

Obsah

1	Teorie množin	4
1.1	Dobře uspořádané množiny a ordinální čísla	5
1.2	Transfinitní indukce	7
1.3	Kardinální čísla a Cantorova-Bernsteinova věta	7
1.4	Operace s kardinálními a ordinálními čísly	8
1.5	Axiom výběru	10
2	Matematická logika	11
2.1	Výroková logika	11
2.2	Predikátová logika	13
2.3	Věta o úplnosti, věta o kompaktnosti a Löwenheimova-Skolemova věta	16
2.4	Gödelova věta o neúplnosti	17
3	Základní algebraické struktury	19
3.1	Grupy, okruhy, obory integrity, tělesa	19
3.2	Homomorfismy a faktorizace v teorii grup a okruhů	22
3.3	Vektorové prostory	22
4	Svazy a univerzální algebra	25
4.1	Modulární, distributivní a úplné svazy	25
4.2	Booleovy algebry	28
4.3	Variety algeber a Birkhoffova věta	29
5	Základy teorie kategorií	32
5.1	Definice a příklady kategorií, funktory a přirozené transformace	32
5.2	Yonedomo lemma	35
5.3	Kartézsky uzavřené kategorie	36
6	Limity	38
6.1	Součiny, součty, ekvalizátory, pullbacky, pushouty	38
6.2	Limity, kolimity	40
6.3	Limity pomocí součinů a ekvalizátorů	42
7	Adjungované funktory	43
7.1	Definice a příklady	43
7.2	Freydova věta	43

8	Rozšíření těles	45
8.1	Algebraická a konečná rozšíření	45
8.2	Rozkladová tělesa a normální rozšíření, algebraický uzávěr	45
8.3	Separabilní a neseeparabilní rozšíření	47
8.4	Klasické konstrukce pravítkem a kružítkem	48
9	Galoisova teorie	50
9.1	Základní věta Galoisovy teorie	51
9.2	Kruhov a abelovská rozšíření tělesa racionálních čísel	52
9.3	Řešitelná a radikálová rozšíření, Galoisova grupa polynomu, řešitelné grupy, souvislost s vyjadřováním kořenů polynomů v radikálech	53
10	Základy teorie modulů	55
10.1	Moduly, homomorfismy, základní konstrukce	55
10.2	Projektivní moduly a krátké exaktní posloupnosti	58
10.3	Tenzorový součin	58
10.4	Ploché moduly, Lazardova věta	59
10.5	Injektivní moduly a injektivní obal	60
11	Komutativní algebra a algebraická geometrie	61
11.1	Rezultant polynomu, polynomy více proměnných	61
11.2	Lokalizace okruhu, noetherovské okruhy a moduly, Hilbertova věta o bázi a Gröbnerova báze	62
11.3	Afinní a projektivní variety	64
11.4	Radikál ideálu, Hilbertova věta o nulách, vztah mezi ideály a algebraickými podmnožinami afinního prostoru, věta o Noetherovské normalizaci	64
12	Algebraická topologie	66
12.1	Definice singulárních homologií a kohomologií a jejich aplikace	66
12.2	Výpočet pro CW-komplexy	69
12.3	Homotopické grupy a jejich základní vlastnosti	71
13	Teorie grafů	73
13.1	Orientované a neorientované grafy a jejich reprezentace	73
13.2	Eulerovské a hamiltonovské grafy	74
13.3	Míry souvislosti grafu	75
13.4	Rovinné grafy: Eulerův vzorec a jeho důsledky, obarvení rovinného grafu pěti barvami	75
13.5	Prohledávání grafu do šířky a do hloubky	77
14	Grafové algoritmy	78
14.1	Minimální kostry: algoritmy Kruskala a Prima	78
14.2	Nejkratší cesty z jednoho vrcholu: Dijkstrův algoritmus, Bellmanův-Fordův algoritmus	79
14.3	Nejkratší cesty mezi všemi dvojicemi vrcholů: nejkratší cesty a násobení matic, Floydův-Warshallův algoritmus	79
14.4	Maximální toky v sítích: síť, Fordova-Fulkersonova metoda, maximální párování v bipartitních grafech	81

15 Lineární programování	83
15.1 Úlohy lineárního programování, dualita v lineárním programování	83
15.2 Geometrie polyedrů	84
15.3 Simplexová metoda a dopravní problém	84
16 Hry v normální formě	86
16.1 Hry n hráčů v normální formě: koncepty rovnováhy	86
16.2 Hry 2 hráčů v normální formě: antagonistické hry, optimální strategie	87
16.3 Řešení maticových her	88
16.4 Neantagonistické hry 2 hráčů: bimaticové hry, teorie užitečnosti, úlohy o dohodě, vyhrožování	89
17 Hry ve tvaru charakteristické funkce	91
17.1 Jádro a jeho existence, aplikace v ekonomii	92
17.2 Von Neumannovo-Morgensternovo řešení	92
17.3 Shapleyho hodnota	93

Kapitola 1

Teorie množin

Jazyk teorie množin je jazyk s rovností obsahující jediný predikátový symbol $\in$ arity dva. Teorie je dána následujícími axiomy (či schémataxiomů)

- Axiom extensionality: dvě množiny jsou si rovny právě tehdy, když mají stejné prvky

$$(\forall x, y)(x = y \leftrightarrow (\forall z)(z \in x \leftrightarrow z \in y))$$

- Axiom dvojice: pro libovolné dvě množiny a, b existuje množina $\{a, b\}$

$$(\forall x, y)(\exists z)(\forall t)(t \in z \leftrightarrow (t = x \vee t = y))$$

- Schéma axiomu vyčlenění: z libovolné množiny $\mathcal{A}$ lze vybrat prvky splňující nějakou formuli φ jazyka teorie množin

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (z \in x \wedge \varphi(z)))$$

- Axiom sjednocení: pro libovolnou množinu $\mathcal{A}$ existuje množina $\bigcup \mathcal{A}$

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow (\exists t)(t \in x \wedge z \in t))$$

- Axiom potenční množiny: pro libovolnou množinu x existuje její potenční množina $y = \mathcal{P}(x)$

$$(\forall x)(\exists y)(\forall z)(z \in y \leftrightarrow z \subseteq x)$$

- Axiom nekonečna: existuje množina přirozených čísel

$$(\exists x)(\emptyset \in x \wedge (\forall y)(y \in x \rightarrow y \cup \{y\} \in x))$$

- Schéma axiomu nahrazení: zadává-li formule F zobrazení, pak pro množinu a existuje množina b obsahující obsahující právě obrazy prvků a ve zobrazení F

$$\forall(x, y, z)((F(x, y) \wedge F(x, z)) \rightarrow y = z) \rightarrow (\forall a)(\exists b)(\forall w)(w \in b \leftrightarrow (\exists v)(v \in a \wedge F(v, w)))$$

- Axiom regularity (též axiom fundovanosti): každá množina vzniká z prázdné množiny.

$$(\forall x)(x \neq \emptyset \rightarrow (\exists y)(y \in x \wedge y \cap x = \emptyset))$$

Všimněme si, že jsme v axiomech použili i znaky ($\subset$, $\cup$, $\cap$, $\emptyset$), které nejsou symboly jazyka teorie množin. Jedná se o syntaktické zkratky, které obdržíme následujícím způsobem.

- Díky schématu axiomu vyčlenění má smysl hovořit o prázdné množině

$$\emptyset = \{x \in \mathcal{A} \mid a \neq a\},$$

podmnožině

$$x \subseteq y \leftrightarrow (\forall z)(z \in x \rightarrow z \in y),$$

průniku

$$A \cap B = \{a \in A \mid a \in B\}$$

a množinovém rozdílu

$$A \setminus B = \{a \in A \mid a \notin B\}$$

- Přímou z axiomu sjednocení dostáváme i sjednocení množin

Představme si několik konstrukcí, které nám dovolí pomocí takto málo obsáhlého jazyka vytvořit složitější množinové objekty.

- $(a, b) = \{\{a\}, \{a, b\}\},$
- $A \times B = \{(a, b) \mid a \in A, b \in B\}$

1.1 Dobře uspořádané množiny a ordinální čísla

Definice 1.1.1. Řekneme, že uspořádaná množina je *dobře uspořádaná*, jestliže libovolná její neprázdná podmnožina má nejmenší prvek.

Příklad. Každá dobře uspořádaná množina A je též lineárně uspořádaná. Vždyť pro libovolné $x, y \in A$ má množina $\{x, y\}$ minimální prvek, řekněme x . V tomto případě pak $x \leq y$. Ne každá lineárně uspořádaná množina je dobře uspořádaná. Například $\mathbb{Z}$ s klasickým lineárním uspořádáním není dobře uspořádaná množina. Podobně třeba $\mathbb{R}_0^+$ není dobře uspořádaná množina. Každý konečný řetězec je dobře uspořádaný.

Definice 1.1.2. Necht A, B jsou uspořádané množiny. Řekneme, že zobrazení $f: A \rightarrow B$ je *izotonní*, jestliže $\forall a, b \in A$ platí

$$a \leq b \Rightarrow f(a) \leq f(b).$$

Jestliže je f bijekce taková, že f i f^{-1} jsou izotonní, řekneme, že f je *izomorfismus uspořádaných množin*.

Lemma 1.1.3. Buď A dobře uspořádaná množina $f: A \rightarrow A$ prosté izotonní zobrazení, pak $\forall a \in A$ platí $a \leq f(a)$.

Definice 1.1.4. Necht A je uspořádaná množina. Množinu $Z \subseteq A$ nazveme *začátkem* množiny A , jestliže $\forall x \in A$ a $y \in Z$ platí $x < y \Rightarrow x \in Z$. Je-li navíc $Z \subset A$, pak Z nazveme *vlastním začátkem* množiny A .

Lemma 1.1.5. Dobře uspořádaná množina není izomorfní se svým vlastním začátkem.

Věta 1.1.6. Buďte A, B dobře uspořádané množiny, pak existuje nejvýše jeden izomorfismus $f: A \rightarrow B$.

Věta 1.1.7. *Nechť A, B jsou dobře uspořádané množiny, pak nastane právě jedna z následujících možností*

1. $A \cong B$,
2. A je izomorfní s vlastním začátkem B ,
3. B je izomorfní s vlastním začátkem A .

Definice 1.1.8. Nechť A, B jsou dobře uspořádané množiny. *Lexikografický součin $A \cdot B$ množin A, B rozumíme kartézský součin $A \times B$ spolu s uspořádáním*

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

Věta 1.1.9. *Nechť A, B jsou dobře uspořádané množiny, pak je též $A \cdot B$ dobře uspořádaná množina.*

Poznámka. Lexikografický součin není obecně komutativní. Například $\omega \cdot 2 \not\cong 2 \cdot \omega$. Lexikografický součin je asociativní v tom smyslu, že $A \cdot (B \cdot C) \cong (A \cdot B) \cdot C$.

Definice 1.1.10. *Součtem $A + B$ dvou dobře uspořádaných disjunktních množin rozumíme jejich sjednocení spolu s uspořádáním*

$$x \leq y \iff (x, y \in A, x \leq y) \vee (x, y \in B, x \leq y) \vee (x \in A, y \in B)$$

Poznámka. Součet dobře uspořádaných množin není komutativní, vždyť $\omega + 1 \not\cong 1 + \omega$.

Definice 1.1.11. Každé dobře uspořádané množině A přiřadíme symbol $\bar{A}$ tak, že $\bar{A} = \bar{B}$ právě tehdy, když $A \cong B$. Symboly $\bar{A}$ se nazývají *ordinální čísla*.

V řeči ZF bychom mohli definovat ordinální číslo takto

Definice 1.1.12. Ordinálním číslem rozumíme tranzitivní množinu (tj. $x \in X \iff x \subseteq X$) dobře uspořádanou relací $\in$.

Definice 1.1.13. Položme $\bar{A} \leq \bar{B}$, jestliže je A izomorfní s vlastním začátkem B .

Poznámka. Díky větě 1.1.7 je relace $\leq$ relací lineárního uspořádání.

Definice 1.1.14. Pro libovolné ordinální číslo α položme

$$W(\alpha) = \{\beta \mid \beta < \alpha \text{ je ordinální číslo}\}.$$

Lemma 1.1.15. *Nechť α je ordinální číslo. Množina $W(\alpha)$ je dobře uspořádaná a platí $\overline{W(\alpha)} = \alpha$.*

Věta 1.1.16. *Třída ordinálních čísel je dobře uspořádaná relací $\leq$.*

Definice 1.1.17. Ordinální číslo se nazývá *limitní*, jestliže množina $W(\alpha)$ nemá největší prvek. V opačném případě se číslo nazývá *izolované*.

