $A_i' := \{i\} \times A_i$. Nechť $(I, \leq_I)$ je uspořádání, stejně tak pro všechna $i \in I$ je $(A_i, \leq_i)$ uspořádání. Pak definujeme uspořádané sjednocení uspořádaných množin na množině $A = \bigcup \mathcal{S}$. Nechť $a, b \in A$, $a \in A_i$, $b \in B_j$. Pak

$$a \leq b \Leftrightarrow (i <_I j \vee (i = j \wedge a \leq_i b)).$$

▶ 3.5.6. Lemma. Usporádání $\leq$ na A je úplné/dobré, pokud $\leq_I$ i všechna $\leq_i$ jsou úplná/dobrá.

◦ *Důkaz.* Obdobně jako pro kartézský součin □

▶ 3.5.7. Definice. Nechť A_1, A_2 jsou dobře uspořádané množiny, $\alpha = \operatorname{ord} A_1$, $\beta = \operatorname{ord} A_2$. Definujeme součet ordinálních čísel:

$$\alpha + \beta := \operatorname{ord} \bigcup \{A_1, A_2\}.$$

▶ 3.5.8. Příklad.

(1) $1 + \omega = \operatorname{ord} \bigcup \{A_1 = \{a\}; A_2 = \mathbb{N}\} = \omega$.

(2) $\omega + 1 = \operatorname{ord} \bigcup \{A_1 = \mathbb{N}; A_2 = \{a\}\} \neq \omega$.

---

4. Algebra

▶ 4.0.1. Definice. Nechť $n \in \mathbb{N}_0$.

(1) Pak n-ární algebraickou operací na $M \neq \emptyset$ rozumíme libovolnou $(n+1)$-ární relaci ω na M, která splňuje podmínku jednoznačnosti:

$$(\forall x_1, \ldots, x_n, y, z \in M)\Big(\big((x_1, \ldots, x_n, y) \in \omega \ \wedge \ (x_1, \ldots, x_n, z) \in \omega\big) \Rightarrow y = z\Big).$$

(2) Číslo n nazýváme arita nebo četnost operace ω.

(3) Poznámka: $\omega \subseteq M^{n+1}$. Podmínka jednoznačnosti vyjadřuje, že ω je zobrazení $M^n \to M$.

(4) Pro $n = 0$ říkáme, že ω je nulární a ω je jednoprvková množina.

(5) Pro $n = 1$ říkáme, že ω je unární.

(6) Pro $n = 2$ říkáme, že ω je binární a značíme $\omega(x_1, x_2) =: x_1 \omega x_2$.

(7) Pro $n = 3$ říkáme, že ω je ternární.

▶ 4.0.2. Definice.

(1) Algebra je uspořádaná dvojice $\mathcal{A} = (M, \Omega)$, kde $M \neq \emptyset$ je nosič algebry $\mathcal{A}$ a Ω je neprázdná množina algebraických operací.

(2) Pro nosič používáme značku $M =: \mathcal{A}^\bullet$, ale často také jen $M =: \mathcal{A}$.

(3) Je-li Ω konečná, $\Omega = \{\omega_1, \ldots, \omega_k\}$, značíme $\mathcal{A} = (M, \omega_1, \ldots, \omega_k)$.

(4) Je-li M konečná, pak počet prvků M značíme $|M|$ a nazýváme jej řád algebry $\mathcal{A}$.

---

5. Teorie grup

5.1. Grupoid. Pologrupa

▶ 5.1.1. Definice. Algebru $G = (M, \omega)$ s binární operací ω nazýváme grupoid. Operaci ω obvykle značíme $\cdot$, a říkáme multiplikativní grupoid, nebo $+$, a říkáme aditivní grupoid.

▶ 5.1.2. Definice. Grupoid $G = (M, \cdot)$ je pologrupa, platí-li asociativní zákon: $(\forall a, b, c \in M)((ab)c = a(bc))$.

▶ 5.1.3. Definice. Definujeme standardní součin: $(a_1) = a_1$; $(a_1 a_2) = a_1 \cdot a_2$; $(a_1 \ldots a_n\, a_{n+1}) = (a_1 \ldots a_n) a_{n+1}$.

▶ 5.1.4. Lemma. Platí-li asociativní zákon, pak platí i zobecněný asociativní zákon:

$$\big(\forall m,n\in\mathbb{N}\big)\big(\forall a_i\in M\big)\big((a_1\dots a_m)(a_{m+1}\dots a_{m+n})=(a_1\dots a_{m+n})\big).$$

◦ *Důkaz.* Důkaz provedeme matematickou indukcí podle n.

$(n=1)$ Plyne z definice standardního součinu.

$(n\to n+1)$ $(a_1\dots a_m)(a_{m+1}\dots a_{m+n}\,a_{m+n+1})=(a_1\dots a_m)((a_{m+1}\dots a_{m+n})a_{m+n+1})=$
$((a_1\dots a_m)(a_{m+1}\dots a_{m+n}))a_{m+n+1}=(a_1\dots a_{m+n})a_{m+n+1}=(a_1\dots a_{m+n+1})$.

□

▶ 5.1.5. Definice. Grupoid $G=(M,\cdot)$ je komutativní grupoid, platí-li komutativní zákon: $(\forall a,b\in M)(ab=ba)$.

▶ 5.1.6. Definice. $\mathbb{S}_n$ je množina všech permutací množiny $\widehat{n}$.

▶ 5.1.7. Lemma. V komutativní pologrupě platí zobecněný komutativní zákon:

$$(\forall n\in\mathbb{N})(\forall\pi\in\mathbb{S}_n)(a_1\dots a_n=a_{\pi(1)}\dots a_{\pi(n)})$$

◦ *Důkaz.* Platí, že každé $\pi\in\mathbb{S}_n$ je konečným složením sousedních transpozicí. □

▶ 5.1.8. Definice. V pologrupě definujeme pro $a\in M$ a $n\in\mathbb{N}_0$ přirozenou mocninu:

$$a^n:=\underbrace{a\cdot a\cdot\dots\cdot a}_{n\text{-krát}}.$$

V multiplikativní pologrupě používáme označení $n\times a$.

▶ 5.1.9. Příklad.

(1) Číselné pologrupy: nosičem je vždy podmnožina $\mathbb{C}$, operace jsou přirozené operace na číslech, tj. $(+)$ nebo $(\cdot)$.

(a) $(\mathbb{Z},+)$ je komutativní pologrupa nazývaná aditivní pologrupa celých čísel.

(b) $(\mathbb{Z},\cdot)$ je komutativní pologrupa nazývaná multiplikativní pologrupa celých čísel.

(c) $(\mathbb{N},\cdot)$ je komutativní pologrupa.

(2) $(\mathbb{Z},-)$ je grupoid.

(3) Nechť $A\neq\emptyset$ a $M=\{f:A\to A\}$ a $\omega=\circ$ je operace složení zorazení. Pak $(M,\circ)$ je pologrupa (nekomutativní) a nazývá se symetrická pologrupa na A.

(4) $(\mathbb{C}^{n,n},\cdot)$ je pologrupa (nekomutativní).

▶ 5.1.10. Definice. Neutrálním prvkem grupoidu $G=(M,\cdot)$ rozumíme libovolný prvek $e\in M$ takový, že $(\forall a\in M)(ea=ea=a)$. Obyčejně značíme v multiplikativním grupoidu $e=:1$ a nazýváme jednotka a v aditivním $e=:0$ a nazýváme nula.

► 5.1.11. Lemma. Grupoid má nejvýše jeden neutrální prvek.

○ *Důkaz.* Nechť e_1, e_2 jsou neutrální prvky. Pak $e_1 = e_1 e_2 = e_2$. □

► 5.1.12. Definice. Nechť $G = (M, \cdot)$ je grupoid s jednotkou. Inverzním prvkem k $a \in M$ je prvek a^{-1} takový, že $a^{-1}a = aa^{-1} = 1$.

► 5.1.13. Lemma. V pologrupě s jednotkou má každý prvek nejvýše jeden inverzní.

○ *Důkaz.* Nechť a_1 a a_2 jsou inverzní k a. Pak $a_1 = a_1 1 = a_1(aa_2) = (a_1 a)a_2 = a_2$. □

► 5.1.14. Definice. Prvky, ke kterým existuje inverzní prvek, se nazývají invertibilní nebo regulární. V multiplikativním grupoidu používáme název opačný prvek a značku $-a$.

► 5.1.15. Definice. Řekneme, že v grupoidu $G = (M, \cdot)$ lze dělit, platí-li, že

$$(\forall a, b \in M)(\exists x, y \in M)(ax = b \ \wedge \ ya = b).$$

► 5.1.16. Definice. Řekneme, že v grupoidu $G = (M, \cdot)$ lze krátit, platí-li, že

$$(\forall a, b, c \in M)\big((ac = bc \vee ca = cb) \Rightarrow a = b\big).$$

► 5.1.17. Příklad. V pologrupě $(\mathbb{N}, +)$ lze krátit, neboť $a + c = b + c \Rightarrow a = b$, ale nelze dělit, neboť $a + x = b$ nemá vždy řešení. Má tedy smysl pojmy zavádět nezávisle, neboť krácení a dělení ze sebe nevyplývají.

• 5.2. Grupa

► 5.2.1. Definice. Pologrupa G, ve které lze dělit, se nazývá grupa. Je-li navíc G komutativní, nazývá se Abelova grupa.

► 5.2.2. Věta. V libovolné grupě existuje jednotka a každý prvek má inverzní.

○ *Důkaz.*

(existence jednotky) Víme, že $(\forall a, b)(\exists x, y)(ax = b \wedge ya = b)$. Tedy pro konkrétní a existuje e tak, že $ae = a$. Ukážeme, že e je jednotka. Mějme libovolné $b \in M$. Pak $(\exists y)(ya = b)$ a $be = (ya)e = y(ae) = ya = b$. Tedy e je univerzální pravá jednotka. Symetricky ukážeme existenci univerzální levé jednotky e'. Platí $e' = e'e = e =: 1$, tedy existuje jen jedna jednotka a je pravá i levá.

(invertibilita) Označme a_P řešení $ax = 1$ a a_L řešení $ya = 1$. Pak $a_L = a_L 1 = a_L(aa_P) = (a_L a)a_P = 1a_P = a_P$. Tedy existuje inverzní a je jeden.

□

► 5.2.3. Věta. Nechť G je pologrupa, ve které existuje pravá jednotka e a libovolný prvek a má zprava inverzní prvek a^{-1} vzhledem k e. Pak G je grupa (tj. lze v G dělit).

◦ *Důkaz.*

$$ea = eae = eaa^{-1}(a^{-1})^{-1} = ee(a^{-1})^{-1} = e(a^{-1})^{-1} = aa^{-1}(a^{-1})^{-1} = ae = a,$$

tedy e je i levou jednotkou. □

► 5.2.4. DEFINICE. V grupě definujeme pro $a \in G^\bullet$ a pro $n \in \mathbb{Z}$ celou mocninu:

(1) a^n definované dříve;

(2) $a^0 := 1$;

(3) $a^{-n} := (a^{-1})^n = (a^n)^{-1}$.

V aditivní grupě $G = (G^\bullet, +)$ používáme pro $n \geq 1$ zápis $n \times a := \underbrace{a + \cdots + a}_{n\text{-krát}}$.

► 5.2.5. LEMMA. V libovolné grupě platí $(a^n)^l = a^{nl}$, v Abelově grupě navíc $(ab)^n = a^n b^n$.

► 5.2.6. PŘÍKLAD.

(1) $Z = (\mathbb{Z}; +)$ je aditivní grupa celých čísel a je Abelova.

(2) $(\mathbb{Q} \setminus \{0\}, \cdot)$ je multiplikativní grupa nenulových racionálních čísel a je Abelova.

(3) Odbobně pro $\mathbb{R} \setminus \{0\}$ a $\mathbb{C} \setminus \{0\}$.

(4) Nechť $A \neq \emptyset$, $M = \{f : A \xrightarrow{\text{bij.}} A\}$. Pak $(M, \circ)$ je grupa nazývaná symetrická grupa na A. Jednotkou je identické zobrazení a inverzním prvkem k f je f^{-1}.

(5) Symetrickou grupu na $\widehat{n}$ značíme $\mathbb{S}_n$.

(6) $E = (\{1\}, \cdot)$ je nejmenší možná grupa nazývaná triviální grupa.

(7) Pro $n \in \mathbb{N}$ a pro $k \in \widehat{n}$ definujeme $a_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ a nazýváme je komplexní n-té odmocniny z 1. Platí $a_k a_l = a_{k+l}$ (nebo $a_k a_l = a_{k+l-n}$ pokud $k + l > n$). Jednotka je $1 = a_n$ a $a_k^{-1} = a_{n-k}$. Označme $\sqrt[n]{1} = \{a_k \mid k \in \widehat{n}\}$. Pak $(\sqrt[n]{1}, \cdot)$ je Abelova grupa.

(8) Nechť V je vektorový prostor. Pak $(V, +)$ je Abelova grupa.

► 5.2.7. DEFINICE. Pologrupa s jednotkou se nazývá monoid.

► 5.2.8. PŘÍKLAD. Monoid slov. Nechť $\mathbb{A} \neq \emptyset$ je abeceda. Pak $\alpha = a_1 \dots a_n$ je slovo. Označme $\mathbb{A}^+$ množinu všech neprázdných slov, ε prázdné slovo a $\mathbb{A}^* = \mathbb{A}^+ \cup \{\varepsilon\}$ množinu všech slov. Definujme operaci zřetězení $\circ$ tak, že $\alpha \circ \beta = a_1 \dots a_n\, b_1 \dots b_m$. Pak $(\mathbb{A}^+, \circ)$ je pologrupa a $(\mathbb{A}^*, \circ)$ je monoid.

• 5.3. PODGRUPA

► 5.3.1. DEFINICE. Nechť $G = (M, \cdot)$ je grupa. Řekneme, že množina $N \subseteq M$, $N \neq \emptyset$ je uzavřená v G, platí-li:

$$(\forall a, b \in N)(ab^{-1} \in N).$$

▶ 5.3.2. Lemma. Je-li N uzavřená v $G = (M, \cdot)$, pak je $H = (N, \cdot)$ grupa.

◦ *Důkaz.* Ukážeme, že H splňuje základní vlastnosti grupy:

(existence jednotky) Vezmu libovolné pevné $a \in N$ a položím $b := a$. Pak vím, že $aa^{-1} = 1 \in N$.

(invertibilita) K libovolnému $b \in N$ položím $a := 1$. Pak vím, že $1b^{-1} = b^{-1} \in N$.

(uzavřenost vůči operaci) K libovolným $a, c \in N$ položím $b := c^{-1}$. Pak vím, že $ab^{-1} = ab \in N$.

□

▶ 5.3.3. Definice. H definované v předchozím lemmatu nazýváme podgrupa grupy G a značíme $H \Subset G$.

▶ 5.3.4. Lemma. $G \Subset G$, $E \Subset G$.

▶ 5.3.5. Definice. Netriviální podgrupa je taková $H \Subset G$, že platí $H \neq G$ a $H \neq E$.

▶ 5.3.6. Věta. Buď $G = (M, \cdot)$ grupa a pro $i \in I$ buď $H_i = (N_i, \cdot)$ systém jejích podgrup. Potom $H := \bigcap_{i \in I} H_i = \left(\bigcap_{i \in I} N_i, \cdot \right) \Subset G$.

◦ *Důkaz.* Nezbytně $1 \in H_i$ tedy $H \neq \emptyset$. $(\forall a, b \in H)(\forall i \in I)(a, b \in H_i) \Rightarrow (\forall a, b \in H)(ab^{-1} \in H_i) \Rightarrow ab^{-1} \in H$. □

▶ 5.3.7. Definice. Mějme $G = (M, \cdot)$ a $a \in M$. Pak označujeme $\langle a \rangle$ nejmenší podgrupu (ve smyslu inkluze) grupy G obsahující a, tj. $\langle a \rangle = \bigcap_{\substack{H \Subset G \\ a \in H,}} H$.

▶ 5.3.8. Lemma. $\langle a \rangle = \left\{ a^k \;\middle|\; k \in \mathbb{Z} \right\}$.

◦ *Důkaz.* Je uzavřená vůči testovací podmínce, je podgrupou a je zjevně nejmenší. □

▶ 5.3.9. Definice. Nechť $G = (M, \cdot)$ je grupa, $N \subseteq M$ libovolná její podmnožina. Pak definujeme podgrupu generovanou N jako $\langle N \rangle = \bigcap \{ H \Subset G \mid N \subseteq H^\bullet \}$. Množinu N nazýváme generátor $\langle N \rangle$.

▶ 5.3.10. Lemma. $\langle N \rangle^\bullet = \left\{ a_1^{k_1} \cdots a_n^{k_n} \;\middle|\; n \in \mathbb{N}_0, a_i \in N, k_i \in \mathbb{Z} \right\} =: K$.

◦ *Důkaz.* Zjevně nemůže být $\langle N \rangle^\bullet$ menší, stačí tedy ukázat, že K je podgrupou: Nechť $a = a_1^{k_1} \cdots a_n^{k_n} \in K$ a $b = b_1^{\ell_1} \cdots b_m^{\ell_m} \in K$ a potom $ab^{-1} = a_1^{k_1} \cdots a_n^{k_n} \, b_m^{-\ell_m} \cdots b_1^{-\ell_1}$. □

▶ 5.3.11. Definice.

(1) Nechť $H, K \Subset G$. Pak definujeme součin podgrup $H \cdot K = \langle H^\bullet \cup K^\bullet \rangle$.

(2) Nechť pro všechna $i \in I$ je $H_i \Subset G$. Pak definujeme $\prod_{i\in I} H_i = \left\langle \bigcup_{i\in I} H_i^\bullet \right\rangle$.

▶ 5.3.12. Příklad.

(1) Nechť S je množina sudých celých čísel. Pak $(S, +) \Subset (\mathbb{Z}, +)$ je netriviální podgrupa. Ověříme uzavřenost: $(\forall a, b \in S)(a - b \in S)$, což ale zjevně platí.

(2) $\mathcal{S}_n$ je grupa permutací $\widehat{n}$, nechť $\mathcal{A}_n$ je množina všech sudých permutací (přesná definice dále). Pak všechna $\pi, \sigma \in \mathcal{A}_n$ jsou složením sudého počtu transpozicí a inverze vznikne přečtením transpozic pozpátku. Tedy $(\mathcal{A}_n, \circ) \Subset (\mathcal{S}_n, \circ)$, kterou nazýváme alternující grupa.

$|\mathcal{S}_n| = n!$; pro $n \geq 2$ je $|\mathcal{A}_n| = n!/2$.

(3) $(\sqrt[n]{1}, \cdot) \Subset (\mathbb{C}, \cdot)$.

• 5.4. Řád prvku grupy

▶ 5.4.1. Definice. Buď $G = (M, \cdot)$ grupa, $a \in M$.

(1) a má nekonečný řád, pokud $(\forall k, \ell \in \mathbb{Z}, k \neq \ell)(a^k \neq a^\ell)$.

(2) Nemá-li a nekonečný řád, pak má konečný řád a řádem prvku a rozumíme $\min\{r \in \mathbb{N} \mid a^r = 1\}$.

▶ 5.4.2. Lemma. Nechť $a \in G$ má řád r a pro nějaké $k \in \mathbb{Z}$ je $a^k = 1$. Pak $r \mid k$.

◦ *Důkaz.* V celých číslech platí princip dělení se zbytkem (důkladně probereme níže):

$$(\forall k, r \in \mathbb{Z}, r \neq 0)(\exists \ell, R \in \mathbb{Z}, 0 \leq R < r)(k = r\ell + R).$$

Platí $a^R = a^k (a^r)^{-\ell} = 1$, tedy $R \in \mathbb{N}$ a $R < r$, což je spor s tím, že r je řád a. Tedy $R = 0$ a $r \mid k$. □

▶ 5.4.3. Definice. Buď $G = (M, \cdot)$ grupa. Řekneme, že G je

(1) periodická/torzní, má-li libovolný její prvek konečný řád.

(2) bez torze, pokud má každý prvek různý od 1 nekonečný řád.

(3) smíšená v ostatních případech.

▶ 5.4.4. Lemma. Libovolná konečná grupa je periodická.

► 5.4.5. Příklad. Ukážeme, že nekonečné grupy mohou být periodické, bez torze i smíšené.

(1) Označme $G_n = (\sqrt[n]{1}, \cdot)$ a $M = \bigcup_{n\in\mathbb{N}} G_n = \{\cos 2q\pi + i \sin 2q\pi \mid q \in \mathbb{Q}\}$. Pak M je uzavřená v $(\mathbb{C}, \cdot)$: $a, b \in M$, $a \in G_k$, $b \in G_\ell$. $(ab^{-1})^{kl} = (a^k)^\ell (b^\ell)^{-k} = 1 \cdot 1 = 1$, tedy $ab^{-1} \in G_{k\ell}$. Zjevně $(M, \cdot)$ je nekonečná grupa a řád prvku $a \in G_k$ je nejvýše roven k. Tedy $(M, \cdot)$ je nekonečná a periodická.

(2) $(\mathbb{Z}, +)$ je zjevně bez torze, neboť pro $z \in \mathbb{Z}$ je $k \times n = 0 \Leftrightarrow z = 0$.

(3) $(\mathbb{C}, \cdot)$ je smíšená, neboť $(M, \cdot) \Subset (\mathbb{C}, \cdot)$ je periodická a např. číslo $2 \in \mathbb{C}$ má nekonečný řád.

► 5.4.6. Věta (algoritmus dělení, o dělení se zbytkem).

$$(\forall k, \ell \in \mathbb{Z}, \ell \neq 0)(\exists_1 q, r \in \mathbb{Z})(k = q\ell + r \ \wedge \ 0 \leq r < |\ell|).$$

◦ *Důkaz.*

(existence) Položme $q' := \left\lfloor \frac{k}{|\ell|} \right\rfloor$, tedy $q' \leq \frac{k}{|\ell|} < q' + 1$. Pak $q' |\ell| \leq k < q' |\ell| + |\ell|$, tedy pro $r := k - q' |\ell|$ platí $0 \leq r < |\ell|$. Položme $q := q' \operatorname{sgn} \ell$, pak platí $q\ell + r = q'\ell \operatorname{sgn} \ell + r = q' |\ell| + k - q' |\ell| = k$.

(jednoznačnost) Mějme druhou dvojici $\tilde{q}, \tilde{r}$ splňující tvrzení věty a pro spor nejprve předpokládejme, že $q \neq \tilde{q}$. Potom $|\tilde{r} - r| = |(k - \tilde{q}\ell) - (k - q\ell)| = |q\ell - \tilde{q}\ell| = |\ell| \, |q - \tilde{q}| \geq |\ell| \cdot 1$. Ale $(\forall q_1, q_2 \in \mathbb{Z}, 0 \leq q_{1,2} \leq |\ell| - 1)(|q_1 - q_2| \leq |\ell| - 1)$, což je spor. Tedy $q = \tilde{q}$ a $r = k - q\ell = k - \tilde{q}\ell = \tilde{r}$.

□

► 5.4.7. Definice. Největší společný dělitel $k, \ell \in \mathbb{Z}$ je takové $d \in \mathbb{Z}$, že:

(1) $d \mid k$, $d \mid \ell$;

(2) $d' \mid k \wedge d' \mid \ell \Rightarrow d' \mid d$.

► 5.4.8. Poznámka. Je-li číslo d největší společný dělitel, pak i číslo $-d$ je největší společný dělitel.

► 5.4.9. Věta. K libovolným číslům $k, \ell \in \mathbb{Z}$ existuje největší společný dělitel d a existují $u, v \in \mathbb{Z}$ takové, že

$$d = uk + v\ell.$$

◦ *Důkaz.* Nechť $k, \ell \neq 0$. Označme $D := \{uk + v\ell \mid u, v \in \mathbb{Z}\} \subseteq \mathbb{Z}$. Množina D je uzavřená na součty a $\mathbb{Z}$-násobky. Definujme $d := \min\{x \in D \mid x > 0\}$ a ukážeme, že je největší společný dělitel.

$k = dq + r$, kde $q \in \mathbb{Z}$ a $0 \leq r < d$. $r = k - dq$, kde $k \in D$ a $dq \in D$, tedy $r \in D$ a $r < d$, tedy musí $r = 0$, jinak by $r > 0 \wedge r < d$. Tedy $d \mid k$ a sjeným postupem $d \mid \ell$.

Nechť $d' \mid k$ a $d' \mid \ell$. Z toho vyplývá, že d' dělí všechna čísla v D, tedy i $d' \mid d$. □

▶ 5.4.10. Definice. Nezáporný největší společný dělitel k a ℓ budeme značit $\delta(k,\ell)$. Řekneme, že k a ℓ jsou nesoudělná, když $\delta(k,\ell)=1$.

▶ 5.4.11. Definice. Nejmenší společný násobek čísel k a ℓ označujeme $\nu(k,\ell)$ a je to nejmenší takové $m\in\mathbb{N}$, že $k\mid m$ a $\ell\mid m$.

• 5.5. Cyklické grupy

▶ 5.5.1. Definice. Řekneme, že grupa G je cyklická, je-li rovna některé ze svých cyklických podgrup, tedy $(\exists a\in G)(G=\langle a\rangle=\{a^n\mid n\in\mathbb{Z}\})$. Prvek a nazýváme generátor grupy G.

▶ 5.5.2. Lemma.

(1) Každá cyklická grupa je Abelova.

(2) Každá cyklická grupa je nejvýše spočetná.

▶ 5.5.3. Příklad.

(1) $Z=(\mathbb{Z},+)$ je nekonečná cyklická grupa generovaná prvkem 1 nebo -1:

$$Z=(\mathbb{Z},+)=\langle 1\rangle=\langle -1\rangle\,.$$

(2) Pro každé $n\in\mathbb{N}$ je $\sqrt[n]{1}$ konečná cyklická grupa s řádem n, generátorem je např. $a_1=\cos\frac{2\pi}{n}+i\sin\frac{2\pi}{n}$.

▶ 5.5.4. Věta. Libovolná podgrupa cyklické grupy je cyklická.

◦ *Důkaz.* $G=\langle a\rangle, H\leqslant G$. Pro $H=E$ je generátorem jednotka. Označme $p=\min\{i\in\mathbb{N}\mid a^i\in H\}$. Ukážeme, že $\langle a^p\rangle=H$.

$(\subseteq)$ Zřejmé.

$(\supseteq)$ Vezměmě libovolné $x\in H$. Pak $(\exists q\in\mathbb{Z})(x=a^q)$. Označme $d=\delta(p,q)=up+vq$. Potom $a^d=a^{up+vq}=(a^p)^u\cdot(a^q)^v\in H$. p je nejmenší, tedy $d\geq p$, ale $d\mid p$, tedy $d\leq p$, což dohromady dává $p=d$. Současně $d\mid q$, tedy $q=pr$ a $a^q=(a^p)^r\in\langle a^p\rangle$.

□

▶ 5.5.5. Lemma. Nekonečná cyklická grupa $\langle a\rangle$ má právě 2 generátory, a to a a a^{-1}.

▶ 5.5.6. Věta. Buď $G=\langle a\rangle$ cyklická grupa řádu n, a nechť $1\leq k\leq n$. Potom a^k generuje G právě tehdy, když jsou k a n nesoudělná.