1.2 Transfinitní indukce

Věta 1.2.1. *Bud' A dobře uspořádaná množina. Nechť pro libovolný prvek $a \in A$ je dán výrok $V(a)$. Předpokládejme, že pro libovolné $a \in A$ platí*

($\star$) *Je-li pravdivý výrok $V(x)$ pro všechna $x < a$, je pravdivý výrok $V(a)$.*

Pak je výrok $V(a)$ pravdivý pro všechna $a \in A$.

Důkaz. Nechť $B = \{a \in A \mid V(a) \text{ není pravdivý}\}$. Pokud by $B \neq \emptyset$, pak B má nejmenší prvek. To je spor s ($\star$).

Transfinitní indukce se někdy formuluje pro ordinální čísla následujícím způsobem:

Věta 1.2.2. *Nechť On značí třídu ordinálních čísel. Pak*

$$(X \subseteq On \wedge (\alpha \in On)(\alpha \subseteq X \Rightarrow \alpha \in X)) \Rightarrow X = On.$$

Věta 1.2.3. *Nechť On značí třídu ordinálních čísel. Nechť*

1. $X \subseteq On$,
2. $\emptyset \in X$,
3. $(\alpha \in On)(\alpha \in X \Rightarrow \alpha \cup \{\alpha\} \in X)$,
4. *pro každý limitní ordinál α platí $\alpha \subseteq X \Rightarrow \alpha \in X$,*

pak $X = On$.

1.3 Kardinální čísla a Cantorova-Bernsteinova věta

Definice 1.3.1. Ordinální číslo α se nazývá *kardinálním číslem*, jestliže každé menší ordinální číslo $\beta < \alpha$ má menší mohutnost (tj. neexistuje injekce $\alpha \rightarrow \beta$).

Alternativně

Definice 1.3.2. Každé množině A přiřadíme symbol $|A|$ takový, že $|A| = |B|$ právě tehdy, když množiny A, B mají stejnou mohutnost, tj. existuje mezi nimi bijekce. Symboly $|A|$ se nazývají kardinální čísla.

Položíme $|A| \leq |B|$, jestliže existuje injektivní zobrazení $A \rightarrow B$.

Příklad. *Nezáporná celá čísla považujeme za kardinální čísla a sice za mohutnosti konečných množin.*

Mohutnost spočetné množiny značíme $\aleph_0$.

Mohutnost množiny reálných čísel nazýváme mohutnost kontinuta a značíme ji c .

Věta 1.3.3 (Cantorova-Bernsteinova). *Jestliže $|A| \leq |B|$ a $|B| \leq |A|$, pak $|A| = |B|$.*

Důkaz. Budte $f: A \rightarrow B$ a $g: B \rightarrow A$ prostá zobrazení. Hledáme bijekci mezi A a B . Uvažme zobrazení

$$\begin{aligned} h: \mathcal{P}(A) &\rightarrow \mathcal{P}(A), \\ h: X &\mapsto A \setminus g(B \setminus f(X)). \end{aligned}$$

Snadno se nahlédne, že h je izotonní zobrazení, kde uspořádání je dáno množinovou inkluzí. Protože je $\mathcal{P}(A)$ úplný svaz, existuje podle Tarského věty pevný bod zobrazení h , označme jej W . Definujme

$$F: A \rightarrow B,$$

$$F: x \mapsto \begin{cases} f(x) & x \in W, \\ g^{-1}(x) & x \in A \setminus W. \end{cases}$$

Je-li $x \in A \setminus W = A \setminus h(W) = A \setminus (A \setminus g(B \setminus f(X))) = g(B \setminus f(X)) \subset \text{im } g$. Dává tedy smysl uvažovat $g^{-1}(x)$. Protože je g injektivní, je vzor nejvýše jednoprvkový. Zobrazení F je tedy dobře definované. Zbývá ukázat, že je bijekce.

Nechť $F(x) = F(y)$. Pokud $x, y \in W$, pak z injektivit f je $x = y$. Pokud $x, y \in A \setminus W$, pak je opět $x = y$, vždyť g je zobrazení. Konečně pokud $x \in W$ a $y \in A \setminus W$, tj. $f(x) = g^{-1}(y)$. Aplikací g dostáváme $g(f(x)) = y \notin W$. Přitom $f(x) \in f(W)$, tedy $f(x) \notin B \setminus f(W)$. Z injektivit g dostáváme, že $g(f(x)) \notin g(B \setminus f(W))$, tedy $g(f(x)) \in A \setminus g(B \setminus f(W)) = W$, což je spor. Nutně je tedy F injektivní.

Nechť $y \in B$ a přitom $y \notin F(A)$. Pak $y \notin f(W)$, tedy $y \in B \setminus f(W)$, a proto $g(y) \notin W$. Proto $y = F(g(y))$, což je spor. F je tedy hledaná bijekce.

Poznámka. Předchozí věta tedy říká, že relace $\leq$ na kardinálních číslech je uspořádání.

1.4 Operace s kardinálními a ordinálními čísly

Definice 1.4.1. Nechť $\alpha = |A|$ a $\beta = |B|$. Klademe

1. $\alpha + \beta = |A \cup B|$ pro $A \cap B = \emptyset$,
2. $\alpha \cdot \beta = |A \times B|$,
3. $\alpha^\beta = |A^B|$,
4. $\sum_{i \in I} \alpha_i = |\bigcup_{i \in I} A_i|$, kde A_i jsou po dvou disjunktní.

Věta 1.4.2. Platí

1. $(\alpha \cdot \beta)^\gamma = \alpha^\gamma \cdot \beta^\gamma$,
2. $(\alpha^\beta)^\gamma = \alpha^{\beta \cdot \gamma}$,
3. $\alpha^{\beta + \gamma} = \alpha^\beta \cdot \alpha^\gamma$.

Dále platí

1. $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$,
2. $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$

Věta 1.4.3 (AC). Pro libovolné nekonečné kardinální číslo $\aleph$ platí $\aleph \cdot \aleph = \aleph$.

Důsledek 1.4.4 (AC). Pro libovolná ordinální čísla α, β platí

$$\aleph_\alpha \cdot \aleph_\beta = \max\{\aleph_\alpha, \aleph_\beta\},$$

$$\aleph_\alpha + \aleph_\beta = \max\{\aleph_\alpha, \aleph_\beta\}.$$

Pokud navíc $\alpha \leq \beta$, pak

$$\aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}.$$

Definice 1.4.5. Necht $\alpha = |A|$ a $\beta = |B|$, pak definujeme

1. $\alpha + \beta = |A + B|$,
2. $\alpha \cdot \beta = |B \cdot A|$.

Věta 1.4.6. *Platí*

1. $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$,
2. $\alpha + 0 = 0 + \alpha = \alpha$,
3. $\alpha \cdot 0 = 0 \cdot \alpha = 0$,
4. $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$,
5. $\alpha \cdot 2 = \alpha + \alpha$.

Příklad. *Operace $+$, $\cdot$ nejsou komutativní*

$$\begin{aligned} 1 + \omega &= \omega \neq \omega + 1, \\ 2 \cdot \omega &= \omega \neq \omega + \omega = \omega \cdot 2. \end{aligned}$$

Lemma 1.4.7. *Pro libovolná ordinální čísla platí*

1. $\alpha < \beta \Rightarrow \gamma + \alpha < \gamma + \beta$,
2. $\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma$,
3. $\alpha < \beta \Rightarrow \gamma \cdot \alpha < \gamma \cdot \beta$,
4. $\alpha \leq \beta \Rightarrow \alpha \cdot \gamma \leq \beta \cdot \gamma$,
5. $\forall \alpha, \beta$ takové, že $\alpha \leq \beta$ existuje jediné γ takové, že $\alpha + \gamma = \beta$,
6. dělení se zbytkem: $\forall \alpha, 0 < \beta$ existují jediná δ, ϱ , kde $\varrho < \alpha$, taková, že

$$\alpha = \beta \cdot \delta + \varrho$$

7. $\alpha^{\beta+\gamma} = \alpha^\beta \cdot \alpha^\gamma$,
8. $\alpha^{\beta^\gamma} = \alpha^{\beta \cdot \gamma}$,
9. každé ordinální číslo α lze zapsat v mocninách ω , tj.

$$\forall \alpha \exists \gamma_0, \dots, \gamma_k, m_0, \dots, m_k \in \mathbb{N}: \alpha = \omega^{\gamma_0} \cdot m_0 + \dots + \omega^{\gamma_k} \cdot m_k$$

1.5 Axiom výběru

Axiom výběru: Buď I množina a $A_i, i \in I$ neprázdné množiny. Pak množina $\prod_{i \in I} A_i$ je rovněž neprázdná.

Axiom říká, že libovolná množina neprázdných množin $\{A_i \mid i \in I\}$ má tzv. výběrovou funkci, tj. zobrazení

$$f: I \rightarrow \bigcup_{i \in I} A_i$$

takové, že $f(i) \in A_i$ pro libovolné $i \in I$. (Uvědomme si, že kartézský součin je právě množina výběrových funkcí, která je podle AC neprázdná.)

Někdy je AC též formulován takto:

$$\forall X (\emptyset \notin X \rightarrow \exists f: X \rightarrow \bigcup X \forall A \in X (f(A) \in A)).$$

Věta 1.5.1. *Následující tvrzení jsou ekvivalentní:*

1. *axiom výběru,*
2. *princip dobrého uspořádání (každou množinu lze dobře uspořádat),*
3. *Zornovo lemma (každá neprázdna uspořádaná množina, ve které má každý řetězec horní zavoru, obsahuje nějaký maximální prvek),*
4. *každý vektorový prostor má bázi,*
5. *každý vlastní ideál netriviálního okruhu lze vnořit do maximálního ideálu,*
6. *Tichonovova věta (součin kompaktních prostorů je kompaktní),*
7. *každý souvislý graf má kostru.*

Kapitola 2

Matematická logika

Nyní budeme chtít pro výrokovou a predikátovou logiku popsat následující

1. Vymezení užívaných symbolů (abecedy)
2. Syntaxe formulí
3. Sémantika
4. Odvozovací systém

2.1 Výroková logika

Definice 2.1.1. *Abecedu výrokové logiky tvoří následující symboly*

- znaky pro *výrokové proměnné* $A, B, C, \dots$, kterých je spočetně mnoho,
- logické spojky $\wedge, \vee, \rightarrow, \neg$,
- závorky $(,)$.

Definice 2.1.2. *Formulí výrokové logiky rozumíme slovo φ nad abecedou výrokové logiky, pro které existuje vytvářející posloupnost, tj. konečná posloupnost slov, $\psi_1, \dots, \psi_k$, kde $k \geq 1$, ψ_k je φ a pro každé $1 \leq i \leq k$ má slovo ψ_i jeden z následujících tvarů*

1. výroková proměnná,
2. $\neq \psi_j$ pro nějaké $1 \leq j < i$,
3. $(\psi_j \circ \psi_l)$ pro nějaká $1 \leq j, l < i$, kde $\circ \in \{\wedge, \vee, \rightarrow\}$.

Poznámka. Při zápisu formulí se obvykle vynechávají vnější závorky a často i některé vnitřní, nevede-li vzniklá syntaktická nejednoznačnost k nejednoznačnosti sémantické.

Dále lze zavést zkratku $\varphi \leftrightarrow \psi$ pro $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

Definice 2.1.3. *Pravdivostní ohodnocení (valiace) je zobrazení v , které každé výrokové proměnné přiřadí hodnotu 0 nebo 1.*

Indukcí se pak valiace rozšíří na všechny výrokové formule uvážením vytvářející posloupnosti, kde logickým spojkám přiřazujeme význam standardním způsobem.

Definice 2.1.4. Řekneme, že výroková formule φ je

- *pravdivá* (respektive *nepravdivá*) při valuaci v , pokud $v(\varphi) = 1$ (respektive $v(\varphi) = 0$),
- *splnitelná*, jestliže existuje valuace v taková, že $v(\varphi) = 1$,
- *tautologie* (respektive *kontradikce*), jestliže $v(\varphi) = 1$ (respektive $v(\varphi) = 0$) pro každou valuaci v .

Soubor T výrokových formulí se nazývá *splnitelný*, jestliže existuje valuace v taková, že $v(\varphi) = 1$ pro každé $\varphi \in T$.

Formule φ, ψ se nazývají *ekvivalentní*, píšeme $\varphi \approx \psi$, jestliže pro každou valuaci v platí $v(\varphi) = v(\psi)$.