◦ *Důkaz.*

$(\Rightarrow)$ $G=\langle a^k\rangle$. Tedy $a=\left(a^k\right)^u$. Z toho vyplývá, že $a^{ku-1}=1$. Každý generátor má řád n, tedy a má řád n, tedy $ku-1=vn$, tedy $uk-vn=1$, tedy $\delta(k,n)=1$.

$(\Leftarrow)$ Z nesoudělnosti existují u, v tak, že $uk+vn=1$. Dále $a=a^1=a^{uk+vn}=\left(a^k\right)^u(a^n)^v=\left(a^k\right)^u 1^v=\left(a^k\right)^u$. Tedy pro libovolné $x\in G$ je $x=a^r=\left(a^{uk}\right)^r$.

□

▶ 5.5.7. Definice. Definujeme Eulerovu funkci $\phi : \mathbb{N} \to \mathbb{N}$, kde $\phi(n)$ je počet čísel z $\widehat{n}$ nesoudělných s n.

▶ 5.5.8. Lemma. n je prvočíslo právě tehdy, když $\phi(n) = n - 1$.

• 5.6. Kongruence

▶ 5.6.1. Definice. Mějme grupoid $G = (M, \cdot)$ a mějme ekvivalneci $\equiv$ na M. Pak pro libovolné $x \in M$ definujeme T_x jako třídu ekvivalence podle $\equiv$, která obsahuje x, tedy $x \in T_x \in M/\equiv$ (korektnost je zajištěna disjunktností tříd ekvivalence).

▶ 5.6.2. Definice. Buďte $G = (M, \cdot)$ grupoid a $\equiv$ ekvivalence na G. Řekneme, že $\equiv$ je kongruence na G, platí-li, že

$$\big(\forall a, b, c, d \in M\big)\big((a \equiv b \wedge c \equiv d) \Rightarrow ac \equiv bd\big).$$

▶ 5.6.3. Definice. Buďte $G = (M, \cdot)$ grupoid a $\equiv$ kongruence na G. Pak definujeme součin tříd ekvivalence $M/\equiv$ jako $T_a \cdot T_b = T_{ab}$. (Korektnost definice je zajišťena definující vlastností kongruence.)

▶ 5.6.4. Definice. Buďte $G = (M, \cdot)$ grupoid a $\equiv$ kongruence na M. Pak definujeme faktorgrupoid G jako $G/\equiv := (M/\equiv, \cdot)$

▶ 5.6.5. Věta. Buďte $G = (M, \cdot)$ grupod a $\equiv$ kongruence na M. Pak $G/\equiv$ je pologrupa, resp. je komutativní, resp. má jednotkou, resp. je grupa, má-li odpovídající vlastnost i G.

◦ *Důkaz.* Všechny body jsou obdobné, ukážeme asociativitu (pologupa). Nechť $T_a, T_b, T_c \in M/\equiv$. Pak $(T_aT_b)T_c = T_{ab}T_c = T_{(ab)c} = T_{a(bc)} = T_aT_{bc} = T_a(T_bT_c)$. □

▶ 5.6.6. Definice. Mějme $Z = (\mathbb{Z}, +)$ a libovolné $m \in \mathbb{Z}$. Pak definujeme kongruenci modulo m (značíme $\equiv_m$) následovně:

$$a \equiv_m b \iff (\exists s \in \mathbb{Z})(a - b = sm).$$

Třídy $Z/\equiv_m$ se nazývají zbytkové třídy po dělení m. Faktorgrupu $Z/\equiv_m$ označujeme Z_m.

▶ 5.6.7. Lemma. Relace $\equiv_m$ je kongruence na Z.

◦ *Důkaz.* Ukážeme, že $\equiv_m$ je ekvivalence a splňuje definiční podmínku kongruence.

(reflexivita) Platí $a - a = 0 = 0m$.

(symetrie) Nechť $a - b = sm$. Pak $b - a = -sm = (-s)m$.

(tranzitivita) Nechť $a-b = sm$ a $b-c = tm$. Pak $a-c = (a-b)+(b-c) = sm+tm = (s+t)m$.

(konguence) Nechť $a - b = sm$ a $c - d = tm$. Pak $(a + c) - (b + d) = sm + tm = (s + t)m$.

□

▶ 5.6.8. Příklad.

($m = 0$) $a \equiv_0 b \Leftrightarrow 0 \mid a - b \Leftrightarrow a = b$, tedy každý prvek má svou jednoprvkovou třídu.

($m = 1$) $a \equiv_1 b \Leftrightarrow 1 \mid a - b$, tedy všechny prvky leží ve stejné třídě.

▶ 5.6.9. Lemma. Pro $m \geq 1$ platí, že dvě celá čísla jsou v jedné třídě $\mathbb{Z} / \equiv_m$ právě tehdy, když dávají stejný zbytek po dělení m. Tedy tříd ekvivalence podle $\equiv_m$ je m.

◦ *Důkaz.*

($\Rightarrow$) $a_1, a_2 \in \mathbb{Z}$, $a_1 \equiv_m a_2$. Pak $a_1 = mq_1 + r_1$, $a_2 = mq_2 + r_2$ a $a_1 - a_2 = sm$. Odečtením prvních dvou máme $a_1 - a_2 = m(q_1 - q_2) + (r_1 - r_2) = sm$, $r_1 - r_2 = m(q_1 - q_2 - s)$, tedy $m \mid r_1 - r_2$, ale protože $0 \leq r_{1,2} < m$, je nutně $r_1 = r_2$.

($\Leftarrow$) Víme, že $r_1 = r_2$, tedy $a_1 - a_2 = m(q_1 - q_2)$, tedy $s = q_1 - q_2$ a $a_1 \equiv_m a_2$.

($|\mathbb{Z} / \equiv_m| = m$) Toto je zjevné z předchozího.

□

▶ 5.6.10. Lemma. Faktorgrupa Z_m grupy Z podle $\equiv_m$ je cyklická s generátorem T_1, tedy $Z_m = \langle T_1 \rangle$.

• 5.7. Homomorfismus

▶ 5.7.1. Definice. Buďte $G_1 = (M_1, \cdot)$, $G_2 = (M_2, \cdot)$ grupoidy. Řekneme, že $h : M_1 \to M_2$ je homomorfismus grupoidů, pokud platí:

$$(\forall x, y \in M_1)\big(h(xy) = h(x)h(y)\big)$$

a budeme též značit $h : G_1 \to G_2$.

▶ 5.7.2. Definice. Homomorfismus h se nazývá:

(1) monomorfismus, je-li prostý (injekce);

(2) epimorfismus, je-li na (surjekce);

(3) izomorfismus, je-li prostý a na (bijekce);

(4) endomorfismus, je-li $G_1 = G_2$.

(5) automorfismus, je-li izomorfní endomorfismus (bijekce $G \to G$).

▶ 5.7.3. Definice. Existuje-li izomorfismus $h : G_1 \to G_2$, nazýváme grupoidy izomorfní a značíme $G_1 \cong G_2$.

▶ 5.7.4. Příklad. $G_1 := (\mathbb{R}^+, \cdot)$, $G_2 := (\mathbb{R}, +)$. Definujeme $h : G_1^\bullet \to G_2^\bullet$ jako $h(x) = \ln x$. Zjevně $h(xy) = h(x) + h(y)$, tedy h je morfismus a z analýzy víme, že je bijekcí. Tedy $G_1 \cong G_2$.

▶ 5.7.5. DEFINICE. Mějme $G = (M, \cdot)$ grupu a kongruenci $\equiv$ na G. Definujeme přirozené zobrazení (přirozený epimorfismus) $h_{\text{nat}} : G \to G / \equiv$ jako $h_{\text{nat}}(x) = T_x$.

▶ 5.7.6. LEMMA. h_{nat} je epimorfismus.

◦ *Důkaz.* Platí $h_{\text{nat}}(xy) = T_{xy} = T_x T_y = h_{\text{nat}}(x) h_{\text{nat}}(y)$, tedy h je homomorfismus. Současně pro každou třídu T_x platí $T_x = h_{\text{nat}}(x)$, tedy je na. □

▶ 5.7.7. VĚTA. Libovolné 2 nekonečné cyklické grupy jsou izomorfní. Libovolné 2 cyklické grupy s počtem prvků $n \in \mathbb{N}$ jsou izomorfní.

◦ *Důkaz.* Mějme libovolnou $G = \langle a \rangle$ nekonečnou. Ukážeme, že $G \cong Z = (\mathbb{Z}, +)$. Definujeme $h : G \to Z$ jako $h(a^n) = n \times 1 = n$. Pak h je prosté zobrazení ($m \neq n \Leftrightarrow a^m \neq a^n$), a neboť je G nekonečná, je na. Operace $\cong$ na grupách je ekvivalencí, tedy pro libovolné G_1, G_2 je $G_1 \cong Z$ a $G_2 \cong Z$, tedy $G_1 \cong G_2$. □

▶ 5.7.8. DEFINICE. Nechť $G = (M, \cdot)$ je grupoid, $N \subseteq M$. Pak $H = (N, \cdot)$ nazveme podgrupoid grupoidu G, pokud je H grupoid, tedy $(\forall x, y \in H)(xy \in H)$. Značíme $H \Subset G$.

▶ 5.7.9. LEMMA. Buďte G_1, G_2 grupoidy, $h : G_1 \to G_2$ homomorfismus. Pak $h(G_1) \Subset G_2$.

▶ 5.7.10. VĚTA (O HOMOMORFISMU). Buďte G_1, G_2 grupoidy, $h : G_1 \to G_2$ homomorfismus. Pak existuje kongruence (označovaná $\equiv_h$) na G_1 taková, že $h(G_1) \cong G_1 / \equiv_h$, kde $h(G_1)$ značí obor hodnot h.

◦ *Důkaz.* Definujeme $\equiv_h$ jako $x \equiv_h y \Leftrightarrow h(x) = h(y)$, tedy $\equiv_h$ je zjevně ekvivalence (je definovaná pomocí rovnosti) Nechť $a \equiv_h b$ a $c \equiv_h d$. Pak $h(ac) = h(a)h(c) = h(b)h(d) = h(bd)$, tedy $ac \equiv_h bd$ a $\equiv_h$ je kongruence.

Definujeme $g : G_1 / \equiv_h \to h(G_1)$ jako $g(T_x) = h(x)$. Definice je korektní, neboť $T_x = T_y \Leftrightarrow h(x) = h(y)$, z tohotéž vyplývá, že g je prosté. Z definice g pomocí h plyne, že pokryje celé $h(G_1)$, tedy je na. Je homomorfismus, neboť $g(T_x T_y) = g(T_{xy}) = h(xy) = h(x)h(y) = g(T_x)g(T_y)$. □

▶ 5.7.11. POZNÁMKA. Všimněme si, jak souvisí korektnost definice s prostotou. Pokud by bylo $T_x = T_y$ a zároveň $h(x) \neq h(y)$, pak definice není korektní. Pokud by bylo $h(x) = h(y)$ a zároveň $T_x \neq T_y$, pak zobrazení není prosté.

▶ 5.7.12. VĚTA. Nechť $h : G_1 \to G_2$ je homomorfismus grupoidů a buď g zobrazení definované v důkazu předchozí věty. Pak $h_{\text{nat}} = g^{-1} h$.

▶ 5.7.13. VĚTA. Buďte G_1, G_2 grupoidy, $h : G_1 \to G_2$ homomorfismus. Je-li G_1 pologrupa, resp. je komutativní, resp. má jednotku, resp. je grupa, má tutéž vlastnost i grupoid $h(G_1)$.

◦ *Důkaz.* Dukaz všech bodů je obdobný, ukážeme přenos jednotky. Nechť $1 \in G_1$, pak $h(1)$ je jednotkou v $h(G_1)$. Neboť pro libovolné $y \in h(G_1)$ existuje $x \in G_1$ takové, že $y = h(x)$. Potom $yh(1) = h(x)h(1) = h(x1) = h(x) = y$. Podobně zleva. □

▶ 5.7.14. Definice. Buď $G = (M, \cdot)$ grupa, $A, B \subseteq M$. Pak definujeme součin podmnožin $A \cdot B$ jako $A \cdot B := \{ab \mid a \in A, b \in B\}$. (vztah mezi součinem podmnožin a podgrup osvětlíme později). Je-li $B = \{b\}$, pak značíme $AB = Ab = \{xb \mid x \in A\}$.

▶ 5.7.15. Definice. Buď $H \Subset G$ podgrupa grupy, definujeme následující 2 relace:

(1) $a \ {}_H\!\equiv b \Leftrightarrow b^{-1}a \in H$;

(2) $a \equiv_H b \Leftrightarrow ab^{-1} \in H$;

které nazýváme levá, resp. pravá ekvivalence indukovaná podgrupou H.

▶ 5.7.16. Lemma. Indukované relace jsou ekvivalence.

◦ *Důkaz.*

(reflexivita) $a \ {}_H\!\equiv a \Leftrightarrow a^{-1}a \in H$, ale $a^{-1}a = 1$.

(symetrie) $a \ {}_H\!\equiv b \Leftrightarrow b^{-1}a \in H^\bullet \Leftrightarrow (b^{-1}a)^{-1} = a^{-1}b \in H^\bullet \Leftrightarrow a \ {}_H\!\equiv b$.

(tranzitivita) $a \ {}_H\!\equiv b \wedge b \ {}_H\!\equiv c \Leftrightarrow b^{-1}a, c^{-1}b \in H^\bullet \Rightarrow c^{-1}bb^{-1}a \in H^\bullet \Rightarrow c^{-1}a \in H^\bullet \Leftrightarrow a \ {}_H\!\equiv c$.

Podobně lze ukázat totéž pro $\equiv_H$. □

▶ 5.7.17. Příklad. Zvolme $b = 1$. Pak $a \ {}_H\!\equiv 1 \Leftrightarrow a \in H$ a současně $a \equiv_H 1 \Leftrightarrow a \in H$, tedy H je jedna ze tříd ekvivalence podle obou indukovaných ekvivalencí.

▶ 5.7.18. Lemma. Označme T_a^L resp. T_a^P třídu ekvivalence podle ${}_H\!\equiv$, resp. $\equiv_H$ obsahující $a \in G^\bullet$. Potom $T_a^L = aH^\bullet$ a $T_a^P = H^\bullet a$.

◦ *Důkaz.* Opět lemma ukážeme pro levou ekvivalenci. T_a^L je třída ${}_H\!\equiv$ obsahující a. Mějme libovolné $x \in G$. Pak $x \in T_a^L \Leftrightarrow x \ {}_H\!\equiv a \Leftrightarrow a^{-1}x \in H^\bullet \Leftrightarrow (\exists h \in H^\bullet)(a^{-1}x = h) \Leftrightarrow (\exists h \in H^\bullet)(x = ah) \Leftrightarrow x \in aH^\bullet$. □

▶ 5.7.19. Věta.

(1) Libovolné 2 třídy rozhladů dle ${}_H\!\equiv$ či $\equiv_H$ jsou (množinově) ekvivalentní. („Každá třída má stejně prvků.“)

(2) Levý rozklad je (množinově) ekvivalentní s pravým rozkladem. („Levých a pravých tříd je stejný počet.“)

◦ *Důkaz.*

(1) Libovolné 2 levé třídy $aH^\bullet$ a $bH^\bullet$. Definujme $f : aH^\bullet \to bH^\bullet$ jako $f(x) = ba^{-1}x$. Nechť $x = ah$, pak $f(x) = bh \in bH^\bullet$ tedy definice je korektní. Mějme $y = bh$, pak $y = f(x) \Leftrightarrow ba^{-1}x \Leftrightarrow h = a^{-1}x \Leftrightarrow x = ah \in aH^\bullet$. Podobně dokážeme, že všechny pravé jsou ekvivalentní. Z tranzitivity a z toho, že $H^\bullet$ je v obou faktorizacích, vyplývá, že všechny levé třídy jsou ekvivalentní se všemi pravými.

(2) Definujeme $g : M /_H\!\equiv \to M /\!\equiv_H$ jako $g(aH^\bullet) = H^\bullet a^{-1}$. Zjevně je na, neboť a^{-1} projde celé G právě tehdy, když a projde celé G. Platí: $g(aH^\bullet) = g(bH^\bullet) \Leftrightarrow H^\bullet a^{-1} = H^\bullet b^{-1} \Leftrightarrow a^{-1} \equiv_H b^{-1} \Leftrightarrow a^{-1}b \in H^\bullet \Leftrightarrow (a^{-1}b)^{-1} = b^{-1}a \in H^\bullet \Leftrightarrow a \ {}_H\!\equiv b \Leftrightarrow aH^\bullet = bH^\bullet$, tedy g je prosté (směr $\Rightarrow$) a definice je korektní (směr $\Leftarrow$).

□

► 5.7.20. Definice. Počtu rozkladových tříd podle indukovaných ekvivalencí se říká index podgrupy H.

► 5.7.21. Věta (Lagrange). Součin řádu a indexu libovolné podgrupy H konečné grupy G je roven řádu G.

◦ *Důkaz.* Všechny třídy mají počet prvků, jako je řád H, a je jich tolik, jako je index H. □

► 5.7.22. Důsledek.

(1) Řád libovolné podgrupy konečné grupy G dělí řád G.

(2) Řád libovolného prvku konečné grupy G dělí řád G.

► 5.7.23. Důsledek. Má-li grupa G prvočíselný řád, je cyklická. Všechny grupy s prvočíselným řádem p jsou izomorfní.

◦ *Důkaz.* Grupa není triviální (má řád nejméně 2). Vezmu $a \neq 1$. Pak řád prvku a je p, (jednotkový řád má jen jednotka), tedy a generuje G. □

► 5.7.24. Definice. Buď G grupa. Řekneme, že podgrupa $H \Subset G$ je normální (invariantní), pokud ${}_H\!\equiv$ a $\equiv_H$ splývají, a značíme $H \lhd G$.

► 5.7.25. Lemma. $E \lhd G$; $G \lhd G$.

◦ *Důkaz.*

(1) $a \ {}_E\!\equiv b \Leftrightarrow b^{-1}a = 1 \Leftrightarrow a = b$; $a \equiv_E b \Leftrightarrow ab^{-1} = 1 \Leftrightarrow a = b$.

(2) $a \ {}_G\!\equiv b \Leftrightarrow b^{-1}a \in G$, což platí pro libovolné a, b; stejně tak pro $\equiv_G$.

□

► 5.7.26. Lemma. Je-li grupa G Abelova, je libovolná její podgrupa $H \Subset G$ normální.

► 5.7.27. Věta. Rozklad grupy G je rozkladem podle kongruence právě tehdy, je-li rozkladem podle některé normální podgrupy $H \lhd G$.

◦ *Důkaz.*

(⇒) Nechť $\equiv$ je kongruence na grupě $G = (M, \cdot)$. Vezměme třídu T_1 a $a, b \in T_1$. Pak $a \equiv 1$ a $b \equiv 1$, tedy $ab \equiv 1$. Také $a^{-1} \equiv a^{-1}$, tedy $1 \equiv a^{-1}$.

Ukážeme, že $H = (T_1, \cdot) \Subset G$ je normální. Vezměme lib. $x \in M$. Pak $x \in T_a \Leftrightarrow x \equiv a \Leftrightarrow xa^{-1} \equiv 1 \Leftrightarrow xa^{-1} \in H^\bullet \Leftrightarrow (\exists h \in H^\bullet)(xa^{-1} = h) \Leftrightarrow (\exists h \in H^\bullet)(x = ha) \Leftrightarrow x \in H^\bullet a$. Budeme-li násobit a^{-1} zleva, dostaneme $x \in aH^\bullet$. Tedy $T_a = aH^\bullet = H^\bullet a$, což znamená, že $H \lhd G$ a $(\equiv) = ({}_H\equiv) = (\equiv_H)$

(⇐) Nechť $H \lhd G$, ukážeme, že $\equiv_H$ je kongruence. Mějme $a, b, c, d \in M$ takové, že $a \equiv_H b$ a $c \equiv_H d$. Potom $ac(bd)^{-1} = acd^{-1}b^{-1}$. Označme $h := cd^{-1} \in H^\bullet$, pak existuje $h' \in H^\bullet$ takové, že $ah = h'a$. Tedy celkově dostáváme $ac(bd)^{-1} = ahb^{-1} = h'ab^{-1} \in h'H^\bullet = H$.

□

• 5.8. Vnitřní automorfismy

▶ 5.8.1. Definice. Nechť $\mathcal{A}^\bullet_G$ je množina všech automorfismů na G. Pak definujme $\mathcal{A}_G = (\mathcal{A}^\bullet_G, \circ)$.

▶ 5.8.2. Lemma. Nechť G je grupa. Pak $\mathcal{A}_G$ je grupa a $\mathcal{A}_G \Subset \mathcal{S}_G$.

◦ *Důkaz.* Součin (složení) 2 automorfismů je automorfismus, existuje jednotka (identita) a každý automorfismus má inverzní. Nechť $x, y \in G^\bullet$, $\alpha \in \mathcal{A}^\bullet_G$, pak $\alpha^{-1}(xy) = \alpha^{-1}(\alpha(\alpha^{-1}(x))\alpha(\alpha^{-1}(y))) = \alpha^{-1}(\alpha(\alpha^{-1}(x)\alpha^{-1}(y))) = \alpha^{-1}(x)\alpha^1(y)$, tedy inverzní je opět morfismem. □

▶ 5.8.3. Lemma. Nechť $a \in M$, $\alpha_a(x) = axa^{-1}$. Pak α_a je automorfismus.

◦ *Důkaz.*

(morfismus) Pro libovolné $x, y \in M$ platí $\alpha_a(x)\alpha_a(y) = axa^{-1}aya^{-1} = axya^{-1} = \alpha_a(xy)$.

(bijekce) Ukážeme, že $\alpha_{a^{-1}}$ je inverzní k α_a, tj. $(\forall x \in M)(\alpha_{a^{-1}}\alpha_a = \alpha_a\alpha_{a^{-1}} = \mathrm{id})$. Pro všechna $x \in M$ platí $(\alpha_{a^{-1}}\alpha_a)(x) = \alpha_{a^{-1}}(axa^{-1}) = a^{-1}axa^{-1}a = 1x1 = x$, obdobně $(\alpha_a\alpha_{a^{-1}})(x) = x$.

□

▶ 5.8.4. Definice. Automorfismus α na G je <u>vnitřní</u>, právě když $(\exists a \in G^\bullet)(\alpha(x) = axa^{-1})$. Takový automorfismus značíme α_a.

Označme $\mathcal{I}^\bullet_G$ množinu všech vnitřích automorfismů.

▶ 5.8.5. Lemma. $\mathcal{I}_G = (\mathcal{I}^\bullet_G, \circ) \Subset \mathcal{A}_G$ je grupa.

◦ *Důkaz.* Jednotkou je α_1, $\alpha_1(x) = 1x1^{-1} = x$. $(\alpha_a\alpha_b^{-1})(x) = ab^{-1}xba^{-1} = (ab^{-1})x(ab^{-1})^{-1} = \alpha_{ab^{-1}}(x)$ □

► 5.8.6. Věta. Podgrupa H grupy G je normální právě tehdy, je-li uzavřená vůči všem vnitřním automorfismům, tj.

$$H \lhd G \iff (\forall a \in G^\bullet)(\forall x \in H^\bullet)(\alpha_a(x) \in H^\bullet).$$

◦ *Důkaz.*

(⇒) Mějme $H \lhd G$ a libovolné $a \in G^\bullet$ a $x \in H^\bullet$. Pak $ax \in aH^\bullet = H^\bullet a \Rightarrow (\exists h \in H^\bullet)(ax = ha) \Rightarrow axa^{-1} \in H^\bullet$.

(⇐) Mějme libovolný $x \in aH^\bullet$, tedy $x = ah = aha^{-1}a = \alpha_a(h)a$ a neboť $\alpha_a(h) \in H^\bullet$, je $x \in aH^\bullet$ a $aH^\bullet \subseteq H^\bullet a$. Obrácenou inkluzi dokážeme obdobně, tedy $aH^\bullet = H^\bullet a$.

□

► 5.8.7. Poznámka. Věta dává návod, jako ověřit, že H je normální. Ale nesmíme opomenout ověřit, že H vůbec je podgrupou.

► 5.8.8. Definice. Buď G grupa. Řekneme, že $x, y \in G^\bullet$ jsou kojungované, existuje-li $a \in G^\bullet$ takové, že $y = \alpha_a(x)$. Značíme $x \equiv_H y$.

► 5.8.9. Lemma. Relace konjungovanosti je ekvivalence na G.

► 5.8.10. Důsledek. Podgrupa H grupy G je normální právě tehdy, je-li sjednocením nějakých tříd konjungovaných prvků.

► 5.8.11. Definice. Buďte G_1, G_2 grupy, $h : G_1 \to G_2$ homomorfismus. Jádrem homomorfismu h rozumíme množinu $\ker h := h^{-1}(\{1\}) = \{h \in G_1^\bullet \mid h(x) = 1\}$.

► 5.8.12. Lemma. Buďte G_1, G_2 grupy, $h : G_1 \to G_2$ homomorfismus. Pak $\ker h \lhd G_1$.

◦ *Důkaz.*

(je podgrupa) Mějme libovolné $x, y \in \ker h$, tj. $h(x) = h(y) = 1$. Pak $h(xy^{-1}) = h(x)h(y^{-1}) = h(x)h(y)^{-1} = 11^{-1} = 1$.

(je uzavřená vůči automorfismům) Nechť $a \in G_1^\bullet$, $x \in \ker h$. Pak $h(axa^{-1}) = h(a)h(x)h(a^{-1}) = h(a)h(a^{-1}) = h(aa^{-1}) = h(1) = 1$.

□

► 5.8.13. Lemma. Mějme $H \lhd G$, faktorgrupu G/H a přirozený epimorfismus $h_{\text{nat}}(x) = T_x$. Pak $\ker h_{\text{nat}} = H$.

◦ *Důkaz.* $\ker h = \{x \in G^\bullet \mid T_x = T_1\}$, ale $T_1 = H^\bullet$, tedy $\ker h = H^\bullet$. □

► 5.8.14. Věta. Normální podgrupy grupy G jsou právě všechna jádra homomorfismů na G, tj.

$$H \lhd G \iff (\exists h, h \text{ je homomorfismus na } G)(H = \ker h).$$

◦ *Důkaz.* Věta shnuje předchozí 2 tvrzení. □

► 5.8.15. Lemma. Homomorfismus $h : G_1 \to G_2$ je prostý právě tehdy, je-li $\ker h = \{1\}$.

◦ *Důkaz.*

(⇒) Obrazem jednoprvkové množiny je nejvýše jednoprvková množina a 1 je v jádru pro všechny homomorfismy.

(⇐) Nechť $\ker h = \{1\}$. Mějme $x, y \in G_1$ takové, že $h(x) = h(y)$. Pak $1 = h(x)h(y^{-1}) = h(xy) \Rightarrow xy^{-1} \in \ker h \Rightarrow xy^{-1} = 1 \Rightarrow x = y$.

□

► 5.8.16. Lemma. Nechť $h : G_1 \to G_2$ je homomorfismus. Pak $a \equiv_{\ker h} b$ právě tehdy, je-li $h(a) = h(b)$.