Definice 2.1.5. Formule je *tautologickým důsledkem* souboru formulí T , píšeme $T \models \varphi$, jestliže $v(\varphi) = 1$ pro každou valuaci v takovou, že $v(\psi) = 1$ pro každou formuli $\psi \in T$. Je-li $T = \emptyset$, píšeme $\models \varphi$.

Můžeme požadovat, aby náš logický systém byl vytvořen z jiných logických spojek. Za tímto účelem zavedeme pojem výrokové funkce.

Definice 2.1.6. *Výrokovou funkcí* rozumíme funkci $F: \{0, 1\}^n \rightarrow \{0, 1\}$, kde $n \geq 1$.

Stejným způsobem nyní můžeme definovat abecedu, formuli a valuaci, pokud místo $\wedge, \vee, \rightarrow$ a $\neg$ uvažíme výrokové funkce $F_1, \dots, F_k$. Obdržíme tím logický systém, který značíme $\mathcal{L}(F_1, \dots, F_k)$. Uvažme na množině výrokových proměnných pevné lineární uspořádání. Pak každá formule φ jednoznačně určuje výrokovou funkci $F_\varphi: \{0, 1\}^n \rightarrow \{0, 1\}$ (dosazením 0, 1 za výrokové proměnné).

Definice 2.1.7. Systém $\mathcal{L}(F_1, \dots, F_k)$ se nazývá *plnohodnotný*, jestliže pro každou výrokovou funkci F existuje formule φ z tohoto systému taková, že $F = F_\varphi$.

Věta 2.1.8. *Systémy $\mathcal{L}(\vee, \wedge, \neg)$ a $\mathcal{L}(\rightarrow, \neq)$ jsou plnohodnotné. Systémy $\mathcal{L}(\vee, \neg)$, $\mathcal{L}(\vee, \wedge)$ plnohodnotné nejsou.*

Definice 2.1.9. Výroková funkce F se nazývá *Schefferovská*, jestliže $\mathcal{L}(F)$ je plnohodnotný systém.

Věta 2.1.10 (o kompaktnosti). *Nechť T je soubor formulí výrokové logiky. T je splnitelný právě tehdy, když je každá konečná část T je splnitelná.*

Uvažme $\mathcal{L}(\rightarrow, \neg)$ a následující (Lukasiewiczův) odvozovací systém, která je dán schématy axiomů

- A1: $\varphi \rightarrow (\psi \rightarrow \varphi)$,
- A2: $(\varphi \rightarrow (\psi \rightarrow \xi)) \rightarrow ((\varphi \rightarrow \psi) \rightarrow (\varphi \rightarrow \xi))$
- A3: $(\neg\varphi \rightarrow \neg\psi) \rightarrow (\psi \rightarrow \varphi)$

a odvozovacím pravidlem

- MP: Z φ a $\varphi \rightarrow \psi$ odvod ψ .

Definice 2.1.11. Buď T systém formulí.

- *Důkazem* formule ψ z předpokladů T rozumíme konečnou posloupnost formulí $\varphi_1, \dots, \varphi_k$, kde φ_k je ψ a pro každé φ_i , kde $1 \leq i \leq k$ platí některá z následujících podmínek

- φ_i je prvek z T ,
- φ_i je instancí jednoho ze schémat $A1 - A3$,
- φ_i vznikne aplikací MP na formule φ_m, φ_n pro vhodné $1 \leq m, n < i$.
- Formule ψ se nazývá *dokazatelná z předpokladů T* , píšeme $T \vdash \psi$, jestliže existuje důkaz ψ z předpokladů T . Je-li $T = \emptyset$, říkáme, že ψ je dokazatelná a píšeme $\vdash \psi$.

Věta 2.1.12 (o dedukci). *Nechť φ, ψ jsou formule a T soubor formulí. Pak $T \cup \{\psi\} \vdash \varphi$ právě tehdy, když $T \vdash \psi \rightarrow \varphi$.*

Věta 2.1.13 (o korektnosti). *Nechť φ je formule a T soubor formulí. Jestliže $T \vdash \varphi$, pak $T \models \varphi$.*

Věta 2.1.14 (o úplnosti). *Nechť φ je formule a T soubor formulí. Jestliže $T \models \varphi$, pak $T \vdash \varphi$.*

2.2 Predikátová logika

Definice 2.2.1. *Jazykem (stejně jako jazykem s rovností) rozumíme systém predikátových symbolů a funkčních symbolů, kde u každého symbolu je dána jeho arita (četnost), který je nezáporným celým číslem.*

Predikátovým a funkčním symbolům se souhrnně říká *mimologické symboly* a jazyk je jimi plně určen.

Definice 2.2.2. Abecedu predikátové logiky pro jazyk $\mathcal{L}$ tvoří následující symboly:

- znaky pro proměnné $x, y, z, \dots$, kterých je spočetně mnoho,
- mimologické symboly
- je-li $\mathcal{L}$ jazyk s rovností, obsahuje abeceda speciální znak $=$ pro rovnost,
- logické spojky $\rightarrow$ a $\neg$,
- symbol $\forall$ pro univerzální kvantifikátor,
- závorky $(,)$.

Definice 2.2.3. *Termem jazyka $\mathcal{L}$ rozumíme slovo t nad abecedou predikátové logiky pro jazyk $\mathcal{L}$, pro které existuje vytvořující posloupnost slov $t_1, \dots, t_k$, kde $k \geq 1$, t_k je t a pro každé $1 \leq i \leq k$ má slovo t_i jeden z následujících tvarů:*

- proměnná
- $f(t_{i_1}, \dots, t_{i_n})$, kde $1 \leq i_1, \dots, i_n < k$, f je funkční symbol jazyka $\mathcal{L}$, a n je arita f .

Term se nazývá *uzavřený*, jestliže neobsahuje proměnné.

Definice 2.2.4. *Formulí predikátového počtu jazyka $\mathcal{L}$ rozumíme slovo φ nad abecedou predikátové logiky pro jazyk $\mathcal{L}$, pro které existuje vytvořující posloupnost slov $\psi_1, \dots, \psi_k$, kde $k \geq 1$, ψ_k je φ , a pro každé $1 \leq i \leq k$ má slovo ψ_i jeden z následujících tvarů:*

- $P(t_1, \dots, t_n)$, kde P je predikátový symbol jazyka $\mathcal{L}$ arity n a $t_1, \dots, t_n$ jsou termy jazyka $\mathcal{L}$,
- $t_1 = t_2$, je-li jazyk $\mathcal{L}$ s rovností a t_1, t_2 jsou termy jazyka $\mathcal{L}$,
- $\neg \psi_j$ pro nějaké $1 \leq j < i$,

- $(\psi_j \rightarrow \psi_l)$ pro nějaká $1 \leq j, l < i$,
- $\forall x \psi_j$, kde x je proměnná a $1 \leq j < i$.

Poznámka. Pro přehlednost se obvykle využívají následující zkratky:

- $\exists x \varphi$ značí $\neg \forall x \neg \varphi$,
- $\varphi \vee \psi$ značí $\neg \varphi \rightarrow \psi$,
- $\varphi \wedge \psi$ značí $\neg(\varphi \rightarrow \neg \psi)$,
- $\varphi \leftrightarrow \psi$ značí stejně jako ve výrokové logice konjunkci obou implikací.

Definice 2.2.5. Každý výskyt proměnné ve formuli predikátového počtu je buď *volný* nebo *vázaný* podle následujícího induktivního předpisu

- Ve formuli $P(t_1, \dots, t_n)$ jsou všechny proměnné volné.
- Výrokové spojky nemění charakter výskytu proměnných.
- Ve formuli $\forall x \psi$ je výskyt proměnné x (včetně výskytu za kvantifikátorem) vázaný, výskyt proměnné různé od x zůstává stejný, jaký byl ve formuli ψ .

Proměnná se nazývá *volnou* (respektive *vázanou*) ve formuli, má-li v ní volný (respektive *vázaný*) výskyt.

Formule se nazývá *otevřená*, jestliže v ní žádná proměnná nemá vázaný výskyt.

Formule se nazývá *uzavřená* (též *sentence*), jestliže v ní žádná proměnná nemá volný výskyt.

Zápis $\varphi(x_1, \dots, x_n)$ značí, že všechny volné proměnné ve formuli φ jsou mezi $x_1, \dots, x_n$ (přičemž ne nutně každá z těchto proměnných musí být volná).

Univerzální uzávěr formule φ je formule tvaru $\forall x_1 \dots \forall x_n \varphi$, kde $x_1, \dots, x_n$ jsou právě všechny volné proměnné formule φ .

Definice 2.2.6. Term t se nazývá *substituovatelný* za proměnnou x ve formuli φ , jestliže žádný výskyt proměnné v termu t se nestane vázaným po provedení substituce termu t za každý výskyt x ve formuli φ . Je-li t substituovatelný za x ve φ , značí zápis $\varphi(x|t)$ formuli, která vznikne nahrazením každého volného výskytu x ve φ za t .

Přirozeným způsobem rozšíříme tuto definici na $\varphi(x_1|t_1, \dots, x_n|t_n)$.

Přejdeme nyní k sémantice predikátové logiky.

Definice 2.2.7. *Realizace* $\mathcal{M}$ jazyka $\mathcal{L}$ je zadána

- Neprázdným souborem M , který se nazývá *univerzum* či *nosič*. Prvky univerza se nazývají *individa*.
- Přiřazením, které každému n -árnímu predikátovému symbolu P přiřadí n -ární relaci P_M na M .
- Přiřazením, které každému m -árnímu funkčnímu symbolu funkci $f_M: M^m \rightarrow M$.

Ohodnocením rozumíme zobrazení přiřazující proměnným prvky univerza M .

Realizaci termu t při ohodnocení e v realizaci $\mathcal{M}$, psáno $t^{\mathcal{M}}[e]$ (případně jen $t[e]$, je-li $\mathcal{M}$ zřejmé z kontextu), definujeme induktivně

- $x[e] = e(x)$,

- $f(t_1, \dots, t_m)[e] = f_M(t_1[e], \dots, t_m[e])$

Definice 2.2.8. Buď $\mathcal{M}$ realizace jazyka $\mathcal{L}$, e ohodnocení a φ formule predikátového počtu jazyka $\mathcal{L}$. Ternární vztah $\mathcal{M} \models \varphi[e]$ definujeme indukcí ke struktuře φ

- $\mathcal{M} \models P(t_1, \dots, t_m)[e]$ právě tehdy, když $(t_1[e], \dots, t_m[e]) \in P_M$,
- je-li $\mathcal{L}$ jazyk s rovností, definujeme $\mathcal{M} \models (t_1 = t_2)[e]$ právě tehdy, když $t_1[e]$ a $t_2[e]$ jsou stejná individua,
- $\mathcal{M} \models \neg\psi[e]$ právě tehdy, když není $\mathcal{M} \models \psi[e]$,
- $\mathcal{M} \models (\psi \rightarrow \xi)[e]$ právě tehdy, když $\mathcal{M} \models \xi[e]$ nebo není $\mathcal{M} \models \psi[e]$,
- $\mathcal{M} \models \forall x\psi[e]$ právě tehdy, když $\mathcal{M} \models \psi[e(x|a)]$ pro každý prvek a univerza M .

Je-li $\mathcal{M} \models \varphi[e]$, říkáme, že φ je *pravdivá v $\mathcal{M}$ při ohodnocení e* .

Je-li $\mathcal{M} \models \varphi[e]$ pro každé e , řekneme, že φ je *pravdivá v $\mathcal{M}$* , píšeme $\mathcal{M} \models \varphi$.

Definice 2.2.9. Buď $\mathcal{L}$ jazyk (případně jazyk s rovností).

- *Teorií* (s jazykem $\mathcal{L}$) rozumíme soubor T formulí predikátového počtu jazyka $\mathcal{L}$. Prvky T se nazývají *axiomy teorie T* .
- Realizace $\mathcal{M}$ jazyka $\mathcal{L}$ se nazývá *model* teorie T , psáno $\mathcal{M} \models T$, jestliže $\mathcal{M} \models \varphi$ pro každé φ z T .
- Teorie se nazývá *splnitelná*, jestliže má model.
- Je-li $\mathcal{M}$ realizace jazyka $\mathcal{L}$, pak $Th(\mathcal{M})$ označuje teorii tvořenou právě všemi uzavřenými formulemi, které jsou v $\mathcal{M}$ pravdivé.
- Formule φ se nazývá *semantickým důsledkem* teorie T , psáno $T \models \varphi$, jestliže φ je pravdivá v každém modelu teorie T .