◦ *Důkaz.* $a \equiv_{\ker h} b \Leftrightarrow ab^{-1} \in \ker h \Leftrightarrow h(ab^{-1}) = 1 \Leftrightarrow h(a) = h(b)$. □

► 5.8.17. Věta (o homomorfismu pro grupy). Nechť $h : G_1 \to G_2$ je homomorfismus grup. Potom $h(G_1) \cong G_1 / \ker h$.

◦ *Důkaz.* $h(G_1) \cong G_1 / \equiv_h = G_1 / \equiv_{\ker h}$. □

► 5.8.18. Věta. Buď G grupa a buďte $H_i \lhd G$ pro $i \in I$. Potom

$$A := \bigcap_{i \in I} H_i \lhd G \quad \text{a} \quad B := \prod_{i \in I} H_i \lhd G.$$

◦ *Důkaz.*

(průnik) Mějme libovolné $a \in G^\bullet$ a $x \in A$. Pak $(\forall i \in I)(x \in H^\bullet) \Rightarrow (\forall i)(\alpha_a(x) \in H_i) \Rightarrow \alpha_a(x) \in A$.

(součin) Mějme libovolné $a \in G^\bullet$ a $x \in B$. Platí $B = \langle \bigcup_I H_i^\bullet \rangle$. Pak $x = a_1^{k_1} \cdots a_n^{k_n}$, kde $k_j \in \mathbb{Z}$ a $(\forall j)(\exists i_j)(a_j \in H_{j_i}^\bullet)$. Protože H_{j_i} je podgrupa, je $a_i^{k_i} \in H_{j_i}^\bullet$ a protože, je normální, je $\alpha_a(a_i^{k_i}) \in H_{j_i}^\bullet$. A konečně $\alpha_a(x) = \alpha_a(a_1^{k_1} \cdots a_n^{k_n}) = \alpha_a(a_1^{k_1}) \cdots \alpha_a(a_n^{k_n})$. Tedy každý prvek součinu je ve sjednocení podgrup, tedy je i v produktu podgrup.

□

► 5.8.19. Lemma (o tečče). Buď G grupa, $A \lhd G$ a $B \Subset G$. Potom $(AB)^\bullet = A^\bullet B^\bullet$.

◦ *Důkaz.* $AB = \langle A^\bullet \cup B^\bullet \rangle$, ale $A^\bullet B^\bullet = \{ab \mid a \in A^\bullet, b \in B^\bullet\}$.

(⊆) Ukážeme, že $A^\bullet B^\bullet$ je uzavřená v grupě G. Platí $A \cup B \subseteq A^\bullet B^\bullet$ Zvolme libovolné $x, y \in A^\bullet B^\bullet$, $x = a_1 b_1$, $y = a_2 b_2$. Potom $xy^{-1} = a_1 b_1 (a_2 b_2^{-1}) = a_1 \underbrace{b_1 b_2^{-1} a_2^{-1} (b_1 b_2^{-1})^{-1}}_{\alpha_{b_1 b_2^{-1}}(a_2^{-1}) \in A^\bullet} b_1 b_2^{-1} = \tilde{a}\tilde{b}$,

kde $\tilde{a} \in A^\bullet$ a $\tilde{b} \in B^\bullet$. Tedy $A^\bullet B^\bullet$ je podgrupa obsahující $A^\bullet \cup B^\bullet$. Ale AB je nejmenší taková, tedy inkluze platí.

(⊇) V AB jsou všechny součiny $x_1 \cdots x_n$, kde $x_i \in A \cup B$ tedy i všechny součiny tvaru ab.

□

► 5.8.20. Definice. Buď G grupa. Pak $C_G := \{c \in G \mid (\forall x \in M)(cx = xc)\}$ nazveme centrum grupy (tedy centrum grupy obsahuje právě ty prvky grupy, které komutují s každým prvkem.)

► 5.8.21. Lemma. Buď G grupa, C_G její centrum. Pak:

(1) je-li G Abelova, je $C_G = G$;

(2) $C_G \lhd G$;

(3) $G \,/\, C_G \cong \mathcal{I}_G$.

◦ *Důkaz.*

(1) V Abelově grupě komutují každé 2 prvky.

(2) Ukážeme, že C_G je uzavřená vůči všem vnitřním automorfismům. Mějme libovolné $a \in G^\bullet$ a $c \in C_G$. Pak $\alpha_a(c) = aca^{-1} = caa^{-1} = c \in C_G$.

(3) Definujme $h : G \to \mathcal{I}_G$ jako $h(a) = \alpha_a$, h je epimorfismus. Pak $I_G = h(G) \cong G \,/\, \ker h$. Platí $x \in \ker h \Leftrightarrow h(x) = \alpha_1 = \mathrm{id}_G \Leftrightarrow (\forall y \in G^\bullet)(xyx^{-1} = y) \Leftrightarrow (\forall y \in G^\bullet)(xy = yx) \Leftrightarrow x \in C_G$, tedy $\ker h = C_G$ a $I_G \cong G \,/\, C_G$.

□

► 5.8.22. Věta (o izomorfismu). Buď $G = (M, \cdot)$ grupa, $A, B \Subset G$. Je-li $A \lhd AB$, potom $A \cap B \lhd B$ a $AB \,/\, A \cong B \,/\, (A \cap B)$.

◦ *Důkaz.* Třídy $AB \,/\, A$ jsou tvaru $A^\bullet c$, kde $c \in (AB)^\bullet = A^\bullet B^\bullet$. Tedy $(\exists a \in A^\bullet, b \in B^\bullet)(c = ab)$. Vezměme $f_{\mathrm{nat}} : AB \to AB \,/\, A$ a položme $f_B = f_{\mathrm{nat}}/B$. Ukážeme, že $f : B \to AB \,/\, A$ je epimorfismus, tedy, že v každé třídě $A^\bullet ab$ leží prvek z B. Tedy i $a^{-1}ab = b$ je v každé třídě. Podlě věty o homomorfismu je $AB \,/\, A \cong B \,/ \ker f_B$, ale $\ker f_B = \{x \in B \mid f_B(x) = T_1 = A\} = \{x \in B \mid x \in A\} = A \cap B$. □

► 5.8.23. Věta. Buď G cyklická grupa řádu n a nechť $k \mid n$. Potom existuje právě jedna podgrupa grupy G řádu k.

◦ *Důkaz.*

(existence) Nechť $a \in G$ je geneártor grupy. Položme $H := \langle a^{n/k} \rangle$. Pak $\left(a^{n/k}\right)^k = 1$ a platí, že pokud $\left(a^{n/k}\right)^\ell = 1$, tak $n\ell/k = sn$, tedy $\ell = ks$ a $\ell \geq k$.

(jednoznačnost) Nechť $K \Subset G$ je řádu k. Pak $K = \langle a^\ell \rangle$ a $\left(a^\ell\right) k = 1$ a $\ell k = sn = skn/k$ a tedy $\ell = sd$ a $a^\ell = \left(a^{n/k}\right)^s \in H$. Tedy $K \Subset H$ a z rovnosti počtu prvků plyne $K = H$.

□

► 5.8.24. Definice. Grupa, která nemá netriviální normální podgrupy, tj. $H \lhd G \Rightarrow H = G \vee H = E$, se nazývá jednoduchá.

► 5.8.25. Příklad.

(1) E je jednoduchá.

(2) G o $p \in P$ prvcích jsou jednoduché, současně jsou cyklické, tedy Abelovy.

► 5.8.26. Věta. Buď $G \neq E$ Abelova grupa. Potom G je jednoduchá právě tehdy, má-li prvočíselný řád p.

◦ *Důkaz.*

(G je cyklická) Nebyla-li by cyklická, obsahovala by netriviální podgrupu, která by byla normální, neboť všechny by byly normální (netriviální podgrupou by bylo libovolné $\langle a \rangle$, kde $a \neq 1$).

(G je konečná) Pokud není konečná, pak $G \cong Z = (\mathbb{Z}, +)$, ale např. $S = (\mathbb{S}, +) \lhd Z$ a S odpovídá nějaké netriviální podgrupa G.

(neex. $1 \neq q \mid p$) Podle předházející věty existuje podgrupa H řádu q, která je v Abelově normální, a tedy G není jednoduchá.

□

• 5.9. Grupy permutací

► 5.9.1. Definice. Buď A množina a M množina všech bijekcí $A \to A$. Pak $\mathcal{S}_A(M, \circ)$ je grupa nazývaná symetrická grupa. Označme ϵ identitu v $\mathcal{S}_A$.

► 5.9.2. Definice. Grupa permutací je libovolná podgrupa symetrické grupy $\mathcal{S}_A$.

► 5.9.3. Věta (Cayley). Libovolná grupa je izomorfní s nějakou grupou permutací.

◦ *Důkaz.* Mějme $G = (M, \cdot)$, $a \in M$; definujeme $\pi_a : M \to M$ jako $\pi_a(x) = ax$. Pro libovolné $y \in M$ řešme $\pi_a(x) = ax = y$, dostaneme jedno řešení $x = a^{-1}y$, tedy π_a je bijekce (permutace).

Definujme $h : M \to \mathcal{S}_M$ jako $h(a) = \pi_a$ a ukážeme, že h je homomorfismus: Mějme $a, b, x \in M$; pak $h(ab)(x) = \pi_{ab}(x) = abx = \pi_a(bx) = \pi_a(\pi_b(x)) = (\pi_a\pi_b)(x) = (h(a)h(b))(x)$.

Ukážeme, že je h je monomorfní (prostý): $\ker h = \{a \in M \mid h(a) = \epsilon\}$, $(\forall x \in M)(\epsilon(x) = x)$, $\pi_a(x) = \epsilon(x) = x$, $a = 1$.

Platí $G \cong h(G) \Subset \mathcal{S}_M$. Tedy $h(G)$ je grupa permutací. □

▶ 5.9.4. Poznámka. Cayleyova věta se dá formulovat i následovně: Libovolnou grupu lze izomorfně vnořit do symetrické grupy.

▶ 5.9.5. Poznámka. Pro $M = \widehat{n}$ se G izomorfně vnoří do $\mathcal{S}_{\widehat{n}} =: \mathcal{S}_n$.

▶ 5.9.6. Poznámka. $\pi \in \mathcal{S}_n$ zapisované $\pi = \begin{pmatrix} 1 & \cdots & n \\ p_1 & \cdots & p_n \end{pmatrix}$ je zobrazení.

▶ 5.9.7. Příklad. $\pi \in \mathcal{S}_8$, $\pi = \begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 2&4&5&1&4&7&6&8 \end{pmatrix}$ lze zapsat jako $1 \to 2 \to 4 (\to 1); 3 \to 5 (\to 3); 6 \to 7 (\to 6); 8 (\to 8)$, ale zkráceně jako $(124)(35)(67)(8)$. Zápis současně vyjadřuje složení cyklů a můžeme vynechat cykly s 1 prvkem. Tedy můžeme psát $\pi = (124)(35)(67)$.

▶ 5.9.8. Definice. Mějme $\pi \in \mathcal{S}_n$. Pak π je <u>cyklus</u>, pokud $\pi = (p_1 p_2 ... p_k)$, $1 \leq k \leq n$, p_k jsou různá. Cykly jsou <u>nezávislé</u>, pokud neobsahují společný prvek.

▶ 5.9.9. Lemma. Libovolná permutace lze rozepsat jako součin nezávislých cyklů.

▶ 5.9.10. Lemma.

$$(k_1 \dots k_p) = (k_1 k_p)(k_1 k_{p-1}) \dots (k_1 k_3)(k_1 k_2).$$

◦ *Důkaz.* Obrázkem. □

▶ 5.9.11. Důsledek. Transpozice generují $\mathcal{S}_n$. (Každá permutace lze zapsat jako součin transpozic.)

▶ 5.9.12. Poznámka. Lze ukázat, že i sousední transpozice generují $\mathcal{S}_n$. Dále lze ukázat, že pro jakékoli n existují 2 permutace, které generují $\mathcal{S}_n$, a to např. $\tau = (12)$ a $\pi = (123 \dots n)$.

▶ 5.9.13. Věta. Buď $n \in \mathbb{N}$ a $\sigma, \pi \in \mathcal{S}_n$, $\sigma = (k_1^1 \dots k_{p_1}^1) \dots (k_1^m \dots k_{p_m}^m)$ je rozklad na ne nutně nezávislé cykly. Potom $\alpha_\pi(\sigma) = (\pi(k_1^1) \dots \pi(k_{p_1}^1)) \dots (\pi(k_1^m) \dots \pi(k_{p_m}^m))$

◦ *Důkaz.*

($m = 1$) Máme $\sigma = (k_1 \dots k_p)$, označme $\sigma_\pi := (\pi(k_1) \dots \pi(k_p))$, tedy chceme $\alpha_\pi(\sigma) = \sigma_\pi$, což, protože π je bijekce, je ekvivalentní $\alpha_\pi(\sigma) \circ \pi = \sigma_\pi \circ \pi$.

Ukážeme, že $(\forall k \in \widehat{n})(\alpha_\pi(\sigma)(\pi(k)) = \sigma_\pi(\pi(k)))$. To jest $(\pi\sigma\pi^{-1})(\pi(k)) = \pi(\sigma(k))? = \sigma_\pi(\pi(k))$.

Nechť $k = k_i$, pak $\sigma(k) = k_{i+1}$ (položíme $k_{p+1} := k_1$), tedy $\pi(\sigma(k)) = \pi(k_{i+1})$. Současně $\sigma_\pi(\pi(k_i)) = \pi(k_{i+1})$, což jsme potřebovali.

Pro $k \neq k_i$ jsou obě strany rovny $\pi(k)$.

($m \in \mathbb{N}$) S využitím případu $m = 1$ dostaneme

$$\alpha_\pi\left(\left(k_1^1 \dots k_{p_1}^1\right) \dots \left(k_1^m \dots k_{p_m}^m\right)\right) = \alpha_\pi\left(k_1^1 \dots k_{p_1}^1\right) \dots \alpha_\pi\left(k_1^m \dots k_{p_m}^m\right) = \left(\pi\left(k_1^1\right) \dots \pi\left(k_{p_1}^1\right)\right) \dots \left(\pi\left(k_1^m\right) \dots \pi\left(k_{p_m}^m\right)\right).$$

□

► 5.9.14. Důsledek. $(\alpha_\pi(\sigma))(\pi(k)) = \pi(\sigma(k))$, $\sigma = \begin{pmatrix} 1 & \cdots & n \\ p_1 & \cdots & p_n \end{pmatrix}$, pak $\alpha_\pi(\sigma) = \begin{pmatrix} \pi(1) & \cdots & \pi(n) \\ \pi(p_1) & \cdots & \pi(p_n) \end{pmatrix}$

► 5.9.15. Lemma. Libovolná podgrupa H grupy G, která má index 2, je normální. (Index je počet rozkladových tříd $G \,/\, H$).

◦ *Důkaz.* Jedna ze tříd je H, druhá tedy nutně $G \setminus H$. Rozklad je tedy jednoznačný. □

► 5.9.16. Definice. Označme $\mathcal{A}_n$ grupu sudých permutací (ověření, že je grupa, je triviální). Pak $\mathcal{A}_n$ nazýváme alternující (pod)grupa.

► 5.9.17. Důsledek. $\mathcal{A}_n \lhd \mathcal{S}_n$.

► 5.9.18. Lemma. Nechť $A \Subset B \Subset G$. Pak $A \lhd G \Rightarrow A \lhd B$.

◦ *Důkaz.* Lze jednoduše ukázat pomocí uzavřenosti na vnitřní automorfismy. □

► 5.9.19. Příklad.

($n = 1$) $\mathcal{A}_1 = \mathcal{S}_1 = E$.

($n = 2$) $\mathcal{A}_2 = E$.

($n \geq 3$) $\mathcal{A}_n$ je netriviální normální podgrupa.

($n = 3$) $\mathcal{S}_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$ a $\mathcal{A}_3 = \{\mathrm{id}, (123), (132)\}$ má prvočíselný počet prvků a je jednoduchá.

($n = 4$) $\mathcal{A}_4$ má řád 12 a není jednoduchá, neboť obsahuje např. $\mathcal{K}_4 := \{\mathrm{id}, (12)(34), (13)(24), (23)(14)\}$ a platí $\mathcal{K}_4 \lhd \mathcal{A}_4$. Předně je $\mathcal{K}_4$ uzavřená na skládání, součin 2 se vždy zobrazí na třetí, např. $(12)(34) \cdot (13)(24) = (23)(14)$. A každá permutace je sama sobě inverzní, tedy $\mathcal{K}_4$ je grupa.

$\mathcal{K}_4$ jsou všechny $(ij)(k\ell)$, kde tato 4 čísla jsou různá. Ukážeme, že $\mathcal{K}_4$ je uzavřená vůči vnitřním automorfismům. $\alpha_\pi((ij)(k\ell)) = (\pi(i)\pi(j))(\pi(k)\pi(\ell))$, ale neboť π je bijekce, jsou to opět čísla $1, 2, 3, 4$, jenom případně přeházené.

$\mathcal{K}_4$ nazýváme Kleinova grupa.

Všimněme si, že také $\mathcal{L}_2 := \{\mathrm{id}, (12)(34)\} \lhd \mathcal{K}_4$ (má polovinu prvků, tedy index rozkladu podle $\mathcal{L}_2$ je 2 a je normální). Ale $\mathcal{L}_2 \not\lhd \mathcal{A}_4$.

► 5.9.20. Věta. Alternující grupy $\mathcal{A}_n$ jsou pro $n \neq 4$ jednoduché (tedy nemají netriviální normální podgrupu).

◦ *Důkaz.* Pro $n \leq 3$ jsme platnost ukázali v předchozím příkladě. Tedy nechť $n \geq 5$. Mějme libovolnou $H \lhd \mathcal{A}_n$, $H \neq E$. Ukážeme, že $H = \mathcal{A}_n$. Důkaz se rozpadá do 3 kroků.

(**v H existuje 3cykl** (u, v, w)) Vezměme $\pi \in H^\bullet$ takovou, která mění nejmenší co počet prvků a není identitou. Určitě není transpozice (ta je lichá). Sporem, nechť $\pi \neq (u, v, w)$. Pak rozklad na nezávislé cykly může vypadat následovně:

(1) $\pi = (pq)(rs)\cdots$. Pak existuje páté číslo, označme jej t.

(2) $\pi = (pqr\cdots)\cdots$ a mění ještě nejméně 2 další čísla s, t.

Mějme $\varrho := (rst) \in \mathcal{A}_n$ sudou permutaci. Pak $\alpha_\varrho(\pi) = \varrho\pi\varrho^{-1} \in H^\bullet$ (neboť H je normální). V prvním případě $\alpha_\varrho(\pi) = (pq)(st)\cdots \neq \pi$ a ve druhém $\alpha_\varrho(\pi) = (pqs)\cdots \neq \pi$. Definujeme $\sigma := \pi^{-1}(\varrho\pi\varrho^{-1}) \in H$ a není jednotková.

Ukážeme, že σ nechává na místě více prvků, než π.

(2) Mějme libovolné $k \in \widehat{n}$ tak, že $\pi(k) = k$. Pak $k \notin \{p, q, r, s, t\}$ a $\varrho(k) = k$. Pak $\sigma(k) = k$, neboť žádná z permutací π, π^{-1}, ϱ a ϱ^{-1} nemění k. Ale $\pi(p) = q$ a $\sigma(p) = p$ TODO. Tedy σ mění nejméně o 1 méně čísel, než π.

Obdobně pro (1). Tedy σ nechává na místě více čísel než π.

(je-li v H jeden 3cykl (u, v, w), jsou tam všechny 3cykly) Zvolme libovolný 3cykl (p, q, r). Položme $\pi := \left(\begin{smallmatrix} u & v & w & y & z \\ p & q & r & Y & Z \end{smallmatrix}\right)$. Nutně existují takové y, z, Y, Z, že π je sudá, tj. $\pi \in \mathcal{A}_n$. Potom $\alpha_\pi((u, v, w)) = (\pi(u), \pi(v), \pi(w)) = (p, q, r)$ a neboť H je normální, je $(p, q, r) \in H$.

(3cykly generují $\mathcal{A}_n$) Ukážeme, že součin π 2 libovolných transpozicí lze rozložit na 3cykly. Je-li $\pi = (p, q)(p, r) = (prq)$ je 3cykl. Je-li $\pi = (p, q)(r, s) = (p, r, s)(p, q, s)$. Je-li $\pi = (p, q)(p, q) = (p, q, r)(r, q, p)$ pro libovolné r.

□

• 5.10. Kartézský a direktní součin grup

► 5.10.1. Definice. Mějme $G_1, \ldots, G_n$ grupy, $G_i = (M_i, \cdot)$. Označme $M := M_1 \times \cdots \times M_n$ a definujme $(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 b_1, \ldots, a_n b_n)$. Jednotkou bude $1_M = (1, \ldots, 1)$ a inverzním prvkem $(a_1, \ldots, a_n)^{-1} = (a_1^{-1}, \ldots, a_n^{-1})$. Grupu $G := (M, \cdot)$ nazýváme kartézský součin grup a značíme $G = \overset{n}{\underset{1}{\times}} G_i$..

► 5.10.2. Definice. Buďte G grupa a $A, B \Subset G$. Řekneme, že G je direktní součin podgrup A, B, je-li zobrazení $f : A \times B \to G$, $f(x, y) = xy$ izomorfismem grup. Značíme $G = A \odot B$.

► 5.10.3. Poznámka. Direktní součin lze přirozeně zobecnit na konečné i spočetné systémy podgrup.

► 5.10.4. Lemma. Zobrazení f z předchozí definice je homomorfismus právě tehdy, když $(\forall a \in A^\bullet, b \in B^\bullet)(ab = ba)$.

◦ *Důkaz.*

($\Rightarrow$) $ab = f(\langle a, b\rangle) = f(\langle 1, b\rangle \langle a, 1\rangle) = f(1, b)f(a, 1) = ba$.

($\Leftarrow$) $f(\langle a_1, b_1\rangle \langle a_2, b_2\rangle) = f(\langle a_1 a_2, b_1 b_2\rangle) = a_1 a_2 b_1 b_2 = a_1 b_1 a_2 b_2 = f(\langle a_1, b_1\rangle) f(\langle a_2, b_2\rangle)$.

□

► 5.10.5. Lemma. Zobrazení f z předchozí definice je „na“ právě tehdy, když $A^\bullet B^\bullet = G^\bullet$.

◦ *Důkaz.* $A^\bullet B^\bullet$ je z definice obor hodnot f. □

► 5.10.6. Lemma. Je-li f z předchozí definice homomorfismus, pak je f prostý právě tehdy, je-li $A^\bullet \cap B^\bullet = \{1\}$.

◦ *Důkaz.*

(⇒) Víme, že $\ker f = \{\langle 1,1\rangle\}$. Nechť $c \in A \cap B$. Pak triviálně $c \in A$ a $c^{-1} \in B$ a $\langle c, c^{-1}\rangle \in A \times B$. A neboť $f(\langle c, c^{-1}\rangle) = cc^{-1} = 1$, je $\langle c, c^{-1}\rangle = \langle 1,1\rangle$, tedy hlavně $c = 1$.

(⇐) Nechť $A^\bullet \cap B^\bullet = \{1\}$. Mějme libovolné $\langle a, b\rangle \in \ker f$. Pak $f(a,b) = ab = 1$, tedy $a = b^{-1}$ a nutně $a = b^{-1} \in A^\bullet \cap B^\bullet$ a tedy $a = b = 1$.

□

► 5.10.7. Věta. Platí $G = A \odot B$ právě tehdy, když platí:

(1) $(\forall a \in A^\bullet, b \in B^\bullet)(ab = ba)$;

(2) $A^\bullet B^\bullet = G^\bullet$;

(3) $A^\bullet \cap B^\bullet = \{1\}$.

► 5.10.8. Poznámka. V aditivní grupě používáme název direktní součet.

► 5.10.9. Věta. Je-li $G = A \odot B$, pak platí

(4) $A \lhd G$, $B \lhd G$;

(5) $AB = G$ (tedy A a B komutují);

(6) $(\forall x \in G^\bullet)(\exists_1 a \in A^\bullet, b \in B^\bullet)(x = ab = ba)$.

◦ *Důkaz.*

(4) Mějme $c \in G^\bullet$, $x \in A$, $y \in B$ a podle (2) je $c = ab$, $a \in A^\bullet$, $b \in B^\bullet$. Pak

$$\alpha_c(x) = cxc^{-1} = abxb^{-1}a^{-1} \overset{(1)}{=} axbb^{-1}a^{-1} = axa^{-1} \in A^\bullet$$

a

$$\alpha_c(y) = cyc^{-1} = a\overbrace{byb^{-1}}^{\in B^\bullet}a^{-1} = byb^{-1}aa^{-1} = byb^{-1} \in B^\bullet.$$

(5) Podle lemmatu o tečce je $G^\bullet = A^\bullet B^\bullet \subseteq (AB)^\bullet = G^\bullet$, tedy $AB = G$.

(6) Zobrazení f je bijekce, tedy existuje právě jedna dvojice a, b taková, že $f(a,b) = c$.

□

► 5.10.10. Věta. Buď G cyklická grupa řádu $p_1^{k_1} \cdots p_n^{k_n}$ – standardní rozklad na prvočísla. Pak $G = A_1 \odot \cdots \odot A_n$, kde A_i má řád p_i.

▶ 5.10.11. Příklad. Pro $Z_6 = Z / \equiv_6 = (\{0,1,\dots,5\},+)$ má řád $6 = 2 \cdot 3$ a lze ji napsat jako $Z_6 = A \oplus B$. Platí $A^\bullet = \{0,3\}$ a $B^\bullet = \{0,2,4\}$.

▶ 5.10.12. Věta. Buď $G = A \odot B$. Pak $G / A \cong B$.

◦ *Důkaz.* Z věty o izomorfismu je $AB / A \cong B / A \cap B$, ale $AB = G$, $A \cap B = E$, tedy $B / E \cong B$, tedy $G / A \cong B$. □

---

6. Okruhy

6.1. Okruh

▶ 6.1.1. Definice. Řekneme, že algebra $R = (M,+,\cdot)$ je okruh (angl. ring), pokud platí:

(1) algebra $(M,+)$ je Abelova grupa; nazýváme ji aditivní grupa okruhu R a značíme R_+;

(2) algebra $(M,\cdot)$ je grupoid; nazýváme jej multiplikativní grupoid okruhu R a značíme $R_\bullet$;

(3) distributivní zákon, tj.

$$(\forall a,b,c \in M)(a(b+c) = (ab)+(ac) \ \wedge \ (b+c)a = (ba)+(ca)).$$

▶ 6.1.2. Příklad. $Z = (\mathbb{Z},+,\cdot)$ je okruh celých čísel.

▶ 6.1.3. Poznámka. Jak jsme zvyklí, má operace násobení větší prioritu než operace sčítání, tj. $ab + c := (ab) + c$.

▶ 6.1.4. Definice. $E = (\{0\},+,\cdot)$ je triviální okruh.

▶ 6.1.5. Definice. Řekneme, že okruh R je asociativní, resp. je komutativní, resp. má jednotku, má-li stejnou vlastnost i multiplikativní grupoid $R_\bullet$.

▶ 6.1.6. Příklad.

(1) Okruh $Z = (\mathbb{Z},+,\cdot)$ je asociativní, komutativní a má jednotku.

(2) Okruh $(\mathbb{C}^{n,n},+,\cdot)$ je asociativní, má jednotku (jednotkovou matici), ale není komutativní.

(3) Vektorový prostor $(V,+)$ s vektorovým součinem $\times$ tvoří orkuh $(V,+,\times)$, který není ani asociativní, ani komutativní.

▶ 6.1.7. Definice. Zerový okruh je okruh $R = (M,+,\cdot)$, kde $(\forall a,b \in M)(ab := 0)$.

▶ 6.1.8. Definice. Definujeme rozdíl prvků, $(\forall a,b \in M)(a - b := a + (-b))$.

▶ 6.1.9. Věta. Buď $R = (M, +, \cdot)$ okruh, nechť $a, b \in M$. Potom platí:

(1) $c(a-b) = ca - cb$; $(a-b)c = ac - bc$;

(2) $0 \cdot a = a \cdot 0 = 0$;

(3) $(-a)b = a(-b) = -(ab)$;

(4) $(-a)(-b) = ab$.

◦ *Důkaz.* Všechno je podobné, ukážeme první dvě.

(1) $c(a-b) = c(a-b) + cb - cb = c(a-b+b) - cb = ca - cb$.

(2) $0 \cdot a = (b-b)a = ba - ba = 0$.

□

▶ 6.1.10. Definice. Číselný okruh je libovolný okruh s přirozenými číselnými operacemi a s nosičem, který je číselnou množinou.

▶ 6.1.11. Definice. Dělitelé nuly jsou libovolné $a, b \in R^\bullet$ takové, že $a, b \neq 0$, ale $ab = 0$. Okruhem bez dělitelů nuly rozumíme okruh, ve kterém neexistují dělitelé nuly.

▶ 6.1.12. Příklad. Např. $\left(\begin{smallmatrix}1&0\\0&0\end{smallmatrix}\right)\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right) = \left(\begin{smallmatrix}0&0\\0&0\end{smallmatrix}\right)$.

▶ 6.1.13. Věta. Číselné okruhy jsou bez dělitelů nuly, tj. pro $a, b \in R^\bullet$ platí, že

$$(ab = 0 \Rightarrow (a = 0 \ \vee \ b = 0)).$$

▶ 6.1.14. Definice. Oborem integrity rozumíme asociativní a komutativní okruh bez dělitelů nuly.

▶ 6.1.15. Definice. Buď $R = (M, +, \cdot)$ okruh. Polynomem nad okruhem R rozumíme libovolnou nekonečnou posloupnost $(a_n)_{n=0}^\infty$ prvků z M, v níž je konečný počet prvků nenulových.

Takové $n \in \mathbb{N}_0$, že $a_n \neq 0$ a $(\forall i > n)(a_i = 0)$ nazveme stupeň polynomu. Pro nulový polynom $\theta = 0\,0\,0\,0\,\ldots$ nedefinujeme stupeň.

Posloupnost $(a_n)_{n=0}^\infty$ označíme $\sum a_n x^n$ nebo $a_0 + a_1 x + a_2 x^2 + \cdots + a_s x^s$, kde s je stupeň polynomu. Jde o formální zápis, nikoli sumu. Množinu všech polynomů nad okruhem R označíme $R[x]^\bullet$.

▶ 6.1.16. Definice. Mějme okruh R a polynomy $P = \sum a_i x^i$, $Q = \sum b_i x^i$. Potom definujeme součet polynomů jako $P + Q := \sum (a_i + b_i) x^i$ a součin polynomů jako $PQ := \sum c_k x^k$, kde $c_k := \sum_{i=0}^k a_i b_{k-i}$.

▶ 6.1.17. Poznámka. Součet i součin polynomů jsou opět polynomy a operace jsou přirozené, jaké známe z analýzy.

▶ 6.1.18. Definice. $R[x] = (R[x]^\bullet, +, \cdot)$ nazveme okruh polynomů nad okruhem R.

▶ 6.1.19. LEMMA. Pokud okruh R je asociativní, resp. je komutativní, resp. má jednotku, má odpovídající vlastnost i $R[x]$. Jednotkou v okruhu polynomů je $1x^0 = 1\,0\,0\,0\cdots$.

▶ 6.1.20. LEMMA. Nemá-li okruh R dělitele nuly, nemá je ani okruh $R[x]$.

◦ *Důkaz.* Mějme $P, Q \in R[x] \setminus \{\theta\}$, $P = \sum a_i x^i$, $Q = \sum b_i x^i$ a nechť stupeň P je p a Q je q. Mějme součin $PQ = \sum c_k x^k$, pak je speciálně $c_{p+q} = \sum_0^{p+q} a_i b_{p+q-i}$. Pro $i > p$ je $a_i = 0$ a pro $i < p$ je $p + q - i > q$ a $b_i = 0$. Tedy $c_{p+q} = a_p b_q$, a neboť oba jsou nenulové a R nemá dělitele nuly, je $c_{p+q} \neq 0$ a tedy $PQ \neq \theta$. □

▶ 6.1.21. DEFINICE. Mějme $x_1, \ldots, x_n$ soubor neučitých. Pak definujeme $R[x_1, \ldots, x_n]$ indukcí jako $R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])[x_n]$.

▶ 6.1.22. VĚTA. Buď R obor integrity, pak také $R[x_1, \ldots, x_n]$ je obor integrity.

◦ *Důkaz.* Důkaz provedeme snadno indukcí podle n s využitím předchozího lemmatu. □

• 6.2. TĚLESO

▶ 6.2.1. DEFINICE. Okruh $R = (M, +, \cdot)$ je <u>těleso</u>, pokud platí, že algebra $(M \setminus \{0\}, \cdot)$ je grupa. Grupu $(M \setminus \{0\}, \cdot)$ nazýváme <u>multiplikativní grupa</u> tělesa a značíme T_*. Těleso značíme T a je-li T_* Abelova, řekneme, že těleso T je <u>komutativní</u>.

▶ 6.2.2. LEMMA. Těleso vždy obsahuje alespoň 2 prvky, a to nulu a jednotku.

▶ 6.2.3. DEFINICE. Definujeme <u>triviální těleso</u> $F = (\{0, 1\}, +, \cdot)$. Operace na triviálním tělese se definují pomocí <u>Cayleyových tabulek</u>:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

▶ 6.2.4. DEFINICE. Základní číselná tělesa:

(1) $Q := (\mathbb{Q}, +, \cdot)$;

(2) $R := (\mathbb{R}, +, \cdot)$;

(3) $C := (\mathbb{C}, +, \cdot)$.

▶ 6.2.5. POZNÁMKA. Okruh celých čísel $Z = (\mathbb{Z}, +, \cdot)$ není tělesem!

▶ 6.2.6. PŘÍKLAD. Položme $M = \left\{a + \sqrt{2}b \;\middle|\; a, b \in \mathbb{Q}\right\}$, pak $(M, +, \cdot)$ je těleso takové, že $\mathbb{Q} \subsetneq M \subsetneq \mathbb{R}$. Jediné zajímavé je ukázat přítomnost inverzního prvku: $(a + \sqrt{2}b)^{-1} = \frac{a - \sqrt{2}b}{a^2 - 2b^2}$.

Obecně lze definovat $\mathbb{Q}_{\sqrt{n}} = ((\mathbb{Q} + \sqrt{n}\mathbb{Q}), +, \cdot)$ pro libovolné $n \in \mathbb{N}$.

▶ 6.2.7. Věta.

(1) Těleso nemá dělitele nuly.

(2) Komutativní těleso je obor integrity.

◦ *Důkaz.*

(1) Nenulové prvky tělesa tvoří grupu, tedy jsou uzavřené vůči násobení a tedy nemůže $ab = 0$.

(2) Těleso je vždy asociativní, tedy je-li i komutativní, je oborem integrity z definice.

□

▶ 6.2.8. Definice. Buďte $R = (M, +, \cdot)$ okruh a $T = (N, +, \cdot)$ těleso.

(1) Řekneme, že $A \subseteq M$, $A \neq \emptyset$ je uzavřená v okruhu R, platí-li

$$(\forall a, b \in A)(ab \in A \ \wedge \ a - b \in A).$$

Algebru $Q = (A, +, \cdot)$ nazveme podokruh okruhu R a značíme $Q \Subset R$.

(2) Řekneme, že $B \subseteq N$, $B \neq \emptyset$ je uzavřená v tělese T, platí-li

$$\big(\forall a, b \in B\big)\big(b \neq 0 \Rightarrow (ab^{-1} \in B \ \wedge \ a - b \in B)\big).$$

Algebru $U = (B, +, \cdot)$ nazveme podtěleso tělesa T a značíme $U \Subset T$. Těleso T nazýváme nadtěleso tělesa U a relaci $\Subset$ rozšířením těles

▶ 6.2.9. Příklad.

(1) Označme $S = \{2k \mid k \in \mathbb{Z}\}$. Pak platí (pro okruhy) $(S, +, \cdot) \Subset_O (\mathbb{Z}, +, \cdot) \Subset_O (\mathbb{Q}, +, \cdot)$.

(2) Pro tělesa platí $(\mathbb{Q}, +, \cdot) \Subset_T (\mathbb{R}, +, \cdot) \Subset_T (\mathbb{C}, +, \cdot)$.

▶ 6.2.10. Věta. Buďte $R = (M, +, \cdot)$ okruh, resp. těleso a nechť $Q_i \Subset R, i \in I$ je systém podokruhů, resp. podtěles. Pak $\bigcap_{i \in I} G_i$ je podokruh, resp. podtěleso R.

▶ 6.2.11. Definice. Buďte $R = (M, +, \cdot)$ okruh, $A \subseteq M$. Pak $\langle A \rangle := \bigcap \{Q \Subset R \mid A \subseteq Q\}$ nazýváme podokruh generovaný množinou A.

▶ 6.2.12. Lemma.

$$\langle A \rangle^{\bullet} = \{k_1 \times a_{11} \dots a_{1m_1} + \dots + k_n \times a_{n1} \dots a_{nm_n} \mid n \in \mathbb{N}_0, m_i \in \mathbb{N}, k_i \in \mathbb{Z}, a_{ij} \in A\}$$

◦ *Důkaz.* Množina obsahuje A, nelze nic vyjmout a je uzavřená v R. □

▶ 6.2.13. Definice. Buďte $R = (M, +, \cdot)$ okruh a nechť $Q_i \Subset R, i \in I$ je systém podokruhů. Pak definujeme součet podokruhů jako $\sum_{i \in I} Q_i := \big\langle \bigcup_{i \in I} Q_i^{\bullet} \big\rangle$

6.3. Kongruence

▶ 6.3.1. Definice. Buď $R = (M, \cdot)$ okruh a $\equiv$ ekvivalence na M. Řekneme, že $\equiv$ je kongruence na okruhu R, platí-li:

$$(\forall a, b, c, d \in M)\big((a \equiv b \ \wedge \ c \equiv d) \Rightarrow (a + c \equiv b + d \ \wedge \ ac \equiv bd)\big).$$

▶ 6.3.2. Definice. Buď $\equiv$ kongruence na okruhu R. Pak $R/\equiv \ := (M/,+,\cdot)$ s operacemi $T_a + T_b := T_{a+b}$ a $T_{ab} := T_a T_b$ nazýváme faktorokruh okruhu R podle kongruence $\equiv$.

▶ 6.3.3. Lemma. Buď $\equiv$ kongruence na okruhu R. Pak faktorokruh $R/\equiv$ je okruh.

▶ 6.3.4. Věta. Je-li okruh R asociativní, resp. komutativní, resp. má jednotku, potom má tutéž vlastnost i faktorokruh $R/\equiv$.

▶ 6.3.5. Poznámka. Neplatí obecně, že faktorokruh tělesa je tělesem (nepřenáší se vlastnost nemíti dělitele nuly).

▶ 6.3.6. Definice. Nechť $Q \Subset R$ je okruh a jeho podokruh. Pak definujeme ekvivalenci $\equiv_Q$ na R tak, že $a \equiv_Q b \Leftrightarrow a - b \in Q$.

▶ 6.3.7. Poznámka. R_+ je Abelova, tedy $\equiv_Q$ je kongruence na grupě R_+, ne však kongruence na okruhu R.

▶ 6.3.8. Definice. Podokruh I okruhu R nazýváme ideál v R a značíme $I \lhd R$, platí-li, že

$$(\forall a \in I^\bullet)(\forall r \in R^\bullet)(ra \in I^\bullet \ \wedge \ ar \in I^\bullet).$$

▶ 6.3.9. Poznámka.

(1) Při ověřování, že I je ideál, je nejprve nutno ověřit, že je podokruhem, a pak teprve definující podmínku ideálu.

(2) Definující vlastnost ideálu je silnější, než uzavřenost vůči násobení, tedy stačí ověřit tuto podmínku a uzavřenost vůči sčítání.

▶ 6.3.10. Věta. Ekvivalence $\equiv$ na R je kongruencí právě tehdy, je-li ekvivalencí indukovanou ideálem, tj. $(\exists I \lhd R)((\equiv) = (\equiv_I))$.

◦ *Důkaz.*

($\Leftarrow$) Vezměme třídu T_0 kongruence $\equiv$ a ukážeme, že $I = (T_0, +, \cdot)$ je hledaný ideál.

Platí $a \equiv 0$ a $b \equiv 0$, tedy $a - b \equiv 0$ a tedy $a - b \in T_0$. Dále $a \equiv 0$ a $r \equiv r$, tedy $ar \equiv 0$ a $ra \equiv 0$ a tedy $ar, ra \in T_0$.

Z grup víme, že $(\equiv) = (\equiv_{T_0})$, což jsme chtěli ukázat.

(⇒) Mějme $I \lhd R$. Pak $a \equiv_I b \Leftrightarrow a - b \in I^\bullet$. Ekvivalence $\equiv_I$ je kongruencí na R_+, tedy zbývá ukázat druhá podmínka, tj. že $ac \equiv_I bd$ pokud $a = b$ a $c = d$. Platí $ac - bd = ac - ad + ad - bd = a(c-d) + (a-b)d$, a neboť $(c-d), (a-b) \in I$ a ideál je uzavřený na násobení všemi prvky R a na sčítání, je i $a(c-d) + (a-b)d \in I$.

□

▶ 6.3.11. Příklad. Mějme okruh celých čísel $Z = (\mathbb{Z}, +, \cdot)$. Pak pro libovolné $m \in \mathbb{N}_0$ definujeme $\equiv_m$ jako $a \equiv_m b \Leftrightarrow (\exists s \in \mathbb{Z})(a - b = sm)$. Pak $I_m := \{sm \mid s \in \mathbb{Z}\}$ je ideál a I_m jsou všechny ideály na Z.

Zjevně splývá $Z/\equiv_m$ a Z/I_m. Budeme proto používat společnou značku Z_m a název okruh zbytkových tříd modulo m.

▶ 6.3.12. Věta. Nechť $m \in \mathbb{N}$ (tedy $m \neq 0$). Pak v jedné třídě Z_m leží 2 čísla a, b právě tehdy, dávají-li stejný zbytek po dělení m. Okruh zbytkových tříd Z_m má řád m.

▶ 6.3.13. Věta. Buďte R okruh s jednotkou, $I \lhd R$ a nechť $1 \in I^\bullet$. Pak $I = R$.

○ *Důkaz.* Mějme libovolné $r \in R^\bullet$ a $1 \in I^\bullet$. Pak nutně $r \cdot 1 \in I$ a tedy $R^\bullet \subseteq I^\bullet$. Opačna inkluze plyne z definice ideálu. □

▶ 6.3.14. Věta. Buť R okruh. Pak:

(1) $R \lhd R$;

(2) $E \lhd R$.

▶ 6.3.15. Definice.

(1) Ideál $I \lhd R$ nazveme netriviální, pokud $I \neq R$ a $I \neq E$.

(2) Okruh R označujeme jednoduchý, pokud nemá netriviální ideály.

• 6.4. Jednoduché okruhy

▶ 6.4.1. Věta. Nechť R je okruh a $I \lhd R$. Pak $I_+ \lhd R_+$. (Tedy je-li I ideál, pak je i normální podgrupou aditivní grupy R_+.)

▶ 6.4.2. Věta.

(1) Okruh R prvočíselného řádu p je jednoduchý.

(2) Libovolné těleso T je jednoduchý okruh.

◦ *Důkaz.*

(1) Pokud by R měl netrivální ideál, pak by R_+ měla netriviální normální podgrupu, ale z prvočíselnosti řádu víme, že taková normální podgrupa neexistuje.

(2) Mějme libovolný ideál $I \lhd T$. Ukážeme, že $I \neq E \Rightarrow I = T$, tedy existují pouze triviální ideály. Ideál je nenulový, tedy $(\exists a \in I^\bullet \setminus \{0\})$. Pak $a^{-1} \in T$, tedy $aa^{-1} = 1 \in I^\bullet$ a tedy $I = T$.

□

▶ 6.4.3. Poznámka. Lze definovat jednostranné ideály, ale z důkazu je vidět, že těleso nemá ani jednostranné ideály.

▶ 6.4.4. Věta. Průnik i součet libovolného systému ideálů v okruhu R je ideál v R.

◦ *Důkaz.* Mějme systém $I_\alpha \lhd R$ pro $\alpha \in J$. Označme $A = \bigcap I_\alpha$ a $B = \sum I_\alpha$

(průnik) Průnik je podokruhem, tedy stačí ukázat definiční podmínku ideálu. Mějme libovolné $a \in A$ a $r \in R^\bullet$. Pak $(\forall \alpha \in J)(a \in I_\alpha)$, tedy $(\forall \alpha \in J)(ar \in I_\alpha)$, tedy $ar \in A$.

(součet) Součet je podokruhem, tedy opět stačí ukázat definiční podmínku ideálu. Mějme libovolné $a \in B$ a $r \in R^\bullet$. Pak a je tvaru $a = k_1 \times a_{11} \dots a_{1n_1} + \dots + k_m \times a_{m1} \dots a_{mn_m}$, kde $k_i \in \mathbb{Z}$ a $a_{i\ell} \in \bigcup I_\alpha$. Tedy zvláště $a_{i1} \in I^\bullet_{\alpha_i}$ (α_i vybere příslušný ideál). Pak součin $a_{i1}a_{i2} \dots a_{in_i}$ je tvaru $a_{i1}r_i$ pro nějaké $r_i \in R^\bullet$, tedy neboť I_α je ideál, je $a_{i1}r_i \in I_\alpha$ a také $b_i = k_i \times a_{i1}r_i \in I_\alpha$. Potom $a = b_1 + \dots + b_m$. Pro libovolné $r \in R^\bullet$ je $ra = rb_1 + \dots + rb_m$ a platí $(\forall i)(rb_i \in I_{\alpha_i})$. Ale $I_{\alpha_i} \subseteq \bigcup I_\alpha \subseteq \langle \bigcup I_\alpha \rangle = B$. Z uzavřenosti B na součty je $ra \in B$ a podobným způsobem ukážeme, že $ar \in B$.

□

▶ 6.4.5. Definice. Buď $R = (M, +, \cdot)$ okruh. Hlavním ideálem generovaným prvkem $a \in M$ (značíme I_a) rozumíme nejmenší ideál v R obsahující prvek a.

▶ 6.4.6. Poznámka. Definice je korektní, neboť každý prvek leží v nějakém ideálu (přinejhorším $a \in R \lhd R$), a existuje nejmenší, neboť průnik systémem ideálů obsahujících a je ideál obsahující a a je nutně nejmenší:

$$I_a = \bigcap_{\substack{J \lhd R \\ a \in J}} J.$$

▶ 6.4.7. Lemma. Nechť R je asociativní a komutativní okruh a $a \in R$ a označme $J_a := \{ra \mid r \in R^\bullet\}$. Pak J_a je ideál a platí:

(1) Má-li R jednotku, je $I_a = J_a$ (tedy J_a je hlavní ideál generovaný a).

(2) Nemá-li R jednotku, je $I_a = \langle J_a \cup \{a\} \rangle = \{ra + k \times a \mid r \in R^\bullet, k \in \mathbb{Z}\}$.

◦ *Důkaz.* Mějme libovolné $b = ra \in J_a$, kde $r \in R$ a $a \in J_a$ a libovolné $q \in R$. Pak $bq = qb = qra \in R^\bullet a = J_a^\bullet$, tedy J_a splňuje definiční vlastnost ideálu. V hlavním ideálu gerenrovaném a leží všechny součiny tvaru ra, tedy nutně $J_a \subseteq I_a$. Pokud navíc existuje jednotka, je $a = 1a \in J_a$ a tedy $J_a = I_a$. Pokud jednotka neexistuje, je nutné J_a rozšířit o násobky a. □

▶ 6.4.8. Definice. Asociativní a komutativní okruh nazveme okruhem hlavních ideálů, je-li v něm každý ideál hlavní.

▶ 6.4.9. Příklad. Ukážeme, že $Z = (\mathbb{Z}, +, \cdot)$ je okruh hlavních ideálů. Ideály $I_m = \{sm \mid s \in \mathbb{Z}\}$ jsou hlavní. Vezměme si libovolný ideál $I \lhd Z$, pak víme, že I_+ je normální podgrupa Z_+. Ale Z_+ je cyklická, tedy i I_+ je cyklická a tedy existuje generátor m takový, že $I = I_+ = \langle m \rangle = \{k \times m \mid k \in \mathbb{Z}\} = \{sm \mid s \in \mathbb{Z}\}$. Tedy $I = I_m$ a je hlavní.

• 6.5. Homomorfismy

▶ 6.5.1. Definice. Buďte R_1, R_2 okruhy, $R_i = (M_i, +, \cdot)$. Řekneme, že $h : M_1 \to M_2$ je homomorfismus okruhů, pokud platí:

$$(\forall x, y \in M_1)\big(h(x + y) = h(x) + h(y) \ \wedge \ h(xy) = h(x)h(y)\big).$$

(Tedy h je homomorfismus na okruhu, pokud je homomorfismem na aditivním i multiplikativním grupoidu.)

Značíme $h : R_1 \to R_2$.

▶ 6.5.2. Definice. Podobně, jako na grupách, definujeme na okruzích monomorfismus, epimorfismus, izomorfismus, endomorfismus, automorfismus.

▶ 6.5.3. Definice. Okruhy R_1 a R_2 jsou izomorfní (značíme $R_1 \cong R_2$), pokud existuje izomorfismus $h : R_1 \to R_2$.

▶ 6.5.4. Lemma. $h(R_1) \Subset R_2$.

▶ 6.5.5. Věta. Je-li R_1 asociativní, resp. komutativní, resp s jednotkou, pak tutéž vlastnost má i $h(R_1)$.

▶ 6.5.6. Poznámka. Nepřenáší se vlastnost nemíti dělitele nuly a býti tělesem.

▶ 6.5.7. Definice. Jádrem homomorfismu $h : R_1 \to R_2$ rozumíme množinu $\ker h := h^{-1}(\{0\}) = \{x \in R_1^\bullet \mid h(x) = 0\}$.

▶ 6.5.8. Lemma. Nechť h je homomorfismus.

(1) $\ker h \lhd R_1$

(2) h je monomorfní (prostý) právě tehdy, když $\ker h = \{0\}$.

▶ 6.5.9. Věta. Podokruh okruhu R je ideál právě tehdy, je-li jádrem nějakého homomorfismu definovaného na R.

▶ 6.5.10. Věta (o homomorfismu okruhů). Buďte R_1, R_2 okruhy a nechť $h : R_1 \to R_2$ je homomorfismus. Potom $h(R_1) \cong R_1 / \ker h$.

▶ 6.5.11. Věta. Buďte R_1, R_2 okruhy, $h : R_1 \to R_2$ monomorfismus. Je-li R_1 bez dělitele nuly, resp. tělesem, pak má odpovídající vlastnost i podokruh $h(R_1)$ okruhu R_2.

6.6. Podílová tělesa

▶ 6.6.1. Věta. Nechť $m \geq 2$. Okruh Z_m je okruhem s děliteli nuly pro m složené, a je komutativním tělesem pro m prvočíselné.

◦ *Důkaz.*

(1) Mějme $m = uv$ takové, že $u, v < m$. Pak $T_0 = T_m = T_u T_v$ a T_u, T_v jsou dělitelé nuly.

(2) Mějme $m \in \mathbb{P}$ a nechť k je takové, že $0 < k < m$. Pak neboť $\delta(k, m) = 1$, existují $u, v \in \mathbb{Z}$ taková, že $uk + vm = 1$, z čehož $T_u T_k = T_1 - T_v T_m = T_1$ a tedy $T_u = T_k^{-1}$.

□

▶ 6.6.2. Lemma. Buď R okruh. Potom R je bez dělitelů nuly právě tehdy, lze-li v jeho multiplikativním grupoidu $R_\bullet$ krátit nenulovým prvkem, tj.

$$(\forall a, b, c \in R^\bullet, c \neq 0)\big((ac = bc \vee ca = cb) \Rightarrow a = b\big)$$

◦ *Důkaz.*

(⇒) Platí $0 = ac - bc = (a - b)c$. Neboť $c \neq 0$ a R je bez dělitelů nuly, je $a - b = 0$ a tedy $a = b$. Krácení zleva se ukáže obdobně.

(⇐) Nechť $ab = 0 = 0 \cdot b$ nebo $ba = 0 = b \cdot 0$. Tedy pro $b \neq 0$ je $a = 0$, což znamená, že nejsou oba nenulové.

□

▶ 6.6.3. Poznámka. Má-li se okruh R vnořit do tělesa, nutně nesmí mít dělitele nuly.

▶ 6.6.4. Lemma. Nechť okruh R_1 lze izomorfně vnořit do okruhu R_2 a nechť $R_1^\bullet \cap R_2^\bullet = \emptyset$. Pak existuje okruh Q takový, že $R_1 \Subset Q$ a $Q \cong R_2$.

◦ *Důkaz.* Definujme $Q^\bullet = (R_2^\bullet \setminus h(R_1)) \cup R_1^\bullet$ a definujme zobrazení $g : Q^\bullet \to R_2^\bullet$ následovně:

$$g(x) = \begin{cases} h(x) \text{ pro } x \in R_1^\bullet \\ x \text{ jinak} \end{cases}$$

Zjevně g je bijekce. To nám umožňuje definovat $Q = (Q^\bullet, \oplus, \odot)$ s operacemi $a \oplus b := g^{-1}(g(a) + g(b))$ a $a \odot b := g^{-1}(g(a) \cdot g(b))$. Pak $g(a \oplus b) = g(a) + g(b)$ a $g(a \odot b) = g(a) \cdot g(b)$, tedy g je homomorfismus a tedy izomorfismus.

Celkově tedy máme, že $Q \cong R_2$ a $R_1 \Subset Q$. □

► 6.6.5. Věta. Libovolný obor integrity R lze vnořit do komutativního tělesa.

○ *Důkaz.* Je-li $R = E$, pak jej lze vnořit do triviálního tělesa F. Tedy předpokládejme $R \neq E$.

Definujme množinu $M := \{\langle a, b\rangle \mid a, b \in R^\bullet, b \neq 0\}$. Dále definujeme $\equiv$ jako $\langle a, b\rangle \equiv \langle c, d\rangle \Leftrightarrow ad = bc$ a ukážeme, že je ekvivalencí. Reflexivita a symetrie je zřejmá, ukážeme transitivitu. Nechť $ad = bc$ a $cf = de$. Pak $adf = bcf = bed$ a z předchozího lemmatu, z nenulovosti d a z komutativity vidíme, že $af = be$.