Opět můžeme uvážit odvozovací systém podobně, jako jsme tomu učinili v predikátové logice. Přibudou nám zde dvě nová schémata axiomů a jedno odvozovací pravidlo.

- Schéma axiomu specifikace $\forall x\varphi \rightarrow \varphi(x|t)$, kde t je substituovatelný za x ve φ .
- Schéma axiomu distribuce $(\forall x(\varphi \rightarrow \psi)) \rightarrow (\varphi \rightarrow \forall x\psi)$, kde x nemá volný výskyt ve φ .
- Odvozovací pravidlo generalizace: z φ odvod $\forall x\varphi$.

Pro jazyk $\mathcal{L}$ s rovností je potřeba ještě přidat axiomy rovnosti

- $x = x$,
- $(x_1 = y_1 \wedge \dots \wedge x_n = y_n \wedge P(x_1, \dots, x_n)) \rightarrow P(y_1, \dots, y_n)$, kde P je predikátový symbol arity n ,
- $(x_1 = y_1 \wedge \dots \wedge x_m = y_m) \rightarrow (f(x_1, \dots, x_m) = f(y_1, \dots, y_m))$, kde f je funkční symbol arity m .

Definice 2.2.10. Buď T teorie jazyka $\mathcal{L}$. *Důkazem* formule φ v teorii T rozumíme konečnou posloupnost formulí $\psi_1, \dots, \psi_k$, kde ψ_k je φ a pro každé ψ_i , kde $1 \leq i \leq k$, platí alespoň jedna z následujících podmínek

- ψ_i je prvek T ,
- ψ_i je instancí některého axiomu,
- ψ_i vznikne aplikací některého odvozovacího pravidla na některé (či některou) z předchozích formulí

Definice 2.2.11. Buď T teorie jazyka $\mathcal{L}$.

- Formule ψ se nazývá *dokazatelná* v teorii T , píšeme $T \vdash \psi$, jestliže existuje důkaz ψ v T . Jestliže $T \vdash \psi$, kde T je prázdná, říkáme, že ψ je dokazatelná a píšeme jen $\vdash \psi$.
- Formule ψ se nazývá *vyvratitelná* v teorii T , jestliže $T \vdash \neg\psi$.
- Teorie T se nazývá *sporná*, jestliže je v T dokazatelná každá formule predikátové logiky jazyka $\mathcal{L}$.
- Teorie je *bezesporná*, jestliže není sporná.

Věta 2.2.12 (o dedukci). *Nechť T je teorie jazyka $\mathcal{L}$, ψ uzavřená formule jazyka $\mathcal{L}$ a φ libovolná formule jazyka $\mathcal{L}$. Pak $T \vdash \psi \rightarrow \varphi$ právě tehdy, když $T \cup \{\psi\} \vdash \varphi$.*

2.3 Věta o úplnosti, věta o kompaktnosti a Löwenheimova-Skolemova věta

Poznámka. Shrňme si značení z předchozích definic

- $\mathcal{M} \models \varphi[e]$ značí, že formule φ je pravdivá v modelu $\mathcal{M}$ při ohodnocení e
- $\mathcal{M} \models \varphi$ značí, že formule φ je pravdivá v modelu $\mathcal{M}$
- $\mathcal{M} \models T$ značí, že každá formule teorie T je pravdivá v modelu $\mathcal{M}$, přitom říkáme, že $\mathcal{M}$ je modelem teorie T
- $T \models \varphi$ značí, že φ je pravdivá v každém modelu teorie T
- $T \vdash \varphi$ značí, že φ je dokazatelná v T

Teorie je sporná, jestliže v ní můžeme dokázat každou formuli. Teorie je bezesporná, jestliže není sporná.

Věta 2.3.1 (o korektnosti). *Nechť T je teorie a φ je formule jazyka teorie T . Jestliže $T \vdash \varphi$, pak $T \models \varphi$.*

Věta 2.3.2 (o úplnosti). *Každá bezesporná teorie má model. Nechť T je teorie a φ je formule jazyka teorie T . Jestliže $T \models \varphi$, pak $T \vdash \varphi$.*

Věta 2.3.3 (o kompaktnosti). *Teorie T má model právě tehdy, když každá její podteorie s konečně mnoha axiomy (a s minimálním jazykem, v němž jsou tyto axiomy formulovatelné) má model.*

Důkaz. „ $\Rightarrow$ “: Zřejmé.

„ $\Leftarrow$ “: Stačí ukázat, že T je bezesporná. Kdyby T byla sporná (případ, kdy $\mathcal{L}$ je bez rovnosti a neobsahuje jediný predikátový symbol, tedy neexistuje žádná formule predikátového počtu nad jazykem $\mathcal{L}$, je zřejmý), existoval by důkaz formule $\psi \wedge \neg\psi$ v T . Tento důkaz je je konečný, využívá jen konečně mnoho axiomů T , které tvoří spornou podteorii T , spor.

Věta 2.3.4. *Nechť T je teorie a nechť pro každé $n \in \mathbb{N}$ existuje model teorie T , jehož nosič má mohutnost alespoň n . Pak T má nekonečný model.*

Věta 2.3.5 (Löwenheimova-Skolemova). *Nechť T je teorie s jazykem $\mathcal{L}$, která má nekonečný model. Nechť κ je nekonečný kardinál takový, že $\kappa \geq |\mathcal{L}|$. Pak T má model mohutnosti κ .*

2.4 Gödelova věta o neúplnosti

Jazyk aritmetiky je jazyk s rovností obsahující konstantu 0, unární funkční symbol S a dva binární funkční symboly $\cdot$ a $+$.

Význačnou realizací jazyka aritmetiky je $(\mathbb{N}_0, \cdot, +)$, kde univerzem je soubor všech nezáporných celých čísel, 0 je realizována jako nula, S jako funkce následníka, $\cdot$ jako násobení a $+$ jako sčítání. Jedním ze základních kroků Hilbertova programu formalizace matematiky mělo být vytvoření rekurzivní a úplné teorie T jazyka aritmetiky, tedy teorie T takové, že

- formule dokazatelné v T jsou právě formule pravdivé v $(\mathbb{N}_0, +, \cdot)$
- pro každou posloupnost symbolů lze mechanicky ověřit, zda je či není důkazem v T

Peanova aritmetika

- $\forall x \ S(x) \neq 0$,
- $\forall x \forall y \ S(x) = S(y) \rightarrow x = y$,
- $\forall x \ x + 0 = x$,
- $\forall x \forall y \ x + S(y) = S(x + y)$,
- $\forall x \ x \cdot 0 = 0$,
- $\forall x \forall y \ x \cdot S(y) = (x \cdot y) + y$,
- $(\varphi(0) \wedge \forall x (\varphi(x) \rightarrow \varphi(S(x)))) \rightarrow \forall x \varphi(x)$, kde φ je formule s jednou volnou proměnnou x

Definice 2.4.1. Řekneme, že teorie T jazyka aritmetiky je *rekurzivní*, jestliže jazyk tvořený zápisy všech důkazů v T je rekurzivní.

Věta 2.4.2. *Nechť T je rekurzivní teorie jazyka aritmetiky. Pak jazyk tvořený všemi formulami dokazatelnými v T je rekurzivně vyčíslitelný.*

Nechť jazyk *Valid* (respektive *Provable*) značí jazyky nad abecedou $\{v, +, \cdot, 0, S, (,), \forall, \rightarrow, \neg, =\}$, kde proměnné zapisujeme $v, vv, vvv, \dots$, obsahující zápisy všech formulí jazyka Peanovy aritmetiky, které jsou pravdivé (respektive dokazatelné) v realizaci $(\mathbb{N}_0, +, \cdot)$, respektive dokazatelné ze systémů axiomů Peanovy aritmetiky.

Jistě $\text{Provable} \subseteq \text{Valid}$, neboť Peanova aritmetika je korektní. Přitom Gödlova věta říká, že tato inkluze je vlastní.

Jazyk *Provable* je rekurzivně spočetný. Dá se ukázat, že jazyk *Valid* rekurzivně vyčíslitelný není.

Věta 2.4.3 (o neúplnosti). *Neexistuje žádná rekurzivní teorie jazyka aritmetiky, ve které jsou dokazatelné právě všechny formule pravdivé v realizaci $(\mathbb{N}_0, +, \cdot)$.*

Speciálně pro každou korektní rekurzivní teorii T (tj. pro teorii, která umožňuje dokázat pouze formule pravdivé v $(\mathbb{N}_0, +, \cdot)$) nutně existuje formule platná v $(\mathbb{N}_0, +, \cdot)$, která není v T dokazatelná.

Nechť PA značí teorii Peanovy aritmetiky a $\mathcal{N}$ značí realizaci $(\mathbb{N}_0, +, \cdot)$ jazyka aritmetiky.

Věta 2.4.4 (1. věta o neúplnosti). *Lze sestavit uzavřenou formuli ϱ , která je pravdivá v $\mathbb{N}$, ale není dokazatelná v PA .*

Nechť $CONSIS$ je formule vyjadřující bezespornost PA

Věta 2.4.5 (2. věta o neúplnosti). *Je-li PA bezesporná, pak $CONSIS$ není v PA dokazatelná. Zejména v „dostatečně silné teorii“ lze dokázat vlastní bezespornost jen v případě, že je tato teorie sporná.*

Poznámka. Význam Gödelových vět je zhruba ten, že neexistuje teorie T mající následující vlastnosti:

- T je bezesporná
- T je úplná
- T má rekurzivně spočetnou množinu axiomů
- v T lze zakódovat aritmetiku nezáporných celých čísel se sčítáním a násobením

Kapitola 3

Základní algebraické struktury

3.1 Grupy, okruhy, obory integrity, tělesa

Definice 3.1.1. Množina G spolu s operací $\cdot : G \times G \rightarrow G$ se nazývá *grupa*, jestliže

1. operace $\cdot$ je asociativní,
2. $\exists e \in G \forall g \in G (g \cdot e = e \cdot g = g)$, prvek e značíme 1 a nazýváme ho *neutrálním* prvkem,
3. $\forall g \in G \exists h \in G (g \cdot h = h \cdot g = 1)$, prvek h značíme g^{-1} a nazýváme ho inverzním prvkem k prvku g .

Je-li operace $\cdot$ komutativní, řekneme, že grupa G je komutativní.

Definice 3.1.2. Necht $(G, \cdot)$ je grupa. Existuje-li přirozené číslo n tak, že $a^n = 1$, pak nejmenší přirozené číslo n s touto vlastností se nazývá *řád prvku a* v grupě G . Neexistuje-li žádné přirozené číslo s touto vlastností, řekneme, že řád prvku a v grupě G je ∞ .

Věta 3.1.3. Necht $(G, \cdot)$ je grupa, $a \in G$. Je-li řád a v grupě G přirozené číslo n , pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \Leftrightarrow k \equiv l \pmod{n}.$$

Je-li naopak řád a roven ∞ , pak pro libovolná $k, l \in \mathbb{Z}$ platí

$$a^k = a^l \Leftrightarrow k = l.$$

Definice 3.1.4. Necht G je konečná grupa. Nejmenší $e \in \mathbb{N}$ takové, že pro každé $a \in G$ platí $a^e = 1$, se nazývá *exponent* grupy G .

Věta 3.1.5. Necht G je konečná komutativní grupa, pak exponent grupy G je roven největšímu z řádů všech prvků grupy G .

Definice 3.1.6. Necht G je grupa, H podmnožina G . Řekneme, že H je *podgrupa* grupy G , píšeme $H \leq G$, jestliže

1. $1 \in H$,
2. $\forall a \in H$ platí $a^{-1} \in H$,
3. $\forall a, b \in H$ platí $a \cdot b \in H$.

Definice 3.1.7. Grupa G se nazývá *cyklická*, jestliže existuje $a \in G$ takové, že $G = \langle a \rangle$. Řádem konečné grupy rozumíme počet prvků této grupy, značíme $|G|$.

Definice 3.1.8. Necht G, H jsou grupy. Zobrazení $f: G \rightarrow H$ se nazývá *homomorfismus* grupy G do grupy H , jestliže pro každé $a, b \in G$ platí $f(a \cdot_G b) = f(a) \cdot_H f(b)$. Injektivní homomorfismus se nazývá *vnoření*, bijektivní homomorfismus se nazývá *izomorfismus*. Množina $\ker f = \{a \in G \mid f(a) = 1_H\}$ se nazývá *jádro homomorfismu* f .

Věta 3.1.9. *Jádro homomorfismu je triviální právě tehdy, když je homomorfismus vnoření.*

Definice 3.1.10. Necht G je grupa, H její podgrupa. Pro libovolný prvek $a \in G$ definujeme jím určenou *levou třídu* $a \cdot H$ rozkladu grupy G podle podgrupy H předpisem $a \cdot H = \{a \cdot h \mid h \in H\}$.