Vezměme faktor-množinu $M/\equiv$ a označujme $\frac{a}{b}$ třídu $M/\equiv$ obsahující prvek $\langle a, b\rangle$, tedy $\langle a, b\rangle \in \frac{a}{b} \in M/\equiv$. „Zlomky“ se chovají přirozeně: $\frac{a}{b} = \frac{c}{d} \Leftrightarrow \langle a, b\rangle \equiv \langle c, d\rangle \Leftrightarrow ad = bc$. Lze také krátit nenulovým prvkem: $\frac{ae}{be} = \frac{a}{b}$.

Definujeme okruh $U_R := (M/\equiv, \oplus, \odot)$ jako $\frac{a}{b} \oplus \frac{c}{d} := \frac{ad+bc}{bd}$ a $\frac{a}{b} \odot \frac{c}{d} := \frac{ac}{bd}$. Neboť R neobsahuje dělitele nuly, nemáme ve jmenovateli nulu. Zbývá ukázat korektnost definice: Mějme $\frac{a'}{b'} = \frac{a}{b}$, tj. $a'b = ab'$, a $\frac{c'}{d'} = \frac{c}{d}$, tj. $c'd = cd'$.

Ukážeme, že $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$, tj. $bd(a'd' + b'c') \stackrel{?}{=} b'd'(ad + bc)$, tj. $bda'd' + bdb'c' \stackrel{?}{=} b'd'ad + b'd'bc$, tj. $(a'b)dd' + (c'd)bb' \stackrel{?}{=} (ab')dd' + (cd')bb'$, ale $a'b = ab'$ a $c'd = cd'$, tedy rovnost platí. Podobně lze rozepsat operaci $\odot$. □

Dále definujeme $h : R \to U_R$ jako $h(x) = \frac{xa}{a}$ pro $a \neq 0$ (nezávislost na výběru a je zřejmá). Ukážeme, že h je monomorfismus. Platí $h(x + y) = \frac{(x+y)a}{a} = \frac{xa+ya}{a} = \frac{(xa)a+(ya)a}{aa} = \frac{xa}{a} \oplus \frac{ya}{a}$ a $h(x) \odot h(y) = \frac{xa}{a} \odot \frac{ya}{a} = \frac{xaya}{aa} = \frac{xya}{a}$. Nechť $h(x) = 0$, tj. $ax = 0$, ale $a \neq 0$ a nejsou dělitelé nuly, tedy $x = 0$ a h je prosté.

Celkově tedy máme $R \cong h(R) \Subset U_R$ a podle předchozího lemmatu existuje těleso T_R takové, že $R \Subset T_R \cong U_R$.

► 6.6.6. Definice. Okruh U_R z předchozí věty nazveme <u>těleso zlomků</u>.

► 6.6.7. Poznámka.

(1) Každý zlomek tvaru $\frac{0}{b}$ je nulou.

(2) Každý zlomek tvaru $\frac{a}{a}$ je jednotkou.

(3) Platí $-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}$.

(4) Pro $a \neq 0$ je $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

(5) U_R je obor integrity s jednotkou, tedy těleso.

► 6.6.8. Definice. Těleso T_R z předchozí věty nazveme <u>podílové těleso</u> oboru itegrity R.

► 6.6.9. Lemma. Buďte R_1, R_2 obory integrity a T_1, T_2 jejich podílová tělesa. Pak $R_1 \cong R_2 \Rightarrow T_1 \cong T_2$.

○ *Důkaz.* Existuje izomorfismus $h : R_1 \to R_2$ a definujme izomorfismus $\bar{h} : U_1 \to U_2$ jako $\bar{h}\left(\frac{a}{b}\right) = \frac{h(a)}{h(b)}$. Je třeba triviálně ukázat, že obraz nezavisí na reprezentantu $\frac{a}{b}$, že $h(b) \neq 0$ a že $\bar{h}$ je izomorfismus. Tedy máme $T_1 \cong U_1 \cong U_2 \cong T_2$. □

► 6.6.10. Lemma. Těleso T_R je nejmenší těleso obsahující obor integrity R.

◦ *Důkaz.* Nechť S je libovolné těleso a $R \Subset S$. Definujeme $h : U_R \to S$ jako $h\left(\frac{a}{b}\right) = ab^{-1}$, což můžeme, protože a, b jsou prvky tělesa a $b \neq 0$. Opět definice nezávisí na reprezentantu.

Ukážeme, že zobrazení h je homomorfismus. $h\left(\frac{a}{b} \oplus \frac{c}{d}\right) = h\left(\frac{ad+bc}{bd}\right) = (ad + bc)(bd)^{-1} = add^{-1}b^{-1} + bcd^{-1}b^{-1} = ab^{-1} + cd^{-1} = h\left(\frac{a}{b}\right) + h\left(\frac{c}{d}\right)$. Zachování součinu se ověří podobně. Opomněli jsme ověřit, že prvky inverzní k prvkům z oboru integrity komutují. Tedy nechť $xy = yx$, pak $y = x^{-1}yx$ a tedy $yx^{-1} = x^{-1}y$. Opět $h\left(\frac{a}{b}\right) = 0 \Leftrightarrow ab^{-1} = 0 \Leftrightarrow a = 0$, tedy h je prosté.

Celkově dostáváme, že $T_R \cong U_R \cong h(U_R) \Subset S$. □

▶ 6.6.11. Důsledek. Podílové těleso komutativního tělesa T (jako oboru integrity) je izomorfní s T.

• **6.7.** Charakteristika tělesa

▶ 6.7.1. Poznámka. Řád jednotky 1 jako prvku aditivní grupy T_+ tělesa T je nejmenší přirozené číslo $n \in \mathbb{N}$ takové, že $n \times 1 = \underbrace{1 + \cdots + 1}_{n\text{-krát}} = 0$. Pokud $(\forall n \in \mathbb{N})(n \times 1 \neq 0)$, má jednotka nekonečný řád.

▶ 6.7.2. Lemma. Jednotka má v T_+ řád nekonečný nebo prvočíselný.

◦ *Důkaz.* Lemma dokážeme sporem. Nechť $n = uv$ a $u, v < n$. Pak $(u \times 1) \cdot (v \times 1) = (1 + \cdots + 1)(1 + \cdots + 1) = (uv) \times 1 = n \times 1 = 0$, tedy $u \times 1$ a $v \times 1$ jsou dělitelé nuly, což je spor. □

▶ 6.7.3. Definice. Řekneme, že těleso T má <u>charakteristiku</u> $p \in \mathbb{P}$, resp. 0, má-li jednotka v T_+ řád p, resp. nekonečný.

▶ 6.7.4. Důsledek.

(1) Všechna číselná tělesa (např. Q, R, C) mají charakteristiku 0.

(2) Každé konečné těleso má nenulovou charakteristiku.

(3) Těleso zbytkových tříd Z_p má charakteristiku p.

▶ 6.7.5. Věta. Buď T těleso charaktestiky p, resp. 0. Pak libovolný prvek $a \in T^\bullet$, $a \neq 0$ má v T_+ řád p, resp. nekonečný.

◦ *Důkaz.* Platí $n \times a = a + \cdots + a = 1a + \cdots + 1a = (1 + \cdots + 1)a = (n \times 1)a$. Tedy $n \times a = 0 \Leftrightarrow n \times 1 = 0$, což jsme chtěli ukázat. □

• **6.8.** Prvotěleso

▶ 6.8.1. Definice. <u>Prvotělesem</u> tělesa T rozumíme jeho nejmenší podtěleso (průnik všech jeho podtěles). Prvotěleso značíme P_T.

▶ 6.8.2. Věta. Buď T těleso charakteristiky p, resp. 0. Potom prvotěleso T je izomorfní s tělesem zbytkových tříd Z_p, resp. s tělesem racionálních čísel Q.

◦ *Důkaz.* Označme P_T prvotěleso tělesa T. Pak nutně $1 \in P_T$. Definuji $S := \{k \times 1 \mid k \in \mathbb{Z}\}$ a nutně $S \in P_T$. Platí $(k \times 1) - (\ell \times 1) = (k - \ell) \times 1 \in S$ a $(\ell \times 1)(k \times 1) = \ell k \times 1 \in S$, tedy S je podokruh okruhu T.

Definujeme $h : Z \to S$ jako $h(k) = k \times 1$. Snadno ukážeme, že h je epimorfismus. Podle věty o homomorfismu je $h(Z) = S \cong Z / \ker h$.

Zkoumejme následující 2 možné případy:

($\operatorname{ch} T = p \in \mathbb{P}$) Pak $\ker h = \{k \in \mathbb{Z} \mid k \times 1 = 0\} = I_p$. Tedy $S \cong Z / I_p = Z_p$ a protože p je prvočíslo, je Z_p těleso. Z izomorfie S je také tělesem a platí $S \subset P_T$ a neboť S je těleso a P_T je nejmenší podtěleso, platí $S = P_T$ a $P_T \cong Z_p$.

($\operatorname{ch} T = 0$) Pak $k \times 1 = 0 \Leftrightarrow k = 0$ a $\ker h = E = \{0\}$. A tedy $S \cong Z / E \cong Z$, ale Z není tělesem, je pouze oborem integrity, tedy i S je oborem integrity a existují podílová tělesa T_S a T_Z, která jsou izomorfní. Vezměme U_S a definujme $g : U_S \to T$ jako $g\left(\frac{a}{b}\right) = ab^{-1}$. O tomto zobrazení jsme již dříve ukázali, že je monomorfismus, tedy $U_S \cong g(U_S) \Subset T$ (podtělesem). Ukážeme, že $g(U_S) = P_T$.

(⊆) P_T je nejmenší podtěleso, tedy $P_T \subseteq g(U_S)$.

(⊇) Mějme libovolné $y \in g(U_S)$, $y = ab^{-1}$, kde $a, b \in S \subseteq P_T$. Ale P_T je těleso, tedy $y \in P_T$.

Tedy celkově máme $P_T = g(U_S) \cong U_S \cong T_S \cong T_Z = Q$.

□

► 6.8.3. Poznámka.

(1) Okruh Z nemá dělitele nuly, ale Z_m pro m složené mají dělitele nuly. To dává protipříklad k domněnce, že obecný homomorfismus zachová vlastnost nemíti dělitele nuly.

(2) Nechť T je jednoduchý okruh, tj. jediné jeho ideály jsou E a T. Ale všechny ideály jsou jádra všech homomorfismů. Tedy buď $\ker h = E$ a h je monomorfismus, nebo $\ker h = T$ a $h(T) = \{0\}$, což zjevně není tělesem. To dává protipříklad k domněnce, že obecný homomorfismus zachovává tělesovost.

---

7. Moduly a lineární algebry

•

7.1. Moduly

► 7.1.1. Definice. Mějme aditivní grupu $G = (M, +)$ a množinu skalárů $S \neq \emptyset$. Pro každé $\alpha \in S$ definujeme endomorfismus značený stejně $\alpha : G \to G$. Pak systém $G_S := (G, S)$ nazýváme grupa s operátory.

► 7.1.2. Definice. Přípustnou podgrupou grupy s operátory nazveme takové $H \Subset G$, že $(\forall \alpha \in S)(\forall a \in H^\bullet)(\alpha a \in H^\bullet)$.

▶ 7.1.3. Příklad.

(1) Mějme libovolnou grupu G a množinu celých čísel $\mathbb{Z}$ jako skaláry. Definujme pro $k \in \mathbb{Z}$ a $x \in G^\bullet$ hodnotu $kx := k \times x$. Pak $G_\mathbb{Z}$ je grupa s operátory.

(2) Nechť G je Abelova grupa. Označme $\mathcal{E}_G$ množinu všech endomofrismů a definujme pro $h, g \in \mathcal{E}_G$ operace $(h \oplus g)(x) := h(x) + g(x)$ a $(h \odot g)(x) := h(g(x))$. Pak $(\mathcal{E}_G, \oplus, \odot)$ tvoří okruh nazývaný okruh endomorfismů. Pak přípustnou podgrupou grupy s operátory $G_{\mathcal{E}_G}$ je taková podgrupa, která je uzavřená vůči všem endomorfismům. Přípustné podgrupy $G_{\mathcal{E}_G}$ se nazývají úplně charakteristické.

(3) Přípustné podgrupy $G_{\mathcal{A}_G}$ se nazývají charakteristické.

(4) Přípustné podgrupy $G_{\mathcal{I}_G}$ se nazývají normální. (Narozdíl od $\mathcal{E}_G$ nejsou $\mathcal{A}_G$ ani $\mathcal{I}_G$ okruhy, přesto mohou jejich prvky být skaláry.)

▶ 7.1.4. Definice. Modulem rozumíme grupu s operátory G_R, kde R je asociativní okruh s jednotkou a $(\forall \alpha, \beta \in R^\bullet)(\forall a \in G^\bullet)\big((\alpha + \beta)a = \alpha a + \beta a \wedge \alpha(\beta a) = \beta(\alpha a)\big)$. Modul G_R nazveme unitární, pokud $1 \cdot a = a$.

▶ 7.1.5. Definice. Unitární modul G_R nazveme vektorovým prostorem, pokud R je tělesem.

▶ 7.1.6. Příklad. Vezměme $G = R_+$ a $R = R$. Pak (R_+, R) je modulem.

• 7.2. Lineární algebry

▶ 7.2.1. Definice. Mějme okruh R a množinu skalárů $S \neq \emptyset$. Pak (R, S) je okruh s operátory, pokud (R_+, S) je grupa s operátory a platí $(\forall \alpha \in S)(\forall a, b \in R^\bullet)\big(\alpha(ab) = (\alpha a)b = a(\alpha b)\big)$.

▶ 7.2.2. Definice. Lineární algebra je dvojice (R, S), kde R je okruh, S je těleso a platí:

(1) (R_+, S) je unitární modul;

(2) (R, S) je okruh s operátory.

▶ 7.2.3. Poznámka. Pokud zapomeneme násobení skaláry, je lineární algebra okruhem. Pokud zapomeneme okruhové násobení, je vektorovým prostorem.

▶ 7.2.4. Příklad.

(1) $(\mathbb{C}^{n,n}, +, \cdot)$ je lineární algebra nad $\mathbb{C}$.

(2) $(\mathbb{C}^{n,n}, +, \cdot)$ je lineární algebra nad $\mathbb{R}$.

(3) C_R je lineární algebra C nad $\mathbb{R}$.

(4) R_R je lineární algebra R nad $\mathbb{R}$.

▶ 7.2.5. Definice. Algebry definované nad tělesem reálných čísel nazýváme reálné.

▶ 7.2.6. Poznámka. Mějme U těleso a $T \Subset U$ jeho podtěleso. Pak U je lineární algebra nad T a U_+ je vektorový prostor nad T.

7.3. Algebra kvaternionů

Vymyslel ji Hamilton v Dublinu 16. října 1843.

Vezměme algebru $\mathbb{C}^{2,2}$ nad $\mathbb{R}$ a uvažujme podmnožinu

$$K := \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \;\middle|\; a, b \in \mathbb{C} \right\}.$$

Ukážeme, že K je podalgebra $\mathbb{C}^{2,2}$. Uzavřenost vůči sčítání matic je zjevná, stejně tak vůči násobení reálným číslem. Zbývá nám uzavřenost vůči součinu:

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} \begin{pmatrix} c & d \\ -\bar{d} & \bar{c} \end{pmatrix} = \begin{pmatrix} ac - b\bar{d} & ad + b\bar{c} \\ -\bar{b}c - \bar{a}\bar{d} & -\bar{b}d + \bar{a}c \end{pmatrix}.$$

Tedy K nad $\mathbb{R}$ je algebrou, kterou nazýváme kvaternionová algebra a její prvky kvaterniony.

Je asociativní, není komutativní, má jednotku $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ a je algebrou s dělením (tedy K jako okruh je tělesem) — ukážeme. Pro dané a, b hledáme c, d, aby $ac - b\bar{d} = 1$ a $\bar{b}c + \bar{a}\bar{d} = 0$. Zbylé dvě rovnice jsou lineárně závislé na těchto dvou. Matice soustavy s neznámými $c, \bar{d}$ je $\left(\begin{smallmatrix} a & -b \\ \bar{b} & \bar{a} \end{smallmatrix}\right)$ a její determinant je $D = |a|^2 + |b|^2$. Tedy podle Cramerova pravidla je $c = \frac{\bar{a}}{D}$ a $\bar{d} = \frac{-\bar{b}}{D}$, tedy $d = \frac{-b}{D}$.

Zapišme $a = \alpha_1 + \alpha_2 i$ a $b = \beta_1 + \beta_2 i$, kde $\alpha_{1,2}, \beta_{1,2} \in \mathbb{R}$. Pak

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = \begin{pmatrix} \alpha_1 + \alpha_2 i & \beta_1 + \beta_2 i \\ -\beta_1 + \beta_2 i & \alpha_1 - \alpha_2 i \end{pmatrix} = \alpha_1 \underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}}_{e} + \alpha_2 \underbrace{\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}}_{i} + \beta_1 \underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_{j} + \beta_2 \underbrace{\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}}_{k}.$$

Tedy $\dim K = 4$ a (e, i, j, k) tvoří bázi K. Prvky báze se násobí podle následující tabulky (první činitel vlevo, druhý nahoře):

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Označme $Q_8 := \{1, -1, i, -i, j, -j, k, -k\}$. Pak Q_8 s násobením podle tabulky je grupa nazývaná kvaternionová grupa. V úvahu přicházejí čtyř- a dvouprvkové podgrupy. Jsou tři 4prvkové podgrupy, např. $\{1, -1, i, -i\}$, a jedna 2prvková $\{1, -1\}$. První 3 mají index 2 a jsou tudíž normální, taktéž 2prvková je normální. Tedy Q_8 je příklad neabelovské grupy, která má všechny podgrupy normální. Takové grupy se nazývají hamiltonovské.

▶ 7.3.1. Věta (Frobenius). Buď A reálná asociativní konečnědimenzionální lineární algebra bez dělitelů nuly. Je-li A komutativní, potom je izomorfní s algebrou C_R nebo R_R. Není-li A komutativní, pak je izomorfní s algebrou kvaternionů.

8. Teorie svazů

8.1. Svazy

▶ 8.1.1. Definice. Svazem (angl. lattice) rozumíme algebru $S = (M, \wedge, \vee)$ se dvěma binárními operacemi takovou, že pro libovolné $a, b, c \in M$ platí:

(1) $a \wedge b = b \wedge a, \quad a \vee b = b \vee a$ (komutativní zákon);

(2) $(a \wedge b) \wedge c = a \wedge (b \wedge c), \quad (a \vee b) \vee c = a \vee (b \vee c)$ (asociativní zákon);

(3) $a \wedge (b \vee a) = a, \quad a \vee (b \wedge a) = a$ (zákon absorpce).

Operaci $\wedge$ nazýváme průsek a operaci $\vee$ spojení.

▶ 8.1.2. Lemma. Ve svazu $S = (M, \wedge, \vee)$ platí pro libovolný prvek $a \in M$, že $a \wedge a = a$ a $a \vee a = a$ (tzv. idempotentnost)

◦ *Důkaz.* $a \wedge a = a \wedge (a \vee (b \wedge a)) = a$, druhá rovnost symetricky. □

▶ 8.1.3. Věta (princip duality v teorii svazů). Máme-li formuli v teorii svazů, která platí ve všech svazech, pak duální formule vzniklá prohozením operací průseku a spojení opět platí ve všech svazech.

8.2. Svazově uspořádaná množina

▶ 8.2.1. Poznámka. Připomeneme důležité pojmy pro uspořádané množiny $(M, \leq)$.

(1) Horní závora množiny $A \subseteq M$ je každé takové $a \in M$, že $(\forall x \in A)(x \leq a)$.

(2) Má-li množina horních závor první prvek, nazveme jej supremum A. Pro $s = \sup A$ platí:

(a) $(\forall a \in A)(a \leq s)$;
(b) $\big(\forall t \in M\big)\big((\forall a \in A)(a \leq t) \Rightarrow s \leq t\big)$.

(3) $\sup \emptyset$ je první prvek množiny M (pokud existuje).

(4) $\sup M$ je poslední prvek množiny M (pokud existuje).

▶ 8.2.2. Definice. Řekneme, že uspořádaná množina $(M, \leq)$ je svazově uspořádaná, má-li v ní libovolná 2prvková množina infimum a supremum.

▶ 8.2.3. Lemma. Pro libovolné prvky svazu platí, že

$$a \wedge b = a \iff a \vee b = b.$$

◦ *Důkaz.*

(⇒) $a \vee b = (a \wedge b) \vee b = b$.

(⇐) $a \wedge b = a \wedge (a \vee b) = a$.

□

▶ 8.2.4. Věta.

(1) Buď $S = (M, \wedge, \vee)$ svaz. Definujme-li na M binární relaci $\leq$ jako $a \leq b \Leftrightarrow a \wedge b = a$, pak $(M, \leq)$ je svazově uspořádaná.

(2) Buď $(M, \leq)$ svazově uspořádaná množina. Definujeme-li na M binární operace $\wedge, \vee$ jako $a \wedge b := \inf\{a, b\}$ a $a \vee b := \sup\{a, b\}$, pak $(M, \wedge, \vee)$ je svazem.

◦ *Důkaz.*

(1) **(reflexivita)** $a \leq a \Leftrightarrow a \wedge a = a$.

(antisymetrie) $a \wedge b = a$ a $b \wedge a = b$, a z komutativity plyne $a = b$.

(transitivita) Nechť $a \leq b$ a $b \leq c$, pak $a \wedge c = a \wedge b \wedge c = a \wedge b = a$.

(je svazové) Ukážeme, že $\inf\{a, b\} = a \wedge b$. Obdobně $\sup\{a, b\} = a \vee b$.

(2) **(komutativita)** $a \wedge b = \inf\{a, b\} = \inf\{b, a\} = b \wedge a$.

(asociativita) $(a \wedge b) \wedge c = \inf\{\inf\{a, b\}, c\} = \inf\{a, b, c\} = \inf\{a, \inf\{b, c\}\} = a \wedge (b \wedge c)$ s využitím následujícího lemmatu a faktu, že každá 2prvková má infimum.

(pohlcení) $\inf\{a, \sup\{b, a\}\} = a$ z definice.

Druhý z každé dvojice axiomů dokážeme podobně.

□

▶ 8.2.5. Lemma. Mějme uspořádanou množinu $(M, \leq)$ a $a, b, c \in M$. Potom pokud existuje $\inf\{\inf\{a, b\}, c\} =: i$, je $i = \inf\{a, b, c\}$. Pokud je navíc $(M, \leq)$ svazově uspořádaná, platí $i = \inf\{a, \inf\{b, c\}\}$.

◦ *Důkaz.*

($i \leq a, b, c$) Je $i \leq c$ a $i \leq \inf\{a, b\}$, tedy $i \leq a, b$.

($d \leq a, b, c \Rightarrow d \leq i$) Neboť $d \leq a$ a $d \leq b$, je $d \leq \inf\{a, b\}$, a současně je $d \leq c$, tedy $d \leq \inf\{c, \inf\{a, b\}\} = i$.

Pokud je navíc uspořádaní svazové, pak existuje infimum 2prvkové množiny $\{b, c\}$ a také infimum 2prvkové množiny $\{a, \inf\{b, c\}\}$. A tedy je podle prvního tvzení $\inf\{a, \inf\{b, c\}\} = \inf\{a, b, c\} = i$. □

▶ 8.2.6. Poznámka. Operace jsou jednoznačně svázané, neboť např. pomocí $\wedge$ definujeme $\leq$ a to nám definuje $\vee$.

▶ 8.2.7. Lemma. Buď $S = (M, \wedge, \vee)$ svaz a nechť $a, b, c \in M$. Potom platí

$$(a \leq b) \Rightarrow (a \wedge c \leq b \wedge c \text{ et } a \vee c \leq b \vee c).$$

◦ *Důkaz.* Z definice: $a \wedge c \wedge b \wedge c = a \wedge c$, $a \vee c \vee b \vee c = b \vee c$. □

▶ 8.2.8. Definice. Mějme svaz $S = (M, \wedge, \vee)$. Pak pro $N \subseteq M$ je $T = (N, \wedge, \vee)$ podsvazem svazu S, pokud je N svazem, tj. pokud je neprázdná a uzavřená vůči oběma operacím.

▶ 8.2.9. Příklad.

(1) Množinový svaz $S = (M, \cap, \cup)$, kde M je systém množin uzavřený na operace. Speciálním případem je $M = \mathcal{P}(A)$, kde snadno ověříme platnost axiomů svazu. Svazové uspořádání množinového svazu je inkluze $\subseteq$.

Mějme A množinu a $B \subseteq A$ její podmnožinu. Pak $(\mathcal{P}(B), \cap, \cup)$ je podsvazem svazu $(\mathcal{P}(A), \cap, \cup)$.

Dále např. ς-algebry tvoří monžinové svazy.

(2) Pro libovolné $a \in S^\bullet$ je $(\{a\}, \wedge, \vee)$ podsvazem S.

Pro libovolné $a, b \in S^\bullet$ je $(\{a, b\}, \wedge, \vee)$ podvazem S, pokud jsou srovnatelné.

(3) Úplně uspořádaná množina je uspořádaná svazově a supremum a infimum přechází v maximum a minimum (vždy to bude jeden z obou prvků). Příkladem jsou číselné množiny $(\mathbb{N}_0, \leq)$ či $(\mathbb{R}, \leq)$.

(4) Mějme uspořádání $(\mathbb{N}_0, |)$ s uspořádáním „dělí“. Pak $k \wedge l$ je největší (podle $|$) takové d, že $d \,|\, k$ a $d \,|\, l$, tj. $k \wedge l = \delta(k, l)$. Obdobně $k \vee l = \nu(k, l)$.

(5) Mějme $G = (M, \cdot)$ grupu a označme M_G systém všech jejích podgrup. Označme $(\wedge) = (\cap)$. Pak umíme definovat $(\leq)$ jako $a \leq b \Leftrightarrow a \cap b = a \Leftrightarrow a \subseteq b$. Tedy průsek i relace jsou stejné jako v množinovém svazu, ale víme, že sjednocení nemůže být spojením. Definujeme ji $a \vee b := \sup\{a, b\}$, to je nejmenší podgrupa G obsahující a i b, což je ab. Tedy platí $(\vee) = (\cdot)$.

(6) $N_G = (N_G^\bullet, \cap, \cdot)$ je svaz všech normálních podgrup grupy G. Pak N_G je podsvazem svazu S_G.

(7) Podobně tvoří svazy systémy podokruhů, ideálů, podtěles, podprostorů vektorového prostoru, doplněné o průnik a součet.

▶ 8.2.10. Definice. Mějme $a, b \in S^\bullet$, $a < b$. Pak intervalem nazveme množinu $\langle a, b\rangle = \{x \,|\, a \leq x \leq b\}$.

▶ 8.2.11. Lemma. Interval $\langle a, b\rangle$ je podsvazem S.

◦ *Důkaz.* Mějme $x, y \in \langle a, b\rangle$. Ukážeme, že $x \wedge y \in \langle a, b\rangle$. Platí $x \geq a$ a $y \geq a$, tedy $x \wedge y \geq a \wedge y \geq a \wedge a = a$. Obdobně pro b a pro druhou operaci. □

•

8.3. Ideály

▶ 8.3.1. Definice. Buď $S = (M, \wedge, \vee)$ svaz. Ideálem rozumíme libovolný jeho podsvaz I takový, že platí

$$(\forall a \in I)(\forall s \in M)(a \wedge s \in I).$$

▶ 8.3.2. Lemma. Buďte $S = (M, \wedge, \vee)$ svaz a I jeho podsvaz. Následující tvrzení jsou ekvivalentní:

(1) $(\forall a \in I)(\forall s \in M)(a \wedge s \in I)$ (tj. I je ideál);

(2) $(\forall a \in I)(\forall b \in S)(b \leq a \Rightarrow b \in I)$;

(3) $(\forall a, b \in S)(a \vee b \in I \Rightarrow a, b \in I)$.

◦ *Důkaz.*

(1 ⇒ 2) Mějme $a \in I$ a $b \leq a$. Pak podle předpokladu $a \wedge b \in I$, ale současně $a \wedge b = b$, tedy $b \in I$.

(2 ⇒ 3) Buď $a \vee b \in I$. Platí $a \leq a \vee b$ a $b \leq a \vee b$ a podle (2) je $a \vee b \in I$.

(3 ⇒ 1) Mějme $a \in I$ a $s \in M$. Pak $a = a \vee (a \wedge s) \in I$ a tedy $a \wedge s \in I$.

□

▶ 8.3.3. Důsledek. Ideály ve svazu S jsou takové $I \subseteq M$, $I \neq \emptyset$, že platí $(\forall a, b \in M)(a, b \in I \Leftrightarrow a \vee b \in I)$.

▶ 8.3.4. Lemma. Buďte S svaz a $a \in M$. Pak množina $I_a := \{x \in M \mid x \leq a\}$ je ideálem.

◦ *Důkaz.* I_a je uzavřená vůči $\vee$ a platí (2) v 8.3.2. □

▶ 8.3.5. Definice. Ideál $I_a := \{x \in M \mid x \leq a\}$ nazýváme hlavní ideál generovaný prvkem a. Je-li ve svazu každý ideál hlavní, nazveme jej svaz hlavních ideálů.

▶ 8.3.6. Definice. Buď $S = (M, \wedge, \vee)$ svaz. Filtrem rozumíme libovolný jeho podsvaz F takový, že platí

$$(\forall a \in F)(\forall s \in M)(a \vee s \in F).$$

• 8.4. Izomorfismus svazů

▶ 8.4.1. Definice. Buďte $S_1 = (M_1, \wedge, \vee)$ a $S_2 = (M_2, \wedge, \vee)$ svazy. Zobrazení $h : M_1 \to M_2$ nazveme homomorfismus, platí-li

$$(\forall x, y \in M_1)(h(x \wedge y) = h(x) \wedge h(y) \text{ et } h(x \vee y) = h(x) \vee h(y)).$$

Izomorfismus je takový homomorfismus, který je bijektivní.

▶ 8.4.2. Lemma. Homomorfismus svazů je izotonní zobrazení.

◦ *Důkaz.* Mějme $h : S_1 \to S_2$ a $x, y \in S_1^{\bullet}$, $x \leq y$. Potom $h(x) \wedge h(y) = h(x \wedge y) = h(x)$, tedy $h(x) \leq h(y)$. □

▶ 8.4.3. Věta. Buďte $S_1 = (M_1, \wedge, \vee)$ a $S_2 = (M_2, \wedge, \vee)$ svazy. Zobrazení $h : M_1 \to M_2$ je izomorfismem svazů právě tehdy, je-li izomorfismem svazově uspořádaných množin.

◦ *Důkaz.* Pro obě implikace je předpokladem bijekce, a tedy existence h^{-1}.

(⇒) Podle předchozího lemmatu je $x \leq y \Rightarrow h(x) \leq h(y)$. Zbývá tedy opačná implikace. Předpokládejme $h(x) \wedge h(y) = h(x)$. Potom díky bijekci je $x \wedge y = x$ a tedy $x \leq y$.

(⇐) Platí $x \wedge y \leq x$, tedy $h(x \wedge y) \leq h(x)$ a $h(x \wedge y)$ je dolní závora $h(x)$, a podobně je dolní závorou $h(y)$. Mějme libovolné $d \in S_2^\bullet$ takové, že $d \leq h(x)$ a $d \leq h(y)$. Neboť h je bijekce, existuje $c \in S_1$ takové, že $h(c) = d$. Platí $h(c) \leq h(x)$ a $h(c) \leq h(y)$, čili $c \leq x$ a $c \leq y$, a tedy $c \leq \inf\{x, y\}$ a konečně $d = h(c) \leq h(x \wedge y)$. Tedy každá dolní závora $h(x), h(y)$ je nejvýše rovna $h(x \wedge y)$. Tedy $h(x) \wedge h(y) = h(x \wedge y)$. Obdobně ukážeme, že $h(x) \vee h(y) = h(x \vee y)$.

□

► 8.4.4. Definice. Má-li svaz nejmenší (první), resp. největší (poslední) prvek, nazveme jej nulou, resp. jednotkou a značíme 0, resp. 1.

► 8.4.5. Příklad.

(1) Mějme množinu A a množinový svaz $(\mathcal{P}(A), \cap, \cup)$ s upořádáním $\subseteq$. Pak jednotkou je A a nulou je $\emptyset$.

(2) Mějme svaz $(\mathbb{N}_0, \delta, \nu)$ s uspořádáním $(|)$. Pak jednotkou je číslo 0 (platí $n \mid 0$) a nulou je číslo 1 (platí $1 \mid n$).

► 8.4.6. Lemma. Libovolný minimální prvek svazu je nulou. Libovolný maximální prvek svazu je jednotkou.

◦ *Důkaz.* Ukážeme pouze první tvrzení, druhé lze ukázat obdobně. Mějme m minimální a libovolné $x \in S^\bullet$. Pak $x \wedge m \leq m$, ale to je možné jen tehdy, když $x \wedge m = m$ a tedy $m \leq x$. Tedy m je první a je nulou. □

• 8.5. Úplné svazy

► 8.5.1. Definice. Svaz $S = (M, \wedge, \vee)$ nazveme úplným svazem, má-li v něm libovolná podmnožina $N \subseteq M$ infimum i supremum.

► 8.5.2. Poznámka. V každém svazu existuje infimum a supremum konečné podmnožiny. V úplném svazu vyžadujeme existenci infima a suprema pro každou (prázdnou, konečnou, spočetnou, nespočetnou) podmnožinu.

► 8.5.3. Lemma. Úplný svaz má nulu a jednotku.

◦ *Důkaz.*

(1) $1 = \sup M = \inf \emptyset$.

(2) $0 = \inf M = \sup \emptyset$.

□

▶ 8.5.4. Příklad. V množinovém svazu $S = (\mathcal{P}(M), \cap, \cup)$ je infimem $\mathcal{A} \subseteq \mathcal{P}(M)$ množina $\bigcap \mathcal{A} \subseteq M$ a supremem $\bigcup \mathcal{A} \subseteq M$, tedy S je úplný svaz.

▶ 8.5.5. Věta (o pevném bodě). Buď $S = (M, \wedge, \vee)$ úplný svaz a buď $f : M \to M$ izotonie. Pak existuje pevný bod izotonie f, tj.

$$(\exists u \in M)(f(u) = u).$$

◦ *Důkaz.* Definujeme $U = \{a \in M \mid f(a) \geq a\}$. Jistě $0 \in U$, tedy U je neprázdná. Označme $u := \sup U$. Mějme libovolné $a \in U$, pak $u \geq a$ a z izotonie je $f(u) \geq f(a) \geq a$, tedy $f(u)$ je horní závora U a tedy $u \leq f(u)$. Z izotonie dále dostáváme, že $f(u) \leq f(f(u))$ a tedy $f(u) \in U$, tedy $f(u) \leq u$. Celkově máme $f(u) = u$. □

▶ 8.5.6. Věta. Buď $(M, \leq)$ uspořádaná množina. Má-li každá podmnožina M infimum, pak má každá podmnožina M supremum.

◦ *Důkaz.* Mějme $N \subseteq M$. Nechť Z je množina horních závor N. Dále $Z \neq \emptyset$, neboť v ní je největší prvek M, což je $\inf \emptyset$. Pokud $N = \emptyset$, pak $\sup N$ je $\inf M$.

Nyní máme $(\forall n \in N)(\forall z \in Z)(n \leq z)$. Tedy každý prvek N je dolní závorou Z a platí $n \leq \inf Z$, jehož existenci předpokládáme. A neboť $(\forall n \in N)(n \leq \inf Z)$, tedy $\inf Z$ je horní závora a je nemenší z nich. Tedy $\sup N = \inf Z$. □

▶ 8.5.7. Důsledek. Buď $(M, \leq)$ uspořádaná množina. Má-li každá podmnožina M supremum, pak má každá podmnožina M infimum.

▶ 8.5.8. Důsledek. Buď $(M, \leq)$ uspořádaná množina. Má-li každá podmnožina M infimum, nebo má-li každá podmnožina M supremum, pak $(M, \wedge, \vee)$ je úplný svaz.

▶ 8.5.9. Lemma. Buď $S = (M, \wedge, \vee)$ úplný svaz. Potom průnik libovolného systému ideálů v S je ideál.

◦ *Důkaz.* Označme J_α jednotlivé ideály a $I := \bigcap J_\alpha$. Neboť $0 \in M$ a $0 \in J_\alpha$, je $0 \in I$ a $I \neq \emptyset$. Dále platí $a \in I \Leftrightarrow (\forall \alpha)(a \in J_\alpha)$ a pro všechna α je $(\forall a \in J_\alpha)(\forall s \in M)(a \wedge s \in I)$, tedy máme $(\forall a \in I)(\forall s \in M)(a \wedge s \in I)$, což je definiční podmínka ideálu. □

▶ 8.5.10. Definice. Řekneme, že svaz S_1 lze izomorfně vnořit do svazu S_2, existuje-li monomorfismus $h : S_1 \to S_2$. Potom platí $S_1 \cong h(S_1) \Subset S_2$.

▶ 8.5.11. Věta. Libovolný svaz lze izomorfně vnořit do úplného svazu.

◦ *Důkaz.* Předpokládejme, že svaz $S_0 = (M_0, \wedge, \vee)$ nemá nulu. Pak definujeme množinu $M := M_0 \cup \{0\}$ a pokládáme $(\forall x \in M_0)(0 < x)$. Tedy $S_0 \Subset S := (M, \wedge, \vee)$.

Označme $\mathfrak{I}_S$ množinu všech ideálů svazu S. Je neprázdná, neboť např. $\{0\}, S \in \mathfrak{I}_S$. Pak $(\mathfrak{I}_S, \subseteq)$ je uspořádaná množina. Pro libovolné $\mathcal{N} \subseteq \mathfrak{I}_S$ je $\inf \mathcal{N} = \bigcap \mathcal{N} \in \mathfrak{I}_S$, a pokud označíme $\mathcal{Z}_\mathcal{N}$ množinu všech horních závor $\mathcal{N}$, platí $\sup \mathcal{N} = \inf \mathcal{Z}_\mathcal{N} = \bigcap \{I \in \mathfrak{I}_S \mid (\forall J \in \mathcal{N})(J \subseteq I)\}$. Tedy pokud položíme $I \wedge J := I \cap J$ a $I \vee J := \bigcap \{K \in \mathfrak{I}_S \mid I, J \subseteq K\}$, je $\mathfrak{U}_S := (\mathfrak{I}_S, \wedge, \vee)$ úplný svaz.

Definujeme zobrazení $h : M \to \mathcal{I}_S$ jako $h(a) = I_a$. Ukážeme, že h je monomorfismus svazů, tj. pokud označíme $\mathcal{H}_S$ množinu všech hlavních ideálů S, máme $h : M \xrightarrow{\text{na}} \mathcal{H}_S$.

(h je prosté) Nechť $h(a) = h(b)$. Pak $I_a = I_b$, tedy $a \leq b$ a $b \leq a$, tedy $a = b$.

(h je množinový izomorfismus $(M, \leq)$ a $(\mathcal{H}_S, \subseteq)$) Mějme $a, b \in M$. Pak $a \leq b \Leftrightarrow I_a \subseteq I_b \Leftrightarrow h(a) \subseteq h(b)$.

(h je svazový izomorfismus) Vyplývá z předchozího bodu a předchozího výkladu.

□

▶ 8.5.12. Příklad. Věta nám umožňuje přechod od $\mathbb{Q}$ k $\mathbb{R}$. Hlavními ideály v $(\mathbb{Q}, \leq)$ jsou $I_a = \{x \in \mathbb{Q} \mid x \leq a\}$. A všemi ideály jsou $\{x \in \mathbb{Q} \mid x \leq r\}$ a $\{x \in \mathbb{Q} \mid x < r\}$ pro všechna $r \in \mathbb{R}$.

• 8.6. Distributivní svazy

▶ 8.6.1. Věta. Buď $S = (M, \wedge, \vee)$ libovolný svaz. Pak pro libovolné prvky $a, b, c \in M$ platí:

(1) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$;

(2) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$;

(3) je-li $a \leq c$, platí $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

◦ *Důkaz.*

(1) Platí $b \leq b \vee c \Rightarrow a \wedge b \leq a \wedge (b \vee c)$ a podobně $a \wedge c \leq a \wedge (b \vee c)$. Tedy $a \wedge (b \vee c)$ je horní závora $\{a \wedge c, a \wedge b\}$ a tedy je větší nebo rovno než $\sup\{a \wedge c, a \wedge b\} = (a \wedge c) \vee (a \wedge b)$.

(2) Symetricky z duality.

(3) Platí $a \vee c = c$, tedy podle (2) je $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$.

□

▶ 8.6.2. Definice. Svaz $S = (M, \wedge, \vee)$ nazveme distributivní, pokud pro libovolné $a, b, c \in M$ platí:

(D1) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;

(D2) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

▶ 8.6.3. Poznámka. Pro rovnosti máme ve všech svazech zaručeno platnost jedné nerovnosti. Stačí tedy dokázat nerovnosti opačné než v předchozí větě.

▶ 8.6.4. Lemma. (D1) $\Rightarrow$ (D2).

◦ *Důkaz.* Vyjdu z pravé strany (D2) a použiji (D1): $(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee ((a \vee b) \wedge c) = a \vee ((a \wedge c) \vee (b \wedge c)) = (a \vee (a \wedge c)) \vee (b \wedge c) = a \vee (b \wedge c)$. □

▶ 8.6.5. Příklad. Příklady distributivních svazů:

(1) množinové svazy;

(2) úplně uspořádané množiny;

(3) $(\mathbb{N}_0, |) = (\mathbb{N}_0, \delta, \nu)$.

▶ 8.6.6. Příklad. Svazy podgrup, normálních podgrup, ... nejsou obecně distributivní.

▶ 8.6.7. Věta. Libovolný podsvaz i libovolný homomorfní obraz distributivního svazu je distributivní.

◦ *Důkaz.* Distributivita je obecná podmínka, tedy se po zmenšení nosiče nemůže porušit. Homomorfismus zachovává průsek i spojení, tedy zachovává distributivitu. □

▶ 8.6.8. Definice. Buď $S = (M, \wedge, \vee)$ svaz. Filtr F se nazývá ultrafiltr, je-li $F \neq M$ a platí

$$(\forall a, b \in M)(a \vee b \in F \Rightarrow (a \in F \text{ vel } b \in F)).$$

Množinu všech ultrafiltrů na S označujeme $\mathcal{U}_S$.

▶ 8.6.9. Poznámka. V definiční podmínce ultrafiltru platí z definice filtru i zpětná implikace.

▶ 8.6.10. Poznámka. V matematické logice hrají filtry důležitou roli, pokud položíme spojení jako „nebo“ a průsek jako „a zároveň“, pak podmínka ultrafiltru vyjadřuje, kdy je konjunkce pravdivá. Podmínka filtru pak bude $a \wedge b \in F \Leftrightarrow (a \in F \text{ et } b \in F)$.

▶ 8.6.11. Příklad. Mějme $S = (\mathcal{P}(A), \cap, \cup)$ a $a \in A$, tedy $\{a\} \in \mathcal{P}(A)$. Pak definujeme hlavní filtr $F_{\{a\}} := \{B \in \mathcal{P}(A) \mid \{a\} \subseteq B\} = \{B \subseteq A \mid a \in B\}$. Pak $F_{\{a\}} \not\ni \emptyset$, tedy $F_{\{a\}} \neq \mathcal{P}(A)$.
Mějme $B_1, B_2 \in \mathcal{P}(A)$ a nechť $a \in B_1 \cup B_2$, pak $a \in B_1$ nebo $a \in B_2$, tedy $B_1 \in F_{\{a\}}$ nebo $B_2 \in F_{\{a\}}$. Tedy $F_{\{a\}}$ je ultrafiltr.
Ale $F_{\{a,b\}}$ pro $a \neq b$ není ultrafiltr.

▶ 8.6.12. Definice. Buď $S = (M, \wedge, \vee)$ a nechť $\emptyset \neq N \subseteq M$. Pak definujeme $\langle N \rangle$ jako nejmenší filtr ve svazu S obsahující N:

$$\langle N \rangle = \bigcap \{F \in \mathcal{F}_S \mid N \subseteq F\}.$$

▶ 8.6.13. Lemma. Buďte S svaz, F filtr ve svazu S a buď $a_0 \in S^\bullet$, dále označme $H := \{x \in S^\bullet \mid (\exists d \in F)(x \geq d \wedge a_0)\}$ Potom $\langle F \cup \{a_0\} \rangle = H$.

◦ *Důkaz.*

(⊇) Pokud $d \in F$, je $d \wedge a_0 \in \langle F \cup \{a_0\} \rangle$ a tedy $x = x \vee (d \wedge a_0) \in \langle F \cup \{a_0\} \rangle$.

(⊆) Ukážeme, že $F \cup \{a_0\} \subseteq H$. Pro $d \in F$ platí, že $d \geq d \wedge a_0$. Dále mějme libovolné $d \in F$, pak $a_0 \geq d \wedge a_0$. Pokud ukážeme, že H je filtr, bude nutně nejmenší filtr nad $F \cup \{a_0\}$ jeho podmnožinou.

Mějme $x_1 \geq d_1 \wedge a_0$ a $x_2 \geq d_2 \wedge a_0$ pro nějaká $d_{1,2} \in F$, pak $x_1 \wedge x_2 \geq d_1 \wedge a_0 \wedge x_2 \geq d_1 \wedge a_0 \wedge d_2 \wedge a_0$. Položme $d := d_1 \wedge d_2 \in F$, pak $x_1 \wedge x_2 \geq d \wedge a_0$, tedy $x_1 \wedge x_2 \in H$.

□

▶ 8.6.14. Lemma. Sjednocení řetězce filtrů $\mathcal{R}$ je filtr.

◦ *Důkaz.*

(1) $a \in \bigcup \mathcal{R}, b \in S^\bullet, b \geq a$. $(\exists F)(a \in F \in \mathcal{R})$, tedy $b \in F$, tedy $b \in \bigcup \mathcal{R}$.

(2) $a, b \in \bigcup \mathcal{R}$. Pak $a \in F_1$, $b \in F_2$, bez újmy na obecnosti nechť $F_1 \subseteq F_2$. Potom $a, b \in F_2$ a tedy $a \wedge b \in F_2 \subseteq \bigcup \mathcal{R}$.

□

▶ 8.6.15. Lemma. Buďte $S = (M, \wedge, \vee)$ distributivní svaz, $a, b \in M$ a nechť neplatí $a \leq b$ (tedy $a > b$ nebo nejsou srovnatelné). Potom existuje ultrafiltr F svazu S tak, že $a \in F$ a současně $b \notin F$.

◦ *Důkaz.* Nechť $\mathcal{F}$ je množina všech filtrů, které obsahují a, ale neobsahují b, tedy platí $\mathcal{F} = \{F \in \mathcal{F}_S \mid a \in F \text{ et } b \notin F\}$. Nutně $F_a = \{x \in S \mid x \geq a\} \not\ni b$, tedy $F_a \in \mathcal{F}$. V $\mathcal{F}$ uspořádané inkluzí má libovolný řetězec $\mathcal{R}$ horní závoru $F = \bigcup \mathcal{F}$, která podle předcházejícího lemmatu je opět filtrem, a tedy triviálně $F \in \mathcal{F}$, neboť $a \in F$ et $b \notin F$. Dle Zornova lemmatu existuje v $\mathcal{F}$ maximální prvek F_0. Ukážeme sporem, že F_0 je ultrafiltr.

Nechť F_0 není ultrafiltr. Tedy existují $a_1, a_2 \in S$ takové, že $a_1 \vee a_2 \in F_0$, ale $a_1 \notin F_0$ ani $a_2 \notin F_0$. Definujme $F_1 := \langle F_0 \cup \{a_1\} \rangle$ a $F_2 := \langle F_0 \cup \{a_1\} \rangle$, přičemž $F_i \supsetneq F_0$ Ukážeme sporem, že $F_1 \in \mathcal{F}$ vel $F_2 \in \mathcal{F}$ a tím vytvoříme spor s maximalitou F_0. Tedy musíme ukázat, že $b \notin F_1$ vel $b \notin F_2$.

Nechť $b \in F_1$ et $b \in F_2$. Platí $F_i = \{x \mid (\exists c_i \in F_0)(x \geq c_i \wedge a_i)\}$, tedy i pro b existují c_i tak, že $b \geq c_1 \wedge a_1$ a $b \geq c_2 \wedge a_2$. Položme $c := c_1 \wedge c_2 \in F_0$, tedy $b \geq c \wedge a_1$ a $b \geq c \wedge a_2$, tedy $b \geq (c \wedge a_1) \vee (c \wedge a_2)$ a díky distributivitě je $b \geq c \wedge (a_1 \vee a_2) \in F_0$, neboť $c \in F_0$, $a_1 \vee a_2 \in F_0$. Ale filtr je uzavřený vůči větším prvkům, tedy $b \in F_0$, což je spor.

Tedy máme $F_1 \in \mathcal{F}$ vel $F_2 \in \mathcal{F}$, což je spor s maximalitou F_0 v $\mathcal{F}$. □

▶ 8.6.16. Věta (Stone). Libovolný distributivní svaz je izomorfní s nějakým množinovým svazem. Jinými slovy: libovolný distributivní svaz lze izomorfně vnořit do svazu všech podmnožin nějaké množiny.

◦ *Důkaz.* Mějme $S = (M, \wedge, \vee)$ distributivní svaz. Označme $\mathcal{U} = (\mathcal{P}(\mathcal{U}_S), \cap, \cup)$. Definujeme $h : M \to \mathcal{P}(\mathcal{U}_S)$ jako $h(x) := \{F \in \mathcal{U}_S \mid x \in F\}$. Ukážeme, že h je monomorfismus.

(injekce) Mějme $a, b \in M$, $a \neq b$, tj. (non $a \leq b$) vel (non $b \leq a$). Pak $(\exists F_1 \in \mathcal{U}_S)(a \in F_1 \text{ et } b \notin F_1)$ vel $(\exists F_2 \in \mathcal{U}_S)(b \in F_1 \text{ et } a \notin F_2)$, tedy $(\exists F_1 \in h(a) \smallsetminus h(b))$ vel $(\exists F_2 \in h(b) \smallsetminus h(a))$, tedy $h(a) \neq h(b)$.

($h(a \wedge b) = h(a) \cap h(b)$) Mějme libovolné $F \in \mathcal{U}_S$. Pak $F \in h(a \wedge b) \Leftrightarrow a \wedge b \in F \overset{\text{filtr}}{\Leftrightarrow} (a \in F$ et $b \in F) \Leftrightarrow (F \in h(a)$ et $F \in h(b)) \Leftrightarrow F \in h(a) \cap h(b)$.

($h(a \vee b) = h(a) \cup h(b)$) Mějme libovolné $F \in \mathcal{U}_S$. Pak $F \in h(a \vee b) \Leftrightarrow a \vee b \in F \overset{\text{ultrafiltr}}{\Leftrightarrow} (a \in F$ vel $b \in F) \Leftrightarrow (F \in h(a)$ vel $F \in h(b)) \Leftrightarrow F \in h(a) \cup h(b)$.

Celkově tedy máme $S \cong h(S) \overset{\text{svaz}}{\Subset} U$. □

8.7. Modulární svazy

▶ 8.7.1. Definice. Svaz $S = (M, \wedge, \vee)$ nazveme modulární, platí-li pro libovolné $a, b, c \in M$, $a \leq c$, vztah $a \vee (b \wedge c) = (a \vee b) \wedge c$.

▶ 8.7.2. Věta. Libovolný distributivní svaz je modulární.

◦ *Důkaz.* Nechť $a \leq c$, tedy $c = a \vee c$ Pak $a \vee (b \wedge c) \overset{(D2)}{=} (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$. □

▶ 8.7.3. Lemma. Svaz S je modulární právě tehdy, když pro libovolné $a, b, c \in S^\bullet$ platí

$$a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c).$$

◦ *Důkaz.*

(⇒) V definičním vztahu položíme místo c spojení $a \vee c \geq a$. Dostaneme přímo dokazovanou rovnost.

(⇐) Pro libovolné $c \geq a$ je $a \vee c = c$, a tedy $a \vee (b \wedge c) = a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$.

□

▶ 8.7.4. Věta. Svaz všech normálních podgrup libovolné grupy G je modulární.

◦ *Důkaz.* Nerovnost $\geq$ v definiční podmínce platí vždy, tedy ukážeme, že

$$(\forall A, B, C \lhd G, A^\bullet \subseteq C^\bullet)(AB \cap C \subseteq A(B \cap C)).$$

Mějme libovolné $x \in (AB \cap C)^\bullet$, tedy $x \in (AB)^\bullet = A^\bullet B^\bullet$ a existují $x = ab$, kde $a \in A^\bullet \subseteq C^\bullet$ a $b \in B^\bullet$, tedy $b = a^{-1}x$, ale a^{-1} i x leží v $C^\bullet$, tedy $b \in C^\bullet$. Tedy $x = ab$, kde $a \in A^\bullet$ a $b \in B^\bullet \cap C^\bullet = (B \cap C)^\bullet$. □

▶ 8.7.5. Věta. Svaz všech ideálů libovolného okruhu je modulární. Svaz všech podprostorů libovolného vektorového prostoru je modulární.

▶ 8.7.6. Definice. Buď $S = (M, \wedge, \vee)$ svaz s nulou a jednotkou. Normální řada ve svazu S je libovolná posloupnost $(a_i)_{i=0}^m$ prvků z M taková, že $1 = a_0 > a_1 > \cdots > a_m = 0$.

▶ 8.7.7. Definice. Řekneme, že normální řada $(b_j)_{i=0}^n$ je zjemněním normální řady $(a_i)_{i=0}^m$, pokud $\{a_i\}_{i=0}^m \subseteq \{b_j\}_{i=0}^n$. Zjemnění nazveme vlastní, pokud $n > m$.

▶ 8.7.8. Definice. Normální řada, která nemá žádné vlastní zjemnění, se nazývá hlavní řada.

▶ 8.7.9. Věta (Schreier). Libovolné 2 normální řady v modulárním svazu mají zjemnění stených délek.

▶ 8.7.10. Věta (Jordan, Hőlder).

(1) Libovolné 2 hlavní řady v modulárním svazu mají stejnou délku.

(2) Existuje-li v modulárním svazu hlavní řada, pak libovolnou normální řadu lze zjemnit na hlavní řadu.