Věta 3.1.11. *Množina G/H všech levých tříd grupy G podle podgrupy H tvoří rozklad na množině G .*

Definice 3.1.12. Počet $|G/H|$ levých tříd grupy G podle podgrupy H se nazývá *index* podgrupy H v grupě G .

Věta 3.1.13. *Necht G je konečná grupa, H její podgrupa, pak platí*

$$|G| = |G/H| \cdot |H|.$$

Důsledek 3.1.14. *Necht G je konečná grupa, H její podgrupa, pak*

1. *řád podgrupy dělí řád grupy (Lagrangeova věta),*
2. *řád prvku dělí řád grupy,*
3. *grupa prvočíselného řádu je cyklická,*
4. *exponent grupy dělí řád grupy,*
5. *$a^{\varphi(m)} \cong 1 \pmod{m}$ pro $m \in \mathbb{N}$, $a \in \mathbb{Z}$ libovolná nesoudělná,*

Definice 3.1.15. Buď G grupa, H její podgrupa. Řekneme, že H je *normální podgrupou* grupy G , jestliže $\forall h \in H$ a $\forall g \in G$ platí $ghg^{-1} \in H$.

To umožňuje zavést strukturu grupy na levých třídách rozkladu podle normální podgrupy.

Věta 3.1.16. *Normální podgrupy grupy G jsou právě jádra homomorfismů vedoucích z G .*

Věta 3.1.17. *Necht $f: G \rightarrow K$ je homomorfismus grup, H normální grupa taková, že $H \subseteq \ker f$. Necht $\pi: G \rightarrow G/H$ je projekce na faktorgrupu. Pak existuje jediné zobrazení $g: G/H \rightarrow K$ takové, že $g \circ \pi = f$. Navíc platí*

1. *g je homomorfismus grup,*
2. *g je injekce právě tehdy, když $H = \ker f$,*
3. *g je surjekce právě tehdy, když f je surjekce.*

Věta 3.1.18. *Necht G je konečná komutativní grupa, $|G| > 1$. Pak existují (ne nutně různá) prvočísla $p_1, \dots, p_s$ a $k_1, \dots, k_s \in \mathbb{N}$ tak, že*

$$G \cong \left(\mathbb{Z}_{p_1^{k_1}}, + \right) \times \dots \times \left(\mathbb{Z}_{p_s^{k_s}}, + \right).$$

Tento rozklad je dán jednoznačně až na pořadí činitelů.

Definice 3.1.19. Množna R spolu s dvěma operacemi $+$ a $\cdot$ se nazývá *okruh*, jestliže platí

1. $(R, +)$ je komutativní grupa,
2. $(R, \cdot)$ je monoid,
3. platí distributivní zákony: $\forall a, b, c \in R$ platí $a(b + c) = ab + ac$, $(a + b)c = ac + bc$.

Řekneme, že okruh R je komutativní, jestliže je monoid $(R, \cdot)$ komutativní.

Neutrální prvek grupy $(R, +)$ značíme 0 a nazýváme *nulou* okruhu R . Neutrální prvek monoidu $(R, \cdot)$ značíme 1 a nazýváme *jedničkou* okruhu R . Inverzní prvek k prvku a vůči sčítání se nazývá prvek opačný, značíme $-a$. Množinu nenulových prvků značíme R^* .

Definice 3.1.20. Prvky a, b okruhu R se nazývají *dělitelé nuly*, jestliže $a \neq 0 \neq b$, ale $ab = 0$. Netriviální komutativní okruh R se nazývá *obor integrity*, jestliže nemá dělitele nuly.

Věta 3.1.21. Netriviální komutativní okruh R je obor integrity právě tehdy, když v něm platí zákon o krácení, tj. $\forall a, b, c \in R$, kde $a \neq 0$ platí $ab = ac \Rightarrow b = c$.

Definice 3.1.22. Buď R okruh. Invertibilní prvek monoidu $(R, \cdot)$ se nazývá *jednotka* okruhu R . Množinu všech jednotek značíme $R^\times$.

Netriviální komutativní okruh se nazývá *těleso*, jestliže $R^* = R^\times$.

Věta 3.1.23. Každé těleso je oborem integrity. Každý konečný obor integrity je tělesem.

Definice 3.1.24. Buď R okruh. Přirozené číslo n takové, že $n1 = 0$, nazýváme *charakteristika* okruhu R . Pokud takové n neexistuje, řekneme, že charakteristika okruhu je nula.

Věta 3.1.25. Je-li R obor integrity, pak je jeho charakteristika buď R nebo nula. Pro $a \neq 0$ platí

- je-li charakteristika R nula, pak $\forall k \in \mathbb{N}$ platí $ka \neq 0$,
- je-li charakteristika R prvočíslo p , pak řád prvku a v grupě $(R, +)$ je p ,

zejména všechny nenulové prvky mají v grupě $(R, +)$ stejný řád.

Důsledek 3.1.26. Je-li R konečné těleso charakteristiky p , pak grupa $(R, +)$ je izomorfní s grupou $(\mathbb{Z}_p, +) \times \cdots \times (\mathbb{Z}_p, +)$. Počet prvků konečného tělesa je tedy mocninou jeho prvočíselné charakteristiky.

Definice 3.1.27. Necht R, S jsou okruhy, zobrazení $f: R \rightarrow S$ se nazývá *homomorfismus* okruhu R do okruhu S , jestliže

1. $\forall a, b \in R$ platí $f(a + b) = f(a) + f(b)$,
2. $\forall a, b \in R$ platí $f(a \cdot b) = f(a) \cdot f(b)$,
3. $f(1) = 1$.

Množina $\ker f = \{a \in R \mid f(a) = 0\}$ se nazývá *jádro homomorfismu* f .

Definice 3.1.28. Necht R je okruh. Neprázdnou množinu $I \subseteq R$ nazveme *ideálem* okruhu R , jestliže

1. $\forall a, b \in I$ platí $a + b \in I$,
2. $\forall r \in R$ a $\forall a \in I$ platí $ra \in I$ a též $ar \in I$.

Řekneme, že ideál I je hlavní, jestliže je generovaný jediným prvkem.

Řekneme, že ideál $I \neq R$ je prvoideál, jestliže $\forall r, s \in R$ platí $rs \in I \Rightarrow (r \in I \vee s \in I)$.

Řekneme, že ideál $I \neq R$ je maximální, jestliže neexistuje ideál J takový, že $I \subset J \neq R$.

Věta 3.1.29. Buď R okruh. Ideály okruhu R jsou právě jádra homomorfismů vedoucích z R .

3.2 Homomorfismy a faktorizace v teorii grup a okruhů

Definice 3.2.1. Buď G grupa, H její normální podgrupa. Na rozkladu G/H grupy G na levé třídy podle normální podgrupy H definujeme operaci $\star$ pomocí reprezentantů následujícím předpisem

$$(a \cdot H) \star (b \cdot H) = (a \cdot b) \cdot H.$$

Poznámka. Víme, že následující podmínky jsou ekvivalentní

- $a \cdot H = b \cdot H$,
- $a \in b \cdot H$,
- $b^{-1}a \in H$.

Chceme dokázat, že nezávisí na volbě reprezentantů. Předpokládejme, že $a \cdot H = a' \cdot H$, $b \cdot H = b' \cdot H$, tj. $a' = ah_1$, $b' = ah_2$. Pak

$$(ah_1)(bh_2) \cdot H = ab \cdot H$$

právě tehdy, když $b^{-1}a^{-1}ah_1bh_2 = b^{-1}h_1bh_2 \in H$, což jistě platí, vždyť $h_1, h_2 \in H$, kde H je normální podgrupa grupy G .

Definice 3.2.2. Buď R okruh, I jeho ideál. Protože I je podgrupa komutativní grupy $(R, +)$, můžeme uvážit faktogrupu R/I . Na této faktorgrupě definujeme strukturu okruhu pomocí reprezentantů následujícím předpisem

$$\begin{aligned} (a + I) + (b + I) &= (a + b) + I, \\ (a + I) \cdot (b + I) &= ab + I. \end{aligned}$$

Věta 3.2.3. *Nechť R je netriviální komutativní okruh, I jeho ideál. Pak platí*

1. *I je prvoideál právě tehdy, když R/I je obor integrity,*
2. *I je maximální ideál právě tehdy, když R/I je těleso.*

Zejména každý maximální ideál je prvoideál.

3.3 Vektorové prostory

Definice 3.3.1. Nechť $(V, +)$ je komutativní grupa (jejíž prvky nazýváme *vektory*) a $(T, \boxplus, \star)$ číselné těleso (jeho prvky nazýváme *skaláry*). Řekneme, že grupa V spolu s operací $\cdot : T \times V \rightarrow V$ tvoří *vektorový prostor* $(V, +, \cdot)$ nad tělesem T , jestliže

1. $t \cdot (\mathbf{u} + \mathbf{v}) = t \cdot \mathbf{u} + t \cdot \mathbf{v}$,
2. $(t \boxplus s) \cdot \mathbf{u} = t \cdot \mathbf{u} + s \cdot \mathbf{u}$,
3. $(t \star s) \cdot \mathbf{u} = t \cdot (s \cdot \mathbf{u})$,
4. $1 \cdot \mathbf{u} = \mathbf{u}$.

Neutrální prvek grupy $(V, +)$ se nazývá *nulový vektor* a označuje se symbolem $\mathbf{o}$. Inverzní prvek k vektoru $\mathbf{v}$ se nazývá *opačný vektor* k vektoru $\mathbf{v}$ a označuje se symbolem $-\mathbf{v}$.

Definice 3.3.2. Necht V je vektorový podprostor nad tělesem T . Neprázdná množina U množiny V se nazývá *podprostor* vektorového prostoru V , jestliže platí:

1. $\mathbf{u}, \mathbf{v} \in U \Rightarrow \mathbf{u} + \mathbf{v} \in U$,
2. $t \in T, \mathbf{u} \in U \Rightarrow t \cdot \mathbf{u} \in U$.

Definice 3.3.3. Buď $\emptyset \neq X \subseteq V$ množina vektorů. *Lineárním obalem* množiny X (píšeme $[X]$) rozumíme množinu všech lineárních kombinací vektorů z X , tj.

$$[X] = \{a_1\mathbf{x}_1 + a_2\mathbf{x}_2 + \dots + a_n\mathbf{x}_n \mid n \in \mathbb{N}, a_1, a_2, \dots, a_n \in K, \mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n \in X\}.$$

Pro $X = \emptyset$ definujeme $[X] = \{\mathbf{o}\}$.

Věta 3.3.4. Buď $X \subseteq V$. $[X]$ je nejmenší lineární podprostor vektorového prostoru V obsahující X .

Definice 3.3.5. Buď V vektorový prostor. Vektory $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in V$ se nazývají *lineárně nezávislé*, jestliže $\forall a_1, a_2, \dots, a_n \in T$ platí

$$a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n = \mathbf{o} \quad \Rightarrow \quad a_1 = a_2 = \dots = a_n = 0.$$

V opačném případě řekneme, že vektory $\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n$ jsou *lineárně závislé*.

Věta 3.3.6 (Steinitzova věta o výměně). Buď V vektorový prostor. Necht $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m \in V$. Jsou-li vektory $\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n$ lineárně nezávislé a všechny patří do lineárního obalu $[\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_m]$, pak $n \leq m$.

Definice 3.3.7. Množina $M \subseteq V$ se nazývá *báze* vektorového prostoru V , jestliže platí jedno z následujících (ekvivalentních) tvrzení:

- M je maximální množina lineárně nezávislých vektorů
- M je minimální množina generátorů vektorového prostoru V

Buď dále $\mathbf{v}$ libovolný vektor. Pak existují $a_1, a_2, \dots, a_n \in T, \mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n \in M$ tak, že $\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n$. Čísla $a_1, a_2, \dots, a_n$ nazýváme *souřadnice vektoru $\mathbf{v}$ v bázi M* .

Poznámka. Buď $\alpha = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ báze vektorového prostoru V . Libovolný vektor $\mathbf{v} \in V$ lze vyjádřit jako $\mathbf{v} = a_1\mathbf{v}_1 + a_2\mathbf{v}_2 + \dots + a_n\mathbf{v}_n$. Symbolem $(\mathbf{v})_\alpha = (a_1, a_2, \dots, a_n)$ značíme jeho souřadnice v bázi α .