◦ *Důkaz.*

(1) Nechť je (a_i) kratší hlavní řada. Pak ji podle Shreierovy věty lze zjemnit (vlastním zjemněním), což je spor s tím, že je hlavní.

(2) Buď (a_i) hlavní řada a (b_j) libovolná řada. Nechť (b_j) nelze zjemnit na hlavní řadu. Pak existuje zjemnění (c_k) delší, než (a_i) a podle Schreierovy věty lze najít jejich zjemnění stejných délek. Protože (c_k) je delší než (a_i), museli bychom (a_i) zjemnit, což je spor s tím, že je hlavní.

□

▶ 8.7.11. Definice. Buďte $S = (M, \wedge, \vee)$ svaz a $a, b \in M$. Pro interval $\langle a, b\rangle$ použijeme označení b/a, tedy $b/a := \langle a, b\rangle = \{x \in M \mid x \geq a \text{ et } x \leq b\}$.

▶ 8.7.12. Věta. Buďte $S = (M, \wedge, \vee)$ modulární svaz s nulou a jednotkou a $a, b \in M$, $a < b$. Pak $(a \vee b)/a \cong b/(a \wedge b)$.

◦ *Důkaz.* Definujme 2 zobrazení, $f : \langle a, a \vee b\rangle \to \langle a \wedge b, b\rangle$ jako $f(x) = x \wedge b$ a $g : \langle a \wedge b, b\rangle \to \langle a, a \vee b\rangle$ jako $g(y) = y \vee a$. Ukážeme korektnost definice, tedy mějme $a \leq x \leq a \vee b$, pak $x \wedge b \geq a \wedge b$ a $x \wedge b \leq (a \vee b) \wedge b = b$; korektnost druhé definice ukážeme obdobně.

Zkoumejme zobrazení $g \circ f$, tedy mějme $x \in \langle a, a \vee b\rangle$, pak $g(f(x)) = g(x \wedge b) = (x \wedge b) \vee a$, a neboť $x \geq a$, je $g(f(x)) = x \wedge (b \vee a)$, a neboť $x \leq a \vee b$, je $g(f(x)) = x$. Podobně ukážeme, že $f \circ g = \mathrm{id}$ a tedy f i g jsou bijekce. Ukážeme, že f a g jsou izomorfismy uspořádaných množin, tedy $x \leq y \Leftrightarrow f(x) \leq f(y) \Leftrightarrow g(x) \leq g(y)$. Směr vpravo je snadný, pokud $x \leq y$, je $f(x) = x \wedge b \leq y \wedge b = f(y)$, a podobně pro g. Pro směr vlevo předpokládejme, že $f(x) \leq f(y)$, pak dostáváme $x = g(f(x)) \leq g(f(y)) = y$, a podobně pro g. Tedy jsme našli množinový, a tím i svazový izomorfismus obou intervalů. □

▶ 8.7.13. Věta. Mějme modulární svaz, ve kterém existují hlavní řady (tedy svaz musí mít nulu a jednotku). Definujeme-li $|a|$ jako délku libovolné hlavní řady hlavního ideálu prvku a, pak platí $|a \vee b| + |a \wedge b| = |a| + |b|$.

◦ *Důkaz.* Dle předchozí věty je $|a \vee b| - |a| = |b| - |a \wedge b|$. □

▶ 8.7.14. Důsledek. 1. věta o dimenzi.

▶ 8.7.15. Poznámka. Pokud ve svazu najdeme 2 hlavní řady různé délky, tak víme, že svaz není modulární.

• 8.8. Komplement

▶ 8.8.1. Definice. Buď $S = (M, \wedge, \vee)$ svaz s nulou a jednotkou. Řekneme, že prvek $a' \in M$ je komplementem prvku $a \in M$, platí-li:

(1) $a \wedge a' = 0$;

(2) $a \vee a' = 1$.

▶ 8.8.2. Poznámka. Zvláště v množinových svazech používáme často pro komplement prvku A značku $\complement A$.

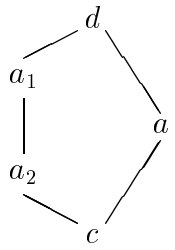
▶ 8.8.3. Příklad. Ve svazu $S = (\mathcal{P}(A), \cap, \cup)$ platí pro $B \subseteq A$, že $B' = A \setminus B$ a komplement existuje právě jeden.

▶ 8.8.4. Příklad. $0' = 1$; $1' = 0$.

▶ 8.8.5. Příklad. Komplement nemusí existovat, ale může jich i existovat více.

(1) Mějme svaz s prvky $\{0, a, 1\}$, pak prvek a nemá komplement.

(2) Mějme svaz $\mathcal{N}_5$ nazývaný pentagon:



K prvku a existují 2 různé srovnatelné komplementy a_1 a a_2. Dále svaz $\mathcal{N}_5$ má 2 hlavní řady různé délky, tedy není modulární, a není ani distributivní.

▶ 8.8.6. Věta. V modulárním svazu nemá žádný prvek 2 různé srovnatelné komplementy.

◦ *Důkaz.* Nechť a_1 a a_2 jsou komplementy a a nechť $a_1 \leq a_2$. Pak platí $a_1 = a_1 \wedge 1 = a_1 \wedge (a \vee a_2) = (a_1 \wedge a) \vee a_2 = 0 \vee a_2 = a_2$. □

▶ 8.8.7. Věta. Svaz je modulární právě tehdy, když neobsahuje jako podsvaz $\mathcal{N}_5$.

◦ *Důkaz.*

(⇒) Sporem, tedy nechť obsahuje pentagon. Pak platí $(a_2 \vee a) \wedge a_1 = d \wedge a_1 = a_1 \neq a_2 = a_2 \vee c = a_2 \vee (a \wedge a_1)$, což je protipříklad proti podmínce modularity.

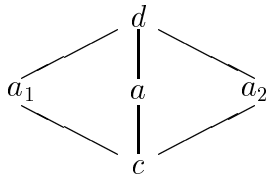
(⇐) Sporem, tedy nechť není modulární. Tedy existují a, b, c takové, že $a \leq c$ ale $a \wedge (b \vee c) < (a \wedge b) \vee c$. Ukážeme, že $a \neq c$ a b je s nimi nesrovnatelný.

Nechť $a = c$, pak $a \wedge (b \vee a) = a = (a \wedge b) \vee a$, což je spor, tedy $a < c$.

Nechť $b < a$ vel $b < c$, pak jistě $b < c$ a $a \wedge (b \vee c) \leq a < c \leq (a \wedge b) \vee c$.

□

► 8.8.8. Příklad. Definujeme svaz $\mathcal{M}_5$ nazývaný Diamant:



Pak $\mathcal{M}_5$ je modulární, ale není distributivní, prvek a má 2 komplementy, které nejsou srovnatelné.

► 8.8.9. Věta. V libovolném distributivním svazu s nulou a jednotkou má každý prvek nejvýše jeden komplement.

◦ *Důkaz.* Mějme a a a_1, a_2 jeho komplementy. Pak $a_1 = a_1 \wedge 1 = a_1 \wedge (a \vee a_2) = (a_1 \wedge a) \vee (a_2 \wedge a_1) = 0 \vee (a_2 \wedge a_1) = a_1 \wedge a_2$, tedy $a_1 \leq a_2$. Ale distributivní svaz je modulární a a_1, a_2 jsou komplementy stejného prvku, tedy $a_1 = a_2$. □

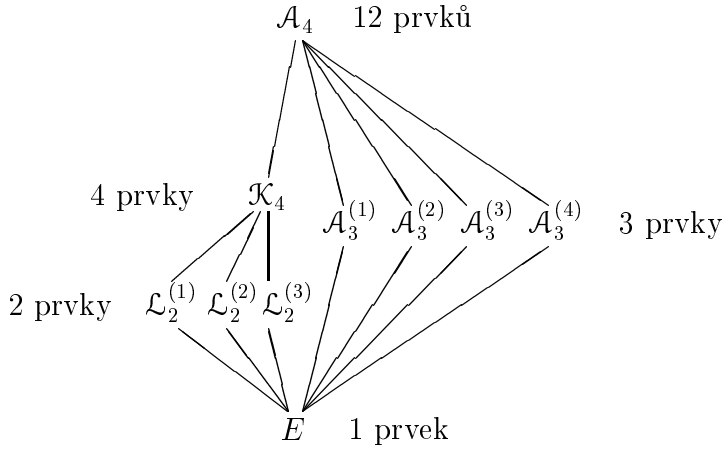
► 8.8.10. Věta. Svaz je distributivní právě tehdy, když neobsahuje jako podsvaz ani $\mathcal{N}_5$, ani $\mathcal{M}_5$.

► 8.8.11. Definice. Řekneme, že svaz s nulou a jednotkou je komplementární, má-li v něm libovolný prvek alespoň jeden komplement.

► 8.8.12. Definice. Řekneme, že svaz s nulou a jednotkou je Booleův, je-li distibutivní a komplementární.

► 8.8.13. Příklad. Příkladem Booleových svazů jsou svazy množinové.

► 8.8.14. Příklad. Vraťme se k 12prvkové alternující grupě $\mathcal{A}_4$, která není jednoduchá a nemá žádnou 6prvkovou podgrupu (přestože $6 \mid 12$), a nakresleme schema svazu jejích podgrup.



Vidíme, že svaz všech podgrup $\mathcal{A}_4$ není modulární, neboť má hlavní řady různé délky. Je to protipříklad, kdyby si někdo myslel, že svaz všech (nejen normálních) podgrup je modulární. Dále svaz podgrup $\mathcal{A}_4$ ani svaz podgrup $\mathcal{K}_4$ není distibutivní. Navíc všechny podgrupy $\mathcal{K}_4$ jsou normální, tedy neplatí, že by libovolný svaz normálních podgrup byl distributivní.

• 8.9. Booleova algebra

► 8.9.1. Definice. Mějme Booleův svaz $S = (M, \wedge, \vee)$. Pak algebru $Q = (M, \wedge, \vee, ', 0, 1)$, kde operace $(')$ je komplement a je unární, a operace 0 a 1 jsou nulární, tedy konstanty, nazveme Booleova algebra.

► 8.9.2. Věta. Buď A Booleova algebra a nechť $a, b \in A^\bullet$. Pak:

(1) $0' = 1, \quad 1' = 0;$

(2) $(a')' = a;$

(3) $a \wedge b = 0 \Leftrightarrow b \leq a', \quad a \vee b = 1 \Leftrightarrow b \geq a';$

(4) $(a \wedge b)' = a' \vee b', \quad (a \vee b)' = a' \wedge b'$ (De Morganovy zákony).

◦ *Důkaz.* Ukážeme pouze tvrzení 3 a 4.

(3) $b = b \wedge 1 = b \wedge (a \vee a') = (b \wedge a) \vee (b \wedge a') = 0 \vee (b \wedge a') = b \wedge a' \Leftrightarrow b \leq a'$

(4) $(a \wedge b)' \wedge (a' \vee b') = (a \wedge b \wedge a') \vee (a \wedge b \wedge b') = 0 \vee 0 = 0,$
$(a \wedge b)' \vee (a' \vee b') = (a \vee a \vee b') \wedge (b \vee a' \vee a') = 1 \wedge 1 = 1;$

□

► 8.9.3. Lemma. Filtr F ve Booleově svazu je ultrafiltr právě tehdy, platí-li

$$(\forall x \in S^\bullet)(x \in F \Leftrightarrow x' \notin F).$$

◦ *Důkaz.*

(⇒) Mějme libovolné x. Pak $x \vee x' = 1 \in F$, tedy $x \in F$ vel $x' \in F$. Kdyby $x, x' \in F$, pak $0 = x \wedge x' \in F$, což je spor s tím, že $F \neq S^\bullet$.

(⇐) Mějme libovolné prvky a, b. Nechť $a \vee b \in F$, ale $a, b \notin F$. Pak $a', b' \in F$, tedy $a' \wedge b' = (a \vee b)' \in F$, což je spor.

□

► 8.9.4. Věta. Libovolná Booleova algebra je izomorfní s nějakou množinovou Booleovou algebrou.

◦ *Důkaz.* Definujeme zobrazení $f(x) = \{F \in \mathcal{U}_S \mid x \in F\}$. Víme, že f zachovává průsek a spojení.

(′) $f(x') = \{F \in \mathcal{U}_S \mid x \in F\} = \{F \in \mathcal{U}_S \mid x \notin F\} = \complement f(x)$

(0) $f(0) = \{F \in \mathcal{U}_S \mid 0 \in F\}$, ale $0 \in F \Rightarrow F = S^\bullet$, což není filtr. Tedy $f(0) = \emptyset$.

(1) $f(1) = \{F \in \mathcal{U}_S \mid 1 \in F\} = \mathcal{U}_S$.

□

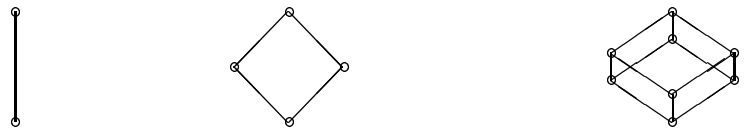
► 8.9.5. Věta. Libovolná konečná Booleova algebra je izomorfní množinové Booleově algebře tvořené všemi podmnožinami vhodné množiny.

► 8.9.6. Věta.

(1) Libovolná konečná Booleova algebra má počet prvků roven číslu 2^n, $n \in \mathbb{N}$.

(2) K libovolnému $n \in \mathbb{N}$ existuje až na izometrii právě jedna Booleova algebra s 2^n prvky.

► 8.9.7. Příklad. 2-, 4- a 8prvková Booleova algebra.



---

9. Polynomy nad komutativními tělesy

• 9.1. Polynomy

► 9.1.1. Poznámka. Budeme značit T komutativní těleso a budeme vyšetřovat okruh polynomů nad tělesem T, který značíme $T[x]$. Víme, že $T[x]$ je asociativní, komutativní, bez dělitelů nuly, tedy je oborem integrity s jednotkou $1 \cdot x^0$.

► 9.1.2. Věta (o dělení se zbytkem, algoritmus dělení). Buďte $P_1, P_2 \in T[x]$ polynomy, přičemž $P_2 \neq \theta$. Pak existují polynomy $Q, R \in T[x]$ takové, že $P_1 = P_2 Q + R$, přičemž $R = \theta$ nebo $\operatorname{st} R < \operatorname{st} P_2$.

◦ *Důkaz.* Pro $P_1 = \theta$ platí $P_1 = P_2 \cdot \theta + \theta$. Pro $\operatorname{st} P_1 < \operatorname{st} P_2$ je $P_1 = P_2 \cdot \theta + P_1$. Tedy nechť $P_1 \neq \theta$ a $\operatorname{st} P_1 \geq \operatorname{st} P_2$. Nechť $P_1 = \sum_{i=0}^{m} a_i x^i$ a $P_2 = \sum_{i=0}^{n} b_i x^i$, kde $a_m \neq 0$, $b_n \neq 0$ a $m \geq n$.
Důkaz provedeme matematickou indukcí podle m.

(1) $m = 0$, tedy i $n = 0$, tedy $P_1 = a_0 x^0$ a $P_2 = b_0 x^0$. Pak $P_1 = a_0 x^0 = (b_0 x^0)(a_0 b_0^{-1} x^0) + \theta$.

(2) Nechť $m > 0$ a nechť tvrzení platí polynomy P_1 stupně menšího než m. Definujme $\tilde{P}_1 := P_1 - (a_m b_n^{-1} x^{m-n})\, P_2$. Stupeň $(a_m b_n^{-1} x^{m-n})\, P_2$ je m a jeho člen s nejvyšší mocninu je $a_m x^m$. Tedy člen $\tilde{P}_1$ s mocninou x^m je $a_m - a_m = 0$. Pokud je $\tilde{P}_1 = \theta$, je $P_1 = P_2(a_m b_n^{-1} x^{m-n}) + \theta$. Pokud $\tilde{P}_1 \neq \theta$, je $\operatorname{st} \tilde{P}_1 < \operatorname{st} P_1$ a podle indukčního předpokaldu existují $\tilde{Q}, \tilde{R}$ takové, že $\tilde{P}_1 = P_2 \tilde{Q} + \tilde{R}$ a $\tilde{R} = \theta$ nebo $\operatorname{st} \tilde{R} < \operatorname{st} P_2$. A konečně $P_1 = \tilde{P}_1 + (a_m b_n^{-1} x^{m-n})\, P_2 = P_2 \left(\tilde{Q} + (a_m b_n^{-1} x^{m-n}) \right) + \tilde{R}$.

□

► 9.1.3. Poznámka. $T[x]$ je Eukleidův okruh, tj. každé 2 polynomy mají největšího společného dělitele a ten se dá najít Eukleidovým algoritmem.

► 9.1.4. Věta. Okruh $T[x]$ je okruhem hlavních ideálů.

◦ *Důkaz.* Mějme libovolný ideál $I \lhd T[x]$. Pokud $I = E = \{\theta\}$ je $I = I_\theta$. Tedy nechť $I \neq E$. Mějme polynom $P \in I$, $P \neq \theta$ takový, že má nejmenší stupeň ze všech nenulových polynomů v I. Ukážeme, že $I = I_P$.

($I \subseteq I_P$) Zvolme libovolný $P_1 \in I$, pak víme, že existují Q, R takové, že $P_1 = PQ + R$, kde $R = \theta$ nebo $\operatorname{st} R < \operatorname{st} P$. Dále $R = P_1 - QP \in I$, tedy pokud by $R \neq \theta$, nutně $\operatorname{st} R < \operatorname{st} P$, což je spor s minimalitou $\operatorname{st} P$. Tedy $R = \theta$ a $P_1 = PQ \in I_P$.

($I_P \subseteq I$) Pokud $P \in I$, pak také $I_P \subseteq I$.

□

► 9.1.5. Definice. Buďte $P, Q \in T[x]$. Řekneme, že Q dělí P, existuje-li $S \in T[x]$ takový, že $P = QS$. Značíme $Q \mid P$.

► 9.1.6. Definice. Buďte T, U komutativní tělesa, $T \Subset U$ a buďte $P = \sum_{i=0}^{n} a_i x^i \in T[x]$ a $\alpha \in U$. Pak položíme hodnotu polynomu P na prvku α jako $P(\alpha) := \sum_{i=0}^{n} a_i \alpha^i \in U$.

► 9.1.7. Definice. Buď $P \in T[x]$. Kořenem polynomu P (řešení algebraické rovnice $P(x) = 0$) rozumíme libovolný prvek α z nějakého nadtělesa $U \Supset T$ takový, že $P(\alpha) = 0$.

► 9.1.8. Věta. Buďte $T \Subset U$, $P \in T[x]$, $\alpha \in U^\bullet$. Potom

$$P(\alpha) = 0 \iff (x - \alpha) \mid P.$$

◦ *Důkaz.*

(⇒) Nechť $P(\alpha) = 0$ a $P = (x-\alpha)Q + R$. Platí $R = \theta$ nebo $\operatorname{st} R < 1$, tedy $R = r_0 x^0$ pro $r_0 \in T$. Pak $0 = P(\alpha) = 0 + r_0$, tedy $r_0 = 0$ a $P = (x-\alpha)Q$.

(⇐) Platí $P = (x-\alpha)S$ tedy $P(\alpha) = 0 \cdot S(\alpha) = 0$.

□

▶ 9.1.9. Důsledek. Má-li P po dvou různé kořeny $\alpha_1, \ldots, \alpha_k$, pak $(x-\alpha_1)\cdots(x-\alpha_k) \mid P$.

◦ *Důkaz.* $P(\alpha_1) = 0 \Rightarrow (x-\alpha_1) \mid P \Rightarrow P = (x-\alpha_1)P_1$.
$P(\alpha_2) = 0 \Rightarrow (\alpha_2-\alpha_1)P_1(\alpha_2) = 0 \Rightarrow P_1 = (x-\alpha_2)P_2 \Rightarrow P = (x-\alpha_1)(x-\alpha_2)P_2$.
Po k krocích dostaneme $P = (x-\alpha_1)\cdots(x-\alpha_k)P_k$. □

▶ 9.1.10. Důsledek. Polynom stupně n má nejvýše n různých kořenů.

▶ 9.1.11. Poznámka. Není-li T komutativní těleso, nemusí poslední důsledek platit.
Vezměme např. okruh Z_{16}, který není tělesem, a $x^2 \in Z_{16}[x]$. Jeho kořeny jsou 0, 4, 8 a 12, tedy jsou čtyři pro polynom stupně 2.
Mějme K těleso kvaternionů, které je nekomutativní, a polynom stupně dva, $P := x^2 + 1 \in K[x]$. Pak pro $\alpha = \pm i, \pm j, \pm k$ platí $\alpha^2 = -1$, tedy má 6 kořenů.

▶ 9.1.12. Definice. Derivací polynomu $P = \sum_{i=0}^{n} a_i x^i \in T[x]$ rozumíme polynom $P' \in T[x]$ daný vztahem

$$P' := \sum_{i=1}^{n} i a_i x^{i-1}.$$

▶ 9.1.13. Poznámka. Ve vztahu $\sum_{i=1}^{m} i a_i x^{i-1}$ není součin $i a_i$ součinem v tělese, ale $i \times a_i$. Pro jednoduchost zápis zkracujeme.

▶ 9.1.14. Poznámka. Derivace polynomu je formálně stejná jako v analýze, nebudeme tedy znovu dokazovat známá tvrzení, jako $(PQ)' = P'Q + PQ'$ apod.

▶ 9.1.15. Definice. Buďte $T \Subset U$, $P \in T[x]$, $\alpha \in U^\bullet$, $m \in \mathbb{N}_0$. Řekneme, že α je m-násobný kořen polynomu P, platí-li $(x-\alpha)^m \mid P$, ale $(x-\alpha)^{m+1} \nmid P$.

▶ 9.1.16. Věta. Buď α m-násobný kořen polynomu P. Potom α je alespoň $(m-1)$-násobným kořenem polynomu P'.

◦ *Důkaz.* Máme $P = (x-\alpha)^m Q$, tedy $P' = m(x-\alpha)^{m-1}Q + (x-\alpha)^m Q' = (x-\alpha)^{m-1}(mQ + (x-\alpha)Q')$. □

▶ 9.1.17. Poznámka. Pokud by T mělo nenulovou charakteristiku p a m bylo násobkem p, pak $mQ(\alpha) = 0$ a platí $P' = (x-\alpha)^m Q'$.

▶ 9.1.18. DEFINICE. Řekneme, že $P \in T[x]$ stupně alespoň 1 je reducibilní nad T, existují-li $P_1, P_2 \in T[x]$ takové, že $1 \leq \operatorname{st} P_i < \operatorname{st} P$ a $P = P_1 P_2$.

V opačném případě řekneme, že P je ireducibilní nad T.

▶ 9.1.19. POZNÁMKA. Reducibilita závisí na tělese.

(1) Polynom $x^2 - 2 \in Q[x]$ je ireducibilní nad Q, ale reducibilní nad R, neboť $x^2 - 2 = \left(x + \sqrt{2}\right)\left(x - \sqrt{2}\right)$.

(2) Polynom $x^2 + 1 \in Q[x]$ je ireducibilní nad R, ale reducibilní nad C, neboť $x^2 + 1 = (x + i)(x - i)$.

▶ 9.1.20. LEMMA. Libovolný polynom stupně 1 je ireducibilní nad libovolným tělesem.

▶ 9.1.21. VĚTA.

(1) Nad C jsou ireducibilní právě jen polynomy 1. stupně.

(2) Nad R jsou ireducibilní právě jen polynomy 1. stupně a polynomy 2. stupně se záporným diskriminantem příslušné kvadratické rovnice.

▶ 9.1.22. LEMMA. Má-li polynom $P \in T[x]$ v tělese T kořen, je nad tělesem T reducibilní.

◦ *Důkaz.* Pokud $P(\alpha) = 0$, platí $P = (x - \alpha)Q$, kde $Q \in T[x]$ □

▶ 9.1.23. POZNÁMKA. Opačná implikace neplatí. Například $P = P_1 P_2$ nad T, kde $\operatorname{st} P_i \geq 2$ a nemají kořen v T.

▶ 9.1.24. LEMMA. Je-li $\operatorname{st} P \leq 3$ a P je reducibilní nad T, pak má P v tělese T kořen.

◦ *Důkaz.* Alespoň jeden z polynomů v rozkladu má stupeň 1. □

▶ 9.1.25. POZNÁMKA. Každý ideál v okruhu polynomů je hlavní, tj. $(\forall I \lhd T[x])(\exists P \in T[x])(I = I_P)$. Dále $I_P = T[x] \cdot P$.

Mějme třídy ekvivalence $T[x] \,/\, I_P$ pro $P \neq \theta$. Pak do jedné zbytkové třídy patří 2 polynomy právě tehdy, dávají-li stejný zbytek po dělení polynomem P

Pro $P = \theta$ jsou polynomy ekvivalentní pouze, když jsou stejné.

Je-li $\operatorname{st} P = n$, pak zbytkové polynomy jsou všechny polynomy stupně nejvýše $n - 1$.

Zbytkovou třídu obsahující polynom R označujeme $\overline{R}$.

▶ 9.1.26. LEMMA. Je-li T konečné těleso řádu q, pak počet zbytkových tříd podle polynomu P stupně n je q^n.

▶ 9.1.27. LEMMA. $T[x] \,/\, I_P$ je asociativní a komutativní okruh s jednotkou. Jednotkou je $\overline{1 \cdot x^0}$.

▶ 9.1.28. VĚTA. Je-li $P \in T[x]$ reducibilní nad T, potom faktorokruh $T[x] \,/\, I_P$ obsahuje dělitele nuly.

◦ *Důkaz.* Existuje netriviální rozklad $P = P_1P_2$. Dále $\overline{\theta} \neq \overline{P_i}$ a $\overline{\theta} = \overline{P} = \overline{P_1P_2}$. □

► 9.1.29. Věta. Je-li $P \in T[x]$ ireducibilní nad T, potom je faktorkokruh $T[x] \,/\, I_P$ komutativní těleso.

◦ *Důkaz.* Víme, že je komutativní s jednotkou, zbývá ukázat, že každá nenulová třída $\overline{A}$ má třídu inverzní. Důkaz provedeme neúplnou matematickou indukcí podle $m = \operatorname{st} A$, přičemž $0 \leq m < \operatorname{st} P$.

(*m* = 0) Platí $A = ax^0$ a $a \neq 0$. Potom $ax^0 \cdot a^{-1}x^0 = 1x^0$, a tedy $\overline{A}\,\overline{a^{-1}x^0} = \overline{1x^0}$.

($m \geq 1$) Nechť každý polynom stupně menšího než m má inverzní. $P = AQ + R$. Pak $R = \theta$ nebo $\operatorname{st} R < \operatorname{st} A = m$. Neboť P je ireducibilní, je $R \neq \theta$, jinak by bylo $P = AQ$, kde $\operatorname{st} A < \operatorname{st} P$.

Tedy podle indukčního předpokladu existuje $\overline{R}^{-1}$ a dále platí: $\overline{\theta} = \overline{P} = \overline{A}\,\overline{Q} + \overline{R}$ a po vynásobení $(\overline{R})^{-1}$ dostáváme $\overline{\theta} = \overline{A}\,\overline{Q}\left(\overline{R}\right)^{-1} + \overline{1x^0}$ a konečně $\left(\overline{A}\right)^{-1} = -\overline{Q}\left(\overline{R}\right)^{-1}$.