V prostoru $\mathbb{R}^n$ značíme $\epsilon = \{(1, 0, \dots, 0)^T, (0, 1, \dots, 0)^T, \dots, (0, 0, \dots, 1)^T\}$ tzv. *kanonickou bázi*.

Definice 3.3.8. Necht $\alpha = \{\mathbf{u}_1, \mathbf{u}_2, \dots, \mathbf{u}_n\}, \beta = \{\mathbf{v}_1, \mathbf{v}_2, \dots, \mathbf{v}_n\}$ jsou báze vektorového prostoru V . Pak $\forall j: 1 \leq j \leq n$ lze vektor $\mathbf{u}_j$ vyjádřit jako

$$\mathbf{u}_j = \sum_{i=1}^n a_{ij}\mathbf{v}_i$$

pro vhodná a_{ij} . Matici $(id)_{\beta, \alpha} = (a_{ij})_{i,j}$ nazýváme *maticí přechodu* od báze α k bázi β .

Věta 3.3.9. Buďte α, β, γ báze vektorového prostoru $V, \mathbf{v} \in V$ libovolný vektor. Pak platí:

- $(\mathbf{v})_\beta = (id)_{\beta, \alpha} (\mathbf{v})_\alpha$,

- $(id)_{\gamma,\beta} \cdot (id)_{\beta,\alpha} = (id)_{\gamma,\alpha}$.

Definice 3.3.10. Popis podprostoru Q výčtem jeho bázových vektorů nazýváme *parametrický popis* podprostoru Q .

Podmnožina $P \subseteq V$ vektorů splňujících homogenní soustavu nerovnic $Ax = 0$, kde $A \in Mat_{n \times m}(T)$, $\dim V = m$ tvoří vektorový podprostor. Naopak pro libovolný vektorový podprostor lze taková soustava nalézt. Je-li vektorový prostor zadán soustavou $Ax = 0$, nazveme tento popis *analytický*.

Poznámka. Buďte P, Q vektorové podprostory. Pak $P \cap Q$ tvoří vektorový podprostor, $P \cup Q$ již vektorový podprostor tvořit nemusí.

Definice 3.3.11. Průnikem vektorových podprostorů P, Q rozumíme vektorový podprostor $P \cap Q$.

Součtem vektorových podprostorů P, Q rozumíme vektorový podprostor $P + Q = [P \cup Q]$.

Definice 3.3.12. Buďte U, V vektorové prostory nad tělesem T . Zobrazení $f: U \rightarrow V$ se nazývá *lineární zobrazení*, jestliže

- $f(\mathbf{u}) + f(\mathbf{v}) = f(\mathbf{u} + \mathbf{v})$ pro všechna $\mathbf{u}, \mathbf{v} \in U$,
- $af(\mathbf{u}) = f(a\mathbf{u})$ pro všechna $a \in T, \mathbf{u} \in U$.

Injektivní lineární zobrazení nazýváme *vnoření*. Bijektivní lineární zobrazení nazýváme *izomorfismus*. Pokud mezi prostory U a V existuje alespoň jeden izomorfismus, řekneme, že U a V jsou izomorfní (píšeme $U \cong V$).

Věta 3.3.13. Všechny vektorové prostory stejné dimenze nad pevně zvoleným tělesem jsou vzájemně izomorfní.

Důsledek 3.3.14. Nechť V je vektorový prostor nad tělesem T a $\dim V = n$. Pak $V \cong T^n$.

Definice 3.3.15. Buď $f: U \rightarrow V$ lineární zobrazení. Jádrem zobrazení f rozumíme množinu

$$\ker f = \{\mathbf{u} \in U \mid f(\mathbf{u}) = \mathbf{0}\}.$$

Obrazem zobrazení f rozumíme množinu

$$\operatorname{im} f = \{\mathbf{v} \in V \mid \exists \mathbf{u} \in U: f(\mathbf{u}) = \mathbf{v}\}.$$

Věta 3.3.16. Buď $f: U \rightarrow V$ lineární zobrazení. Pak $\ker f$ tvoří vektorový podprostor U a $\operatorname{im} f$ tvoří vektorový podprostor V . Navíc platí $\dim \ker f + \dim \operatorname{im} f = \dim U$.

Definice 3.3.17. Maticí lineárního zobrazení $f: U \rightarrow V$ vzhledem k bázím $\alpha = \{\mathbf{u}_1, \dots, \mathbf{u}_n\} \subseteq U$ a $\beta = \{\mathbf{v}_1, \dots, \mathbf{v}_m\} \subseteq V$ rozumíme matici

$$(f)_{\beta,\alpha} = (f(\mathbf{u}_1)_\beta, \dots, f(\mathbf{u}_n)_\beta) \in Mat_{m \times n}.$$

Věta 3.3.18. Buď $f: U \rightarrow V$ lineární zobrazení vzhledem k bázím α, β . Pak $\forall \mathbf{u} \in U$ platí:

$$(f(\mathbf{u}))_\beta = (f)_{\beta,\alpha}(\mathbf{u})_\alpha$$

přičemž $(f)_{\beta,\alpha}$ je jediná matice s touto vlastností.

Kapitola 4

Svazy a univerzální algebra

4.1 Modulární, distributivní a úplné svazy

Definice 4.1.1. *Svazem* rozumíme uspořádanou množinu $(G, \leq)$ v níž mají každé dva prvky $a, b \in G$ své infimum $a \wedge b$ a své supremum $a \vee b$.

Příklad. Pro libovolnou množinu X je $(2^X, \subseteq)$ svaz, kde infimum je průnik množin a supremum jejich sjednocení.

$(\mathbb{N}, |)$ je svaz, kde infimum je největší společný dělitel a supremem nejmenší společný násobek.

Poznámka. $a \vee b = a \Leftrightarrow a \geq b \Leftrightarrow a \wedge b = b$.

V každém svazu platí

- $\vee, \wedge$ jsou idempotentní, tj. $\forall a \in G$ platí $a \wedge a = a \vee a = a$,
- $\vee, \wedge$ jsou komutativní,
- $\vee, \wedge$ jsou asociativní,
- $\vee, \wedge$ jsou svázány absorpčními zákony: $\forall a, b \in G$ platí

$$(a \vee b) \wedge a = a, \quad (a \wedge b) \vee a = a$$

Věta 4.1.2. *Nechť $(G, \vee, \wedge)$ je množina se dvěma idempotentními, asociativními, komutativními operacemi, které jsou svázány absorpčními zákony. Pak*

1. *pro každé $a, b \in G$ platí $a \wedge b = a \Leftrightarrow a \vee b = b$,*
2. *definujeme na G relaci $\leq$ takto: pro libovolné $a, b \in G$ klademe*

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

pak je $\leq$ uspořádání na G takové, že $(G, \leq)$ je svaz v němž pro libovolné prvky $a, b \in G$ je prvek $a \vee b$ jejich supremum a $a \wedge b$ jejich infimum.

Věta 4.1.3. *V libovolném svazu G platí pro každou trojici $a, b, c \in G$ tzv. distributivní nerovnosti*

$$\begin{aligned} (a \vee b) \wedge (a \vee c) &\geq a \vee (b \wedge c), \\ (a \wedge b) \vee (a \wedge c) &\geq a \wedge (b \vee c). \end{aligned}$$

Je-li navíc $c \leq a$, platí tzv. modulární nerovnost

$$(a \wedge b) \vee c \leq a \wedge (b \vee c).$$

Definice 4.1.4. Necht G je svaz. Podmnožina $A \subseteq G$ se nazývá

- *podsvaz* svazu G , jestliže platí

$$\forall a, b \in A: a \vee b \in A, \quad a \wedge b \in A,$$

- *ideál* svazu G , jestliže je podsvazem a platí

$$\forall a \in A \forall g \in G: g \leq a \Rightarrow g \in A,$$

ideál je tedy dolů dědičný podsvaz,

- *filtr* svazu G , jestliže je podsvazem a splňuje

$$\forall a \in A \forall g \in G: g \geq a \Rightarrow g \in A,$$

filtr je tedy nahoru dědičný podsvaz.

Definice 4.1.5. Necht G, S jsou svazy. Řekneme, že zobrazení $f: G \rightarrow S$ je *homomorfismem svazů*, jestliže

$$\begin{aligned} f(a \vee b) &= f(a) \vee f(b), \\ f(a \wedge b) &= f(a) \wedge f(b). \end{aligned}$$

Je-li f bijekce a současně homomorfismus svazů, nazývá se *izomorfismem svazů*.

Definice 4.1.6. Necht $(M, \leq)$, $(N, \preceq)$ jsou uspořádané množiny. Zobrazení $f: M \rightarrow N$ se nazývá *izotonní*, jestliže $\forall a, b \in M \ a \leq b \Rightarrow f(a) \preceq f(b)$. Je-li f bijekce a platí-li, že f i f^{-1} jsou obě izotonní, nazývá se f *izomorfismem uspořádaných množin*.

Poznámka. Porovnejme nyní zavedené pojmy homomorfismů.

- Každý homomorfismus svazů je izotonní.

$$a \leq b \Leftrightarrow a \wedge b = a \Rightarrow f(a) = f(a \wedge b) = f(a) \wedge f(b) \Leftrightarrow f(a) \leq f(b).$$

- Ne každé izotonní zobrazení mezi svazy je homomorfismus
Uvažme svazy $G = (\{1, 2, 3, 6\}, |)$, $S = (\{1, 2, 3, 4\}, \leq)$ a zobrazení $f: G \rightarrow S$ dané předpisem

$$f(1) = 1, f(2) = 2, f(3) = 3, f(6) = 4,$$

pak f je izotonní, ale není homomorfismus svazů.

- Inverzní zobrazení k izomorfismu svazů je izomorfismus svazů.

$$\begin{aligned} x, y \in S, \quad x &= f(a), \quad y = f(b), \\ f^{-1}(x \wedge y) &= f^{-1}(f(a) \wedge f(b)) = f^{-1}(f(a \wedge b)) = a \wedge b = f^{-1}(x) \wedge f^{-1}(y). \end{aligned}$$

- Každý izomorfismus svazů je izomorfismem uspořádaných množin.

- Každý izomorfismus uspořádaných množin mezi dvěma svazy je izomorfismus svazů.

Definice 4.1.7. Svaz G se nazývá

- *úplný*, jestliže zde má každá podmnožina své infimum a supremum,
- *modulární*, jestliže pro libovolné $a, b, c \in G$ takové, že $c \leq a$ platí

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

- *distributivní*, jestliže pro každé $a, b, c \in G$ platí

$$(a \vee b) \wedge (a \vee c) = a \vee (b \wedge c)$$

Věta 4.1.8. *Nechť G je svaz. Následující podmínky jsou ekvivalentní.*

- G je úplný svaz,
- G má nejmenší prvek a každá neprázdná podmnožina množiny G má v G supremum, tj. každá podmnožina má supremum,
- G má největší prvek a každá neprázdná podmnožina množiny G má v G infimum, tj. každá podmnožina má infimum.

Věta 4.1.9 (Tarski). *Nechť G je úplný svaz a $f: G \rightarrow G$ izotonní zobrazení. Pak $\exists a \in G$ $f(a) = a$.*

Důkaz. Označme $A = \{x \in G \mid x \leq f(x)\}$, $a = \sup A$. Jistě je A neprázdná, vždyť G má nejmenší prvek, který jistě leží v A . Navíc pro každé $b \in A$ platí, že $b \leq f(b)$, a z protože je f izotonní, je i $f(b) \leq f(f(b))$, zejména tedy $f(b) \in A$. Přitom pro každé $b \in A$ je $b \leq a$, tedy $b \leq f(b) \leq f(a)$. Proto $f(a)$ je horní závora A , přitom a je nejmenší horní závora, nutně $a \leq f(a)$, tedy $a \in A$. Proto též $f(a) \geq a \in A$, což dává $a = f(a)$.

Věta 4.1.10. *Buď H grupa. Označme $\mathcal{N}$ množinu všech normálních podgrup grupy H . Pak $(\mathcal{N}, \subseteq)$ je úplná svaz, který je modulární.*

Věta 4.1.11. *Nechť G je svaz. Následující podmínky jsou ekvivalentní*

1. G je modulární,
2. pro každé $a, b, c \in G$ platí $(a \wedge b) \vee (a \wedge c) = a \wedge (b \vee (a \wedge c))$,
3. pokud pro $a, b, c \in G$ platí $c \leq a$, $c \vee b = a \vee b$, $c \wedge b = a \wedge b$, pak $a = c$,
4. G neobsahuje podsvaz izomorfní s pětiúhelníkem (tj. svazem N_5).

Důsledek 4.1.12. *Nechť G je modulární svaz, $f: G \rightarrow S$ homomorfismus svazů.*

- Součin modulárních svazů je modulární.
- $f(G)$ je modulární
- Systém vektorových prostorů vektorového podprostoru uspořádaný inkluzí je modulární svaz.

Věta 4.1.13. *Nechť G je svaz. Následující podmínky jsou ekvivalentní.*

1. G je distributivní,
2. pokud pro $a, b, c \in G$ platí $a \vee b = c \vee b$, $a \wedge b = c \wedge b$, pak $a = c$,
3. G neobsahuje podsvaz izomorfní pětiúhelníku či diamantu (tj. svazu N_5 nebo M_5).

Věta 4.1.14. Nechť G je distributivní svaz, $f: G \rightarrow S$ homomorfismus svazů.

- Součin distributivních svazů je distributivní.
- $f(G)$ je distributivní.
- G je modulární
- Je-li G konečný, pak je izomorfní s vhodným podsvazem svazu všech podmnožin nějaké konečné množiny.

4.2 Booleovy algebry

Definice 4.2.1. Nechť G je svaz

- Nechť G má nejmenší prvek, značíme 0 , a největší prvek, značíme 1 . Nechť $a \in G$. Prvek $b \in G$ nazveme *komplementem prvku a* , jestliže

$$a \wedge b = 0, \quad a \vee b = 1.$$

- G se nazývá *komplementární*, jestliže má nejmenší a největší prvek a každý jeho prvek má komplement.
- *Booleovou algebrou* rozumíme komplementární distributivní svaz.

Poznámka. V distributivních svazích je komplement prvku a (pokud existuje) určen jednoznačně. Budeme jej značit a' .

Příklad. Pro libovolnou množinu X je $(2^X, \subseteq)$ Booleova algebra.

Věta 4.2.2. Nechť B je Booleova algebra. Pak platí

- $0' = 1, 1' = 0$,
- $a'' = a$,
- $(a \vee b)' = a' \wedge b'$,
- $(a \wedge b)' = a' \vee b'$.

Definice 4.2.3. Podstav L Booleovy algebry B se nazývá *Booleova podalgebra*, jestliže $0, 1 \in L$ a pro každé $a \in L$ je též $a' \in L$.

Definice 4.2.4. Nechť B, G jsou Booleovy algebry. Zobrazení $f: B \rightarrow G$ nazveme *homomorfismem Booleových algeber*, jestliže f je homomorfismus svazů splňující $f(0) = 0$ a $f(1) = 1$.

Definice 4.2.5. Okruh $(R, +, \cdot)$ se nazývá *Booleovým okruhem*, jestliže je idempotentní, tj. $\forall x \in R \ x \cdot x = x$.

Věta 4.2.6. Netriviální Booleův okruh je komutativní charakteristiky 2.

Věta 4.2.7. Necht B je booleova algebra. Definujme na B operace $+$, $\cdot$ takto:

$$x + y = (x \wedge y') \vee (x' \wedge y), \quad x \cdot y = x \wedge y,$$

Pak $(B, +, \cdot)$ je Booleův okruh.

Věta 4.2.8. Necht $(R, +, \cdot)$ je Booleův okruh. Definujme na R operace $\vee$ a $\wedge$ takto:

$$x \vee y = x \cdot y + x + y, \quad x \wedge y = x \cdot y.$$

Pak $(R, \vee, \wedge)$ je Booleova algebra, kde pro každé $x \in R$ platí $x' = x + 1$.

4.3 Variety algeber a Birkhoffova věta

Definice 4.3.1. Necht G je množina, $n \in \mathbb{N}_0$, n -ární operací na množině G rozumíme libovolné zobrazení $G^n \rightarrow G$ (přitom $G^0 = \{\emptyset\}$).

Definice 4.3.2. Typem rozumíme libovolnou množinu Ω spolu se zobrazením $a: \Omega \rightarrow \mathbb{N}_0$, kterému říkáme *arita*. Prvky $f \in \Omega$ nazýváme *operační symboly*, číslu $a(f)$ říkáme *arita operačního symbolu* f .

Definice 4.3.3. Necht Ω je typ. Univerzální algebrou typu Ω (též Ω -algebrou) rozumíme množinu A spolu se zvolenou n -ární operací $f_A: A^n \rightarrow A$ pro každý operační symbol $f \in \Omega$ arity n .

Definice 4.3.4. Necht A je Ω -algebra. Podmnožinu $B \subseteq A$ nazýváme *podalgebrou* Ω -algebry A , jestliže pro každý n -ární $f \in \Omega$ a každé $b_1, \dots, b_n \in B$ platí $f_A(b_1, \dots, b_n) \in B$. Tedy B je uzavřená na všechny operace $f \in \Omega$.

Věta 4.3.5. Průnik podalgeber je podalgebra.

Definice 4.3.6. Necht A je Ω -algebra. $M \subseteq A$ je libovolná podmnožina. Pak *podalgebrou generovanou podmnožinou* M , značíme $\langle M \rangle$, rozumíme průnik všech podalgeber Ω -algebry A obsahující M jako svou podmnožinu.

Definice 4.3.7. Necht Ω je typ a A, B jsou Ω -algebry a $\varphi: A \rightarrow B$ je zobrazení. Řekneme, že φ je *homomorfismus* Ω -algeber, jestliže pro každý n -ární operační symbol $f \in \Omega$ a každé $a_1, \dots, a_n \in A$ platí

$$\varphi(f_A(a_1, \dots, a_n)) = f_B(\varphi(a_1), \dots, \varphi(a_n)).$$

Injektivní homomorfismus se nazývá *vnoreň*, bijektivní homomorfismus *izomorfismus* Ω -algeber.

Definice 4.3.8. Necht Ω je typ. A je Ω -algebra. Necht $\sim$ je relace ekvivalence na množině A . Řekneme, že relace $\sim$ je *kongruence*, jestliže $\forall f \in \Omega$, f je n -ární, a $\forall a_1, \dots, a_n \in A$ platí

$$a_1 \sim b_1, \dots, a_n \sim b_n \Rightarrow f_A(a_1, \dots, a_n) \sim f_A(b_1, \dots, b_n).$$

Věta 4.3.9. Necht $\varphi: A \rightarrow B$ je homomorfismus Ω -algeber. Definujme na nosné množině Ω -algebry A relaci $\sim$ takto:

$$\forall a_1, a_2 \in A (a_1 \sim a_2 \Leftrightarrow \varphi(a_1) = \varphi(a_2))$$

Pro $\sim$ je kongruence na Ω -algebře A .

Definice 4.3.10. Kongruence z předchozí věty se nazývá *jádro homomorfismu* φ .

Definice 4.3.11. Necht $\sim$ je kongruence na Ω -algebře A . Definujme na rozkladu $A/\sim$ množiny A podle kongruence $\sim$ pro každý n -ární $f \in \Omega$ operaci $f_{A/\sim}$ pomocí reprezentantů. Množina $A/\sim$ spolu s takto definovanými operacemi tvoří opět Ω -algebru, kterou nazýváme *faktoralgebrou*.

Věta 4.3.12. Necht A je Ω -algebra, $\sim$ je relace ekvivalence na A . Následující podmínky jsou ekvivalentní

1. $\sim$ je kongruence,
2. $\sim$ je jádro nějakého homomorfismu $f: A \rightarrow B$ pro vhodnou Ω -algebru B ,
3. $\sim$ je podalgebra součinu $A \times A$.

Definice 4.3.13. Necht Ω je typ. Označme $\Omega_0 = \{f \in \Omega \mid f \text{ je nulární}\}$. Položme $M_0 = \Omega_0 \cup \{x_1, x_2, \dots\}$. Pro každé $n \in \mathbb{N}$ položme

$$M_n = \{f(t_1, \dots, t_k) \mid f \in \Omega, f \text{ } k\text{-ární}, t_1, \dots, t_k \in M_{n-1}\} \cup Mn - 1.$$

Množina

$$F(\Omega) = \bigcup_{n=0}^{\infty} M_n$$

se nazývá *množina všech termů typu Ω* .

Pro libovolné $m \in \mathbb{N}_0$ označme

$$F_m(\Omega) = \{t \in F(\Omega) \mid \text{v } t \text{ se nevyskytuje } x_r \text{ pro } r > m\}.$$

Prvkům F_m říkáme *m -ární termy typu Ω* .

Definice 4.3.14. Necht Ω je typ, $t \in F_m(\Omega)$ pro $m \in \mathbb{N}_0$. Pro libovolnou Ω -algebru A definujeme n -ární operaci $t_A: A^n \rightarrow A$ takto:

- je-li $t = x_k$, pak $k \leq m$ a klademe

$$t_A(a_1, \dots, a_m) = a_k,$$

- je-li $t = f \in \Omega_0$, pak

$$t_A(a_1, \dots, a_m) = f_A,$$

- je-li $t = f(t_1, \dots, t_k)$, kde $f \in \Omega$, f je k -ární, $t_1, \dots, t_k \in F_m(\Omega)$, pak

$$t_A(a_1, \dots, a_m) = f_A((t_1)_A(a_1, \dots, a_m), \dots, (t_k)_A(a_1, \dots, a_m))$$

pro libovolné $a_1, \dots, a_m \in A$.

Definice 4.3.15. Výraz $t_1 = t_2$, kde $t_1, t_2 \in F(\Omega)$ pro pevně zvolený typ Ω se nazývá *rovnost typu Ω* .

Definice 4.3.16. Necht A je Ω -algebra, $m \in \mathbb{N}_0$, $t_1, t_2 \in F_m(\Omega)$. Řekneme, že rovnost $t_1 = t_2$ platí v A , jestliže $(t_1)_A, (t_2)_A$ jsou stejné m -ární operace na A .

Příklad. Je-li $\Omega = \{\cdot\}$ binární, pak Ω -algebry jsou právě grupoidy.

Pologrupy jsou ty z nich, v nichž platí rovnost $x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3$.

Komutativní grupoidy jsou ty v nichž platí rovnost $x_1 \cdot x_2 = x_2 \cdot x_1$.

Definice 4.3.17. Necht Ω je typ. *Teorií* typu Ω rozumíme libovolnou množinu rovností typu Ω .

Definice 4.3.18. Necht T je teorie typu Ω . *Varietou* Ω -algeber určenou teorií T rozumíme třídu všech Ω -algeber, v nichž platí všechny rovnosti z teorie T .

Příklad. $\Omega = \{\cdot, {}^{-1}, 1\}$, kde $\cdot$ je *birární*, ${}^{-1}$ *unární* a 1 *nulární*. *Teorie*

$$T = \{x_1 \cdot (x_2 \cdot x_3) = (x_1 \cdot x_2) \cdot x_3, x_1 \cdot 1 = x_1, 1 \cdot x_1 = x_1, x_1^{-1} \cdot x_1 = 1, x_1 \cdot x_1^{-1} = 1\}$$

nám dá varietu všech grup.

Příklad. $\Omega = \emptyset$. *Teorie* $T = \{x_1 = x_2\}$ *zadává varietu všech nejvýše jednoprvkových množin.*

Definice 4.3.19. Necht V je třída Ω -algeber. Řekneme, že V je *uzavřená třída*, jestliže platí

1. $\forall A \in V$ leží ve V i všechny podalgebry A ,
2. pro každý surjektivní homomorfismus Ω -algeber $\varphi: A \rightarrow B$ platí, že $A \in V \Rightarrow B \in V$,
3. pro každou $I \neq \emptyset$ takovou, že $\forall i \in I$ je dána Ω -algebra $A_i \in V$ platí $\prod_{i \in I} A_i \in V$,
4. V obsahuje alespoň jednu jednoprvkovou Ω -algebru.

Věta 4.3.20 (Birkhoff). *Necht V je třída Ω -algeber, pak V je uzavřená právě tehdy, když V je varieta.*

Kapitola 5

Základy teorie kategorií

5.1 Definice a příklady kategorií, funktory a přirozené transformace

Definice 5.1.1. Kategorii $\mathcal{K}$ se skládá z třídy objektů $ob(\mathcal{K})$ a třídy morfismů $mor(\mathcal{K})$ tak, že

1. morfismy lze skládat a toto složení je asociativní, tj. pokud $f: A \rightarrow B$, $g: B \rightarrow C$ a $h: C \rightarrow D$, pak $(f \circ g) \circ h = f \circ (g \circ h): A \rightarrow D$.
2. pro každý objekt $A \in ob(\mathcal{K})$ existuje morfismus $id_A: A \rightarrow A$ takový, že pro libovolný morfismus $f: A \rightarrow B$ platí $f \circ id_A = id_B \circ f = f$.