□

► 9.1.30. Příklad. Mějme reálný polynom $P := x^2+1 \in R[x]$. Pak $R[x] \,/\, I_P = \left\{\overline{a+bx} \;\middle|\; a, b \in \mathbb{R}\right\}$. Platí

$$\overline{a_1 + b_1x} + \overline{a_2 + b_2x} = \overline{(a_1 + a_2) + (b_1 + b_2)x}$$

a

$$\overline{a_1 + b_1x} \cdot \overline{a_2 + b_2x} = \overline{(a_1a_2) + (a_1b_2 + a_2b_1)x + (b_1b_2)x^2}.$$

A neboť $x^2 \equiv_{I_P} -1$, je $\overline{x^2} = \overline{-1}$, a tedy

$$\overline{a_1 + b_1x} \cdot \overline{a_2 + b_2x} = \overline{(a_1a_2 - b_1b_2) + (a_1b_2 + a_2b_1)x}.$$

Víme $R[x] \,/\, I_P$ je komutativní těleso a operace jsou stejné, jako v C. To nám umožňuje pomocí R definovat komplexní čísla, stačí místo x psát všude i.

• 9.2. Adjunkce

► 9.2.1. Definice. Mějme dvojici těles $T \Subset U$ a $A \subseteq U^\bullet$. Pak definujeme těleso $T(A) := \bigcap\{V \Subset U \mid T^\bullet \cup A^\bullet \subseteq V\}$ a říkame, že vzniká tělesovou adjunkcí A k T.

Je-li A jednoprvková, $A = \{\alpha\}$, pak používáme označení jednoduchá adjunkce, a značíme $T(\alpha) := T(\{\alpha\})$.

► 9.2.2. Příklad.

(1) Je-li $A \subseteq T$, je $T(A) = T$.

(2) $Q\left(\left\{\sqrt{2}\right\}\right) = \left\{a + b\sqrt{2} \;\middle|\; a, b \in \mathbb{Q}\right\}$.

(3) $R(i) = C$.

► 9.2.3. Definice. Pro $T \Subset U$ a $\alpha \in U$ definujeme $T[\alpha] := \{P(\alpha) \mid P \in T[x]\}$.

► 9.2.4. Lemma. $T[\alpha]$ je podokruh $T(\alpha)$.

◦ *Důkaz.* Pro libovolný polynom $P \in T[x]$ je $P(\alpha)$ kombinací α a prvků z T, tedy $T[\alpha] \subseteq T(\alpha)$. Snadno se ukáže, že je okruhem. □

► 9.2.5. Lemma. $T[\alpha]$ je obor integrity.

◦ *Důkaz.* $T[\alpha]$ je podokruhem komutativního tělesa $T(\alpha)$, tedy je oborem integrity. □

► 9.2.6. Lemma. Těleso $T(\alpha)$ je izomorfní s podílovým tělesem oboru integrity $T[\alpha]$.

◦ *Důkaz.* Označme $H = T[\alpha]$. Pak těleso zlomků U_H je izomorfní s podílovým tělesem T_H.

Definujeme $h : U_H \to T(\alpha)$ jako $h\left(\frac{a}{b}\right) = ab^{-1}$ pro $a, b \in H$ a $b \neq 0$. Tedy existují $P, Q \in T[x]$ takové, že $a = P(\alpha)$ a $b = Q(\alpha)$. Korektnost definice a fakt, že h je monomorfismus jsme ukázali dříve pro obdobný případ, tedy $U_H \cong h(U_H) \overset{\text{těl.}}{\Subset} T(\alpha)$.

Ukážeme, že $T \cup \{\alpha\} \subseteq h(U_H)$, což už stačí pro to, aby $T(\alpha) \Subset h(U_H)$. Zvolíme $Q = 1x^0$, tedy $b = Q(\alpha) = 1$. Volbou $P = x$ dostaneme $a = P(\alpha) = \alpha$ a tedy $h\left(\frac{a}{b}\right) = \alpha$. Volbou $P = tx^0$ pro libovolné $t \in T$ dostaneme $a = P(\alpha) = t$ a tedy $h\left(\frac{a}{b}\right) = t$. □

► 9.2.7. Lemma. Buďte $T \Subset U$ tělesa, $\alpha \in U^\bullet$, a nechť $h : T[x] \to T[\alpha]$ je definované jako $h(P) = P(\alpha)$. Potom $T[\alpha] \overset{\text{okr.}}{\cong} T[x] \,/\, \ker h$, přičemž $\ker h = \{P \in T[x] \mid P(\alpha) = 0\}$.

◦ *Důkaz.* Je $h(P + Q) = (P + Q)(\alpha) = P(\alpha) + Q(\alpha) = h(P) + h(Q)$ a podobně pro $h(PQ)$, tedy h je homomorfismus. Současně h je z definice $T[\alpha]$ na, tedy h je epimorfismus. Tvrzení lemmatu již plyne z věty o homomorfismu. □

► 9.2.8. Definice. Buďte $T \Subset U$ tělesa, $\alpha \in U^\bullet$. Pomocí zobrazení h z předchozího lemmatu dělíme prvky U do 2 skupin.

($\ker h = E = \{\theta\}$) Pak α nazýváme <u>transcendentní prvek</u> nad tělesem T.

Dále podle lemmatu je $T[\alpha] \cong T[x] \,/\, E \cong T[x]$ a izomorfní obory integrity mají izomofní podílová tělesa, tedy $T(\alpha) \cong T(x)$, kde symbolem $T(x)$ značíme podílové těleso k $T[x]$, tj. těleso racionálních funkcí.

($\ker h \neq E$) Pak α nazýváme <u>algebraický prvek</u>.

Dále $\ker h$ je ideálem a my jsme v okruhu hlavních ideálů, tedy $\ker h = I_Q$ pro nějaké $Q \in T[x]$, $Q \neq \theta$. Ze všech takových Q vybereme polynom s nejmenším stupněm n, který je normovaný (koeficient u x^n je 1) a nazveme jej <u>minimální polynom</u> prvku α nad T a budeme jej značit M_α^T. Číslo n nazveme <u>stupněm</u> prvku α a budeme jej značnit $\operatorname{st}\alpha$.

Navíc $T[\alpha] \cong T[x] \,/\, I_{M_\alpha}$, kde pravá strana je těleso, a tedy z izomorfie i $T[\alpha]$ je těleso (pro algebraické α). A dále $T(\alpha) \cong T_{T[\alpha]} = T[\alpha] = T[x] \,/\, I_{M_\alpha^T}$.

► 9.2.9. Lemma. Minimální polynom je ireducibilní nad T.

► 9.2.10. Věta. Buď α algebraický prvek nad tělesem T. Potom $T(\alpha) \cong T[x] \,/\, I_{M_\alpha^T}$.

▶ 9.2.11. Příklad.

(1) Všechny prvky $\alpha \in \mathbb{C}$ jsou algebraické nad C a platí $M_\alpha^C = x - \alpha$.

(2) Všechny prvky $\alpha \in \mathbb{C}$ jsou algebraické nad R. Pro $\alpha \in \mathbb{R}$ platí $M_\alpha^R = x - \alpha$ a pro $\alpha \notin R$ platí $M_\alpha^{\mathbb{R}} = (x-\alpha)(x-\bar{\alpha}) = x^2 - 2\operatorname{Re}\alpha x + |\alpha|^2$.

(3) Algebraické číslo (bez udání tělesa) znamená algebraické nad $\mathbb{Q}$. Totéž pro transcendentní. Příklady transcendentních jsou π a e.

▶ 9.2.12. Lemma. Buď α algebraický prvek nad T. Potom $T[\alpha] = T(\alpha)$.

◦ *Důkaz.* Pro $\beta \in T$ definujeme $P = \alpha^{-1}\beta x^1$, pak $P(\alpha) = \beta$; položme $P = 1x^1$, pak $P(\alpha) = \alpha$. Tedy $T(\alpha) \subseteq T[\alpha]$. Opačnou inkluzi jsme ukázali dříve. □

▶ 9.2.13. Věta. Buď α algebraický prvek nad tělesem T a nechť $\operatorname{st}\alpha = n$. Potom $\dim_T T(\alpha) = n$ a jednou z bází $T(\alpha)$ je soubor $(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ a tedy libovolný prvek $\beta \in T(\alpha)$ lze psát ve tvaru $\beta = \sum_{i=0}^{n-1} b_i\alpha^i$, kde $b_i \in T^\bullet$.

◦ *Důkaz.* Mějme libovolné $\beta \in T(\alpha) = T[\alpha]$. Tedy $(\exists P \in T[x])(\beta = P(\alpha))$. Pak podle věty o dělení se zbytkem je $P = M_\alpha Q + R$, kde $R = \theta$ nebo $\operatorname{st} R < \operatorname{st} M_\alpha = n$, a platí $R(\alpha) = P(\alpha) = \beta$. Je-li $R = \sum_{i=0}^{n-1} b_i x^i$, pak $\beta = \sum_{i=0}^{n-1} b_i\alpha^i$ a tedy definovaný soubor generuje.

Ukážeme, že je nezávislý. Nechť existuje nenulová lineární kombinace souboru, pak je tato kombinace polynomem s nižším stupněm než n, který má v bodě α hodnotu 0, což je spor s minimalitou stupně M_α. Tedy daný soubor je bází a dimenze je n. □

▶ 9.2.14. Věta. Libovolný ireducibilní polynom má kořen (obecně v nadtělese).

◦ *Důkaz.* Máme ireducibilní $P \in T[x]$. Je-li $\operatorname{st} P = 1$, je $P = a_0 + a_1 x$ a má kořen v T. Tedy nechť $\operatorname{st} P \geq 2$.

Označme $U := T[x]\,/\,I_P$ a neboť P je ireducibilní, je U komutativní těleso. Definujeme zobrazení $h : T \to U$ jako $h(a) := \overline{ax^0}$. Snadno se ukáže, že h je okruhový monomorfismus, tedy $T \cong h(T) \Subset U$. Známým postupem najdeme k tělesu T nadtěleso V tak, že z U vyjmeme $h(T)$ a nahradíme jej T, tedy $V = (U \setminus h(T)) \cup T \cong U$. Definujeme izomorfismus $g : V \to U$ jako

$$g(\beta) := \begin{cases} h(\beta) \mid \beta \in T \\ \beta \quad\;\; \mid \beta \in V \setminus T. \end{cases}$$

Ukážeme, že kořenem P je prvek $\alpha \in V$, $\alpha = g^{-1}(\overline{x})$. Platí

$$P(\alpha) = \sum_{i=0}^{n} a_i\alpha^i = g^{-1}\left(\sum_{i=0}^{n} g(a_i)\,g(\alpha^i)\right) = g^{-1}\left(\sum_{i=0}^{n} \overline{a_i x^0}\,\overline{x^i}\right) = g^{-1}\left(\overline{\sum_{i=0}^{n} a_i x^i}\right) = g^{-1}\left(\overline{P}\right) = g^{-1}\left(\overline{\theta}\right) = 0.$$

□

▶ 9.2.15. Důsledek. Libovolný polynom stupně většího než nula má kořen.

▶ 9.2.16. Poznámka. V předchozí větě je α algebraický nad T a navíc P je jeho minimálním polynomem.

◦ *Důkaz.* Máme $P(\alpha) = 0$, tedy $M_\alpha^T \mid P$ (z věty o dělení). Navíc P je ireducibilní, tedy P nemá netriviální dělitele a je tedy minimálnímu polynomu roven až na normování koeficientu u nejvyšší mocniny na 1. □

▶ 9.2.17. Definice. Buďte T těleso a $P \in T[x]$. Rozkladové těleso polynomu P je nejmenší nadtěleso $U \ni T$ takové, že v něm lze P rozložit na součin lineárních polynomů, tj. že v něm leží všechny kořeny P.

▶ 9.2.18. Věta. Libovolný polynom stupně alespoň 1 má rozkladové těleso.

◦ *Důkaz.* Mějme $P \in T[x]$ a nechť $P = P_1 \cdots P_k$ pro $P_i \in T[x]$ je rozklad na ireducibilní polynomy. Jsou-li všechny P_i stupně jedna, je T samo rozkladovým tělesem. Tedy nechť např. P_1 má stupeň alespoň 2. Pak existuje $V \ni T$ takové, že P_1 má ve V kořen α, tedy lze rozložit na polynom a lineární polynom.

Tedy máme $P = Q_1 \cdots Q_\ell$ rozklad v tělese V, kde jistě $\ell > k$, neboť jsme P_1 rozložili. Je možné, že jsme rozložili víc, než jen P_1. Pokud opět zbydou nějaké stupně alespoň 2, proces opakujeme. □

---

10. Konečná tělesa

10.1. Konečná tělesa

▶ 10.1.1. Věta (Wedderburn). Libovolné konečné těleso je komutativní.

▶ 10.1.2. Věta. Libovolné konečné těleso T má řád p^n, kde $p \in \mathbb{P}$ a $n \in \mathbb{N}$, přičemž $p = \operatorname{ch} T$ a $n = \dim_{Z_p} T$.

◦ *Důkaz.* T je vektorový prostor nad tělesem Z_p (až na izomorfie) a $\dim_{Z_p} T = n$, a tedy $T \ni \alpha = \sum_{i=1}^n \alpha_i u_i$, kde $\alpha_i \in Z_p$ a $(u_i)_{i=1}^n$ je báze T. Počet n-tic $(\alpha_1, \ldots, \alpha_n)$ je p^n a z jednoznačnosti vyjádření prvku v bázi dostáváme, že prvků T je také p^n. □

▶ 10.1.3. Lemma (binomická věta). Nechť R je asociativní a komutativní okruh s jednotkou, nechť $a, b \in R^\bullet$ a $n \in \mathbb{N}$. Pak platí:

$$(a+b)^n = a^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i b^{n-i} + b^i.$$

▶ 10.1.4. Lemma. V tělese charakteristiky $p \in \mathbb{P}$ platí:

$$(a \pm b)^{p^m} = a^{p^m} \pm b^{p^m}.$$

◦ *Důkaz.* Nechť nejprve $m = 1$. Důkaz provedeme matematickou indukcí podle m.

($m = 1$, $a + b$) Chceme ukázat, že $\sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} = 0$. Zjevně platí, že $p \mid p! = \binom{p}{i} i!(p-i)!$. Neboť p je prvočíslo, musí dělit alespoň jeden z činitelů. Neboť pro $0 < i < p$ je $i < p$ a $p - i < p$, platí $p \mid \binom{p}{i}$, tedy $\binom{p}{i}$ je násobkem charakteristiky a tedy $\binom{p}{i} a^i b^{p-i} = 0$.

($m=1$, $a-b$) Pro $p=2$ je $(a-b)^2 = a^2 - 2ab + b^2 = a^2 - b^2 = a^2 - b^2 + 2b^2 = a^2 + b^2$ Pro p liché je $(a-b)^p = (a+(-b))^p = a^p + (-b)^p = a^p - b^p$.

($m \to m+1$) $(a \pm b)^{p^{m+1}} = \left((a \pm b)^{p^m}\right)^p = \left(a^{p^m} \pm b^{p^m}\right)^p = \left(a^{p^m}\right)^p \pm \left(b^{p^m}\right)^p = a^{p^{m+1}} \pm b^{p^{m+1}}$.

□

▶ 10.1.5. Lemma. V konečném tělese řádu q platí pro všechny prvky $a^q = a$.

◦ *Důkaz.* Nechť $|U| = q$, lib. $a \in U$, $a \neq 0$. Pak $a \in U_*$, $|U_*| = q-1$ a podle Lagrangeovy věty řád a dělí $q-1$ a tedy $a^{q-1} = 1$. Potom též $a^q = a$, což platí i pro $a = 0$, tedy pro všechny prvky. □

▶ 10.1.6. Věta. K libovolným číslu $p \in \mathbb{P}$ a $n \in \mathbb{N}$ existuje až na izomorfismus právě jedno těleso řádu p^n. Takové těleso značíme $\mathrm{GF}(p^n)$ (Galoisova tělesa).

◦ *Důkaz.* Položme $q := p^n$ a definujme $P := x^q - x \in Z_p[x]$. Nechť U je rozkladové těleso polynomu P a nechť $U_0 = \{\alpha \in U \mid P(\alpha) = 0\} = \{\alpha \in U \mid \alpha^q = \alpha\}$. Dále $P' = qx^{q-1} - 1x^0 = pp^{n-1}x^{q-1} - 1x^0 = -1x^0$, tedy derivace nemá kořen a tedy všechny kořeny P jsou 1násobné.

Ukážeme, že U_0 je těleso, tedy že je uzavřené v tělese U. Mějme $\alpha, \beta \in U_0$. Pak $(\alpha-\beta)^q = (\alpha-\beta)^{p^n} = \alpha^q - \beta^q = \alpha - \beta$, tedy $\alpha - \beta \in U_0$. Nechť navíc $\beta \neq 0$, pak $(\alpha\beta^{-1})^q = \alpha^q (\beta^q)^{-1} = \alpha\beta^{-1}$, tedy $\alpha\beta^{-1} \in U_0$. Tedy jsme nalezli těleso o p^n prvcích.

Jednoznačnost nedokazujeme. □

▶ 10.1.7. Lemma. Buď $G = (M, \cdot)$ grupa a nechť $a, b \in M$ komutují, tj. $ab = ba$, a označme $m = |a|$, $n = |b|$ a $r = |ab|$ řády prvků a, b a ab. Pak $r \mid mn$ a tedy $r \leq mn$. A jsou-li m, n nesoudělná, je $r = mn$.

◦ *Důkaz.* Platí $(ab)^{mn} = (a^m)^n (b^n)^m = 1^n 1^m = 1$, tedy $r \mid mn$.

Pro nesoudělná m, n je $1 = (ab)^{mr} = (a^m)^r b^{mr} = b^{mr} \Rightarrow n \mid mr \Rightarrow n \mid r$. Podobně také $m \mid r$, tedy $mn \mid r$. □

▶ 10.1.8. Věta. Buď $G = (M, \cdot)$ grupa a nechť $a, b \in M$ komutují, tj. $ab = ba$, a označme $m = |a|$, $n = |b|$ řády prvků a a b. Potom $(\exists c \in M)(|c| = \nu(mn))$.

◦ *Důkaz.* Položme $m = p_1^{k_1} \cdots p_r^{k_r} p_{r+1}^{k_{r+1}} \cdots p_{r+s}^{k_{r+s}}$ a $n = p_1^{\ell_1} \cdots p_r^{\ell_r} p_{r+1}^{\ell_r+1} \cdots p_{r+s}^{\ell_r+s}$, přičemž $k_i \geq \ell_i$ pro $i \in \widehat{r}$ a $k_i < \ell_i$ jinak.

Dále označme $\bar{m} = p_1^{k_1} \cdots p_r^{k_r}$ a $\bar{n} = p_{r+1}^{\ell_r+1} \cdots p_{r+s}^{\ell_r+s}$. Zjevně $\delta(\bar{m}, \bar{n}) = 1$. Označme $\bar{a} = a^{\frac{m}{\bar{m}}}$ a $\bar{b} = b^{\frac{n}{\bar{n}}}$. Pak $|\bar{a}| = \bar{m}$ a $|\bar{b}| = \bar{n}$. Dále $\bar{a}$ a $\bar{b}$ komutují a mají nesoudělné řády, označme $c = \bar{a}\bar{b}$, pak $|c| = \bar{m}\bar{n} = \nu(m, n)$. □

▶ 10.1.9. Věta. Multiplikativní grupa libovolného konečného tělesa T je cyklická.

◦ *Důkaz.* Označme $q = p^n = |T|$ počet prvků tělesa T, tedy $T = \mathrm{GF}(q)$ Víme, že $|T_*| = q - 1$. Vezměme libovolné $a \in T_*^\bullet$

Nechť $|a| = q-1$, pak $\langle a\rangle = T_*$ a jsme hotovi. Nechť tedy $m = |a| < q-1$. Mějme libovolné b takové, že pro $n = |b|$ platí $n \,|\, m$. Tedy víme, že $b^m = 1$ a tedy b je kořenem polynomu $x^n - 1 \in Z_p[x]$, který má nejvýše m kořenů. A neboť $m < q-1$, existuje alespoň jeden prvek b takový, že pro $n = |b|$ platí $n \nmid m$. Víme, že T_* je komutativní, tedy $(\exists c)(|c| = \nu(m,n))$ a neboť $n \nmid m$, je $\nu(m,n) > m$.

Po konečně mnoha krocích musíme nezbytně dojít k číslu $q-1$. □

► 10.1.10. Definice. Primitivním prvkem konečného tělesa T je libovolný generátor jeho multiplikativní grupy.

► 10.1.11. Důsledek. Libovolné konečné těleso má primitivní prvek.

► 10.1.12. Poznámka. Mějme $Z_p[x]$ a $P \in Z_p[x]$ ireducibilní stupně n. Pak $Z_p[x] \,/\, I_P$ je těleso o p^n prvcích a v následující větě ukážeme, že takto lze zkonstruovat všechna konečná tělesa.

► 10.1.13. Příklad. Prozkoumejme GF(9).

$9 = 3^2$, tedy $Z_3 = \{0,1,2\}$ a $P = x^2 + x + 2$, P nemá v Z_3 kořen, tedy je ireducibilní.

Platí $x^2 + x + 2 \equiv_P \theta$, tedy $x^2 \equiv_P -x - 2 \equiv_P 2x + 1$ a $2x^2 = x + 2$.

Prvky jsou $\{0, x^0 \equiv 1,\ x^1 \equiv x,\ x^2 \equiv 2x+1,\ x^3 \equiv 2x^2 + x \equiv 2x + 2,\ x^4 \equiv 2,\ x^5 \equiv 2x,\ x^6 \equiv x + 2,\ x^7 \equiv x^2 + 2x \equiv x + 1\}$. Pro kontrolu spočítáme, že $x^8 \equiv x^2 + x \equiv 1 = x^0$.

Tedy $\overline{x}$ je primitivním prvkem GF(9). Vždy existuje P, aby $\overline{x}$ bylo primitivním prvkem příslušného konečného tělesa. Takové P nazýváme primitivní polynom.

► 10.1.14. Věta. K libovolným $p \in \mathbb{P}$ a $n \in \mathbb{N}$ existuje $P \in Z_p[x]$, takový, že $\mathrm{st}\, P = n$ a P je ireducibilní nad Z_p.

◦ *Důkaz.* Už víme, že existuje $U = \mathrm{GF}\,(p^n)$, platí $\mathrm{ch}\, U = p$ a Z_p je prvotěleso U. Nechť α je primitivní prvek U. Ukážeme, že $U = Z_p(\alpha)$.

(⊆) Pokud $x = 0$, je $x \in Z_p(\alpha)$, pokud $x \neq 0$, je $x = \alpha^k$, tedy $x \in Z_p(\alpha)$.

(⊇) Platí $Z_p \cup \{\alpha\} \subseteq U$ a $Z_p(\alpha)$ je nejmenší takové, tedy $Z_p(\alpha) \subseteq U$.

Nutně $\alpha \neq 0$, tedy $\alpha \in U_*$ a $\alpha^{q-1} = 1$, kde $q = p^n$. Tedy α je kořenem polynomu $x^{q-1} - 1 \in Z_p[x]$ a α je algebraický nad Z_p. Nechť M_α je minimální polynom prvku α nad Z_p. Pak M_α je ireducibilní a je $\mathrm{st}\, M_\alpha = \mathrm{st}\, \alpha = \dim_{Z_p} Z_p(\alpha) = \dim_{Z_p} U = n$.

Hledaným polynomem je tedy minimální polynom primitivního prvku tělesa GF(q). □

• 10.2. Eulerova funkce ϕ

► 10.2.1. Definice. $\phi : \mathbb{N} \to \mathbb{N}$, $\phi(n)$ je počet čísel z $\widehat{n}$, která jsou s n nesoudělná.

► 10.2.2. Příklad. $\phi(1) = 1$, $\phi(2) = 1$, $\phi(3) = 2$, $\phi(4) = 2$, $\phi(5) = 4$.

► 10.2.3. Věta. Buďte $p, q \in \mathbb{P}$, $n, m \in \mathbb{N}$. Pak

(1) $\phi(p) = p - 1$;

(2) $\phi(p^n) = p^n - p^{n-1} = p^n \left(1 - \frac{1}{p}\right)$;

(3) $p \neq q$, pak $\phi(pq) = \phi(p)\phi(q)$;

(4) $\delta(m, n) = 1$, pak $\phi(mn) = \phi(m)\phi(n)$.

◦ *Důkaz.*

(1) Speciální případ (2).

(2) S p^n jsou soudělné právě všechny násobky p, kterých je v $\widehat{p^n}$ právě p^n/p.

(3) S pq jsou nesoudělné právě všechny násobky p a q, kterých je v $\widehat{pq}$ právě $q + p - 1$.

(4) Bez důkazu.

□

► 10.2.4. Lemma. Nechť $k, \ell, m \in \mathbb{N}$. Pak pokud $\delta(k, m) = \delta(\ell, m) = 1$, platí $\delta(k\ell, m) = 1$.

◦ *Důkaz.* Existují $u, v_{1,2} \in \mathbb{Z}$ tak, že $u_1 k + v_1 m = 1$ a $u_2 \ell + v_2 m = 1$. Vynásobením rovností dostaneme $(u_1 u_2)kl + (u_1 v_2 k + v_1 u_2 \ell + v_1 v_2 m)m = 1$. □

► 10.2.5. Věta. Mějme $m \in \mathbb{N}$, $m \geq 2$. Uvažujme Z_m a definujme $G_m^\bullet := \left\{\overline{k} \;\middle|\; \delta(k, m) = 1\right\} \subseteq Z_m^\bullet$. Pak G_m s operací násobení tříd je grupa o $\phi(m)$ prvcích.

◦ *Důkaz.* Součin tříd pomocí předchozího lemmatu zůstane v G. Taktéž $\delta(1, m) = 1$, tedy G má jednotku $\overline{1}$.

Pokud $\overline{k} \in G^\bullet$, pak $(\exists u, v)(uk + vm = 1)$, tedy $\overline{u}\overline{k} + \overline{v}\underbrace{\overline{m}}_{\overline{0}} = \overline{u}\overline{k} = \overline{1}$ a $\left(\overline{k}\right)^{-1} = \overline{u}$. A z definice Eulerovy funkce plyne, že $|G_m| = \phi(m)$. □

► 10.2.6. Věta (Euler, Fermat). Buďte $m \in \mathbb{N}$, $m \geq 2$ a nechť $k \in \widehat{m}$ je nesoudělné s m. Pak $k^{\phi(m)} \equiv_m 1$.

◦ *Důkaz.* Pro $\overline{k} \in G_m^\bullet$ je $\left(\overline{k}\right)^{\phi(m)} = \overline{1}$, tedy $k^{\phi(m)} \equiv_m 1$. □

► 10.2.7. Věta (Malá Fermatova věta). Je-li $p \in \mathbb{P}$ a $k \in \widehat{p - 1}$, pak $k^{p-1} \equiv_p 1$

◦ *Důkaz.* Speciální případ Eulerovy-Fermatovy věty pro $p \in \mathbb{P}$ a tedy $\phi(p) = p - 1$. □

► 10.2.8. Věta (Velká Fermatova věta). Pro $n \in \mathbb{N}$, $n > 2$ neexistují přirozená a, b, c taková, že $a^n + b^n = c^n$.

Rejstřík