$\mathcal{K}(A, B)$ značí třídu morfismů z objektu $A \in ob(\mathcal{K})$ do objektu $B \in ob(\mathcal{K})$.

Příklad.

<i>Kategorie</i>	<i>Objekty</i>	<i>Morfismy</i>
<i>Set</i>	<i>Množiny</i>	<i>zobrazení</i>
<i>Gp</i>	<i>Grupy</i>	<i>homomorfismy</i>
<i>Ab</i>	<i>Abelovské grupy</i>	<i>homomorfismy</i>
<i>PoSet</i>	<i>Uspořádané množiny</i>	<i>izotonní zobrazení</i>
<i>Metrické prostory</i>	<i>Metrické prostory</i>	<i>spojitá zobrazení</i>

Poznámka. Uvědomme si, že kategorie *Set* má jako objekty všechny množiny, nemá tedy množinu objektů, ale skutečně třídu. Může však nastat, že objektů bude pouze množina, nebo morfismů mezi libovolnými dvěma objekty bude pouze množina. Tyto případy jsou podstatné, a proto má smysl definovat následující pojmy.

Definice 5.1.2. Necht $\mathcal{K}$ je kategorie.

- Jestliže jsou $ob(\mathcal{K})$ a $mor(\mathcal{K})$ množiny, nazývá se kategorie $\mathcal{K}$ *malá*.
- Jestliže je $\mathcal{K}(A, B)$ pro libovolné dva objekty $A, B \in ob(\mathcal{K})$, nazývá se kategorie $\mathcal{K}$ *lokálně malá*.
- Jestliže pro všechna $A, B \in \mathcal{K}$ je $|\mathcal{K}[A, B]| \leq 1$, nazývá se kategorie $\mathcal{K}$ *tenká*.

Definice 5.1.3. Necht $\mathcal{K}$ je kategorie, $A, B \in ob(\mathcal{K})$ objekty. Morfismus $f: A \rightarrow B$ se nazývá *izomorfismus*, jestliže $g: B \rightarrow A$ takový, že $f \circ g = id_B$, $g \circ f = id_A$.

Definice 5.1.4. Pro libovolnou kategorii $\mathcal{K}$ můžeme definovat duální kategorii $\mathcal{K}^{op}$, pro kterou platí

1. $ob(\mathcal{K}) = ob(\mathcal{K}^{op})$,
2. pro libovolné $A, B \in ob(\mathcal{K})$ platí $\mathcal{K}(A, B) = \mathcal{K}^{op}(B, A)$.

Jedná se tedy o kategorii, kde otočíme všechny šípky.

Definice 5.1.5. Nechť $\mathcal{K}$ je kategorie.

- Objekt $I \in ob(\mathcal{K})$ se nazývá *iniciální*, jestliže pro libovolný objekt $A \in ob(\mathcal{K})$ existuje právě jeden morfismus $I \rightarrow A$.
- Objekt $T \in ob(\mathcal{K})$ se nazývá *terminální*, jestliže pro libovolný objekt $A \in ob(\mathcal{K})$ existuje právě jeden morfismus $A \rightarrow T$.

Věta 5.1.6 (Základní věta teorie kategorií). *Iniciální objekt je určen jednoznačně až na izomorfismus.*

Příklad.

Kategorie	Iniciální objekt	Terminální objekt
<i>Set</i>	$\emptyset$	jednoprvková množina
<i>Gp</i>	0	0
<i>Množiny a prostá zobrazení</i>	$\emptyset$	-

Příklad. • Uvažme kategorii $\mathcal{A}$ obsahující jediný objekt A . Tuto kategorii pak můžeme chápat jako monoid, jehož prvky jsou morfismy $\text{mor}(\mathcal{A})$. Neutrálním prvkem je id_A , operace je skládání morfismů, která je z definice kategorie asociativní.

- Vzpomeňme, že předuspořádání je reflexivní a tranzitivní relace. Nechť S je množina vybavená předuspořádáním $\leq$. Uvažme kategorii $\mathcal{K}$ takovou, že

$$\begin{aligned} - ob(\mathcal{K}) &= S, \\ - |\mathcal{K}(A, B)| &= \begin{cases} 1 & A \leq B, \\ 0 & \text{jinak} \end{cases} \end{aligned}$$

máme tedy kategorii $\mathcal{K}$, kde mezi libovolnými dvěma objekty existuje nejvýše jeden morfismus $f: A \rightarrow B$ a to právě tehdy, když $A \leq B$. Díky tomu jsou identity a kompozice jednoznačně dány.

Definice 5.1.7. Nechť $\mathcal{K}$ je kategorie, $A, B \in ob(\mathcal{K})$ objekty a $f: A \rightarrow B$ morfismus. Řekneme, že f je

- *monomorfismus*, jestliže pro každé $u, v: X \rightarrow A$ platí $f \circ u = f \circ v \Rightarrow u = v$,
- *epimorfismus*, jestliže pro každé $u, v: B \rightarrow X$ platí $u \circ f = v \circ f \Rightarrow u = v$.

Definice 5.1.8. Nechť $\mathcal{A}, \mathcal{B}$ jsou kategorie. Funktor $F: \mathcal{A} \rightarrow \mathcal{B}$ se sestává z

1. $F_{ob}: ob(\mathcal{A}) \rightarrow ob(\mathcal{B})$,
2. $F_{mor}: \mathcal{A}(A, B) \rightarrow \mathcal{B}(F(A), F(B))$, tj. pro $f: A \rightarrow B$ dostáváme $F(f): F(A) \rightarrow F(B)$, přitom platí
 - $F(f \circ g) = F(f) \circ F(g)$,
 - $F(\text{id}_A) = \text{id}_{F(A)}$ pro $A \in \mathcal{A}$.

Příklad. Uvažme funktor $U: Gp \rightarrow Set$, který každé grupě G přiřadí její nosnou množinu a homomorfismu $f: G \rightarrow H$ přiřadí tuto množinovou funkci. Takový funktor U nazýváme zapomínající.

Podobně lze uvažovat i jiné typy zapomínajících funktorů. Například funktor $F: Ring \rightarrow Ab$ posílající $(R, +, \cdot)$ na $(R, +)$.

Příklad. Uvažme dva monoidy jakožto kategorie $\mathcal{A}, \mathcal{B}$ s jedním objektem. Funktor $F: \mathcal{A} \rightarrow \mathcal{B}$ posílá jediný objekt kategorie $\mathcal{A}$ na jediný objekt kategorie $\mathcal{B}$, takže je funktor F plně určen tím, kam pošle morfismy. Zřejmě je funktor F homomorfismem monoidu $\mathcal{A}$ do monoidu $\mathcal{B}$.

Definice 5.1.9. Necht $\mathcal{A}, \mathcal{B}$ jsou kategorie. Kontravariantním funktorem z $\mathcal{A}$ do $\mathcal{B}$ rozumíme funktor $F: \mathcal{A}^{op} \rightarrow \mathcal{B}$.

Zejména zobrazí $f: K_1 \rightarrow K_2$ na $F(f): F(K_2) \rightarrow F(K_1)$ a platí $F(f \circ g) = F(g) \circ F(f)$.

Definice 5.1.10. Necht $\mathcal{K}$ je lokálně malá kategorie, $K \in ob(\mathcal{K})$.

- Funktor $\mathcal{K}(K, -): \mathcal{K} \rightarrow Set$ se nazývá homfunktor.
- Funktor $\mathcal{K}(-, K): \mathcal{K}^{op} \rightarrow Set$ se nazývá kontravariantní homfunktor.

Definice 5.1.11. Funktor $F: \mathcal{A} \rightarrow \mathcal{B}$ se nazývá věrný (respektive plný), jestliže pro libovolné $A, A' \in ob(\mathcal{A})$ je

$$\begin{aligned} \mathcal{A}(A, A') &\rightarrow \mathcal{B}(F(A), F(A')) \\ f &\mapsto F(f) \end{aligned}$$

injektivní (respektive surjektivní).

Necht $\mathcal{A}$ je podkategorie kategorie $\mathcal{B}$. Řekneme, že $\mathcal{A}$ je plná podkategorie, jestliže funktor inkluze je plný.

Příklad. Ab je plná podkategorie Gp .

Definice 5.1.12. Necht $\mathcal{A}, \mathcal{B}$ jsou kategorie a $F, G: \mathcal{A} \rightarrow \mathcal{B}$ jsou funktory mezi nimi. Přírozenou transformací $\alpha: F \rightarrow G$ rozumíme soubor morfismů $(F(A) \xrightarrow{\alpha_A} G(A))_{A \in \mathcal{A}}$ v $\mathcal{B}$ takových, že pro libovolný morfismus $f \in \mathcal{A}(A, A')$ diagram

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(A') \\ \alpha_A \downarrow & & \downarrow \alpha_{A'} \\ G(A) & \xrightarrow{G(f)} & G(A') \end{array}$$

komutuje.

Poznámka. Protože přírozené transformace jsou šipky mezi funktory, můžeme je též chtít skládat. Uvažme tedy kategorie $\mathcal{A}, \mathcal{B}$, funktory $F, G, H: \mathcal{A} \rightarrow \mathcal{B}$ a přírozené transformace $\alpha: F \rightarrow G$ a $\beta: G \rightarrow H$. Chceme definovat složení $\beta \circ \alpha: F \rightarrow H$. To lze udělat přírozeně tak, že položíme $(\beta \circ \alpha)_A = \beta_A \circ \alpha_A$ pro každé $A \in ob(\mathcal{A})$. Protože pro každý funktor F máme přírozenou transformaci $F \rightarrow F$ (identita), můžeme pro libovolnou dvojici kategorií $\mathcal{A}, \mathcal{B}$ uvažovat kategorii, jejíž objekty jsou funktory z $\mathcal{A}$ do $\mathcal{B}$ a jejíž morfismy jsou právě přírozené transformace. Tato kategorie se nazývá *kategorie funktorů* $\mathcal{A} \rightarrow \mathcal{B}$, značí se $\mathcal{B}^{\mathcal{A}}$ nebo též $[\mathcal{A}, \mathcal{B}]$.

Definice 5.1.13. Necht $\mathcal{A}, \mathcal{B}$ jsou kategorie. Přírozeným izomorfismem funktorů $F, G: \mathcal{A} \rightarrow \mathcal{B}$ rozumíme izomorfismus F, G jako objektů v kategorii $[\mathcal{A}, \mathcal{B}]$.

Lemma 5.1.14. *Nechť $\mathcal{A}, \mathcal{B}$ jsou kategorie, $F, G: \mathcal{A} \rightarrow \mathcal{B}$ jsou funktory. Přirozená transformace $\alpha: \mathcal{A} \rightarrow \mathcal{B}$ je přirozený izomorfismus právě tehdy, když $\alpha_A: F(A) \rightarrow G(A)$ je izomorfismus pro všechna $A \in \mathcal{A}$.*

Poznámka. $F(A) \cong G(A)$ přirozeně v A znamená, že existuje přirozený izomorfismus mezi F a G .

5.2 Yonedovo lemma

Definice 5.2.1. Nechť $\mathcal{K}$ je lokálně malá kategorie. Funktor $y: \mathcal{K} \rightarrow \text{Set}^{\mathcal{K}^{op}}$ posílající objekt $K \in \text{ob}(\mathcal{K})$ na kontravariantní reprezentovatelný funktor, tj.

$$y(C) = \text{Hom}_{\mathcal{K}}(-, C): \mathcal{K}^{op} \rightarrow \text{Set}$$

a morfismus $f: K \rightarrow L$ na přirozenou transformaci

$$y(f) = \text{Hom}_{\mathcal{K}}(-, f): \text{Hom}_{\mathcal{K}}(-, K) \rightarrow \text{Hom}_{\mathcal{K}}(-, L),$$

se nazývá *Yonedovo vnoření*.

Věta 5.2.2 (Yonedovo lemma). *Nechť $\mathcal{K}$ je lokálně malá kategorie. Pro libovolný objekt $K \in \mathcal{K}$ a libovolný funktor $F \in \text{Set}^{\mathcal{K}^{op}}$ existuje izomorfismus*

$$\text{Hom}(y(K), F) \cong F(K),$$

který je přirozený pro K i F .

Poznámka.

- Přirozenost pro K :

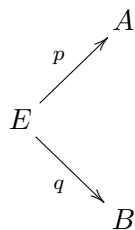
$$\begin{array}{ccc} \text{Hom}(y(K_1), F) & \xrightarrow{\cong} & F(K_1) \\ \text{Hom}(y(h), F) \downarrow & & \downarrow F(h) \\ \text{Hom}(y(K_2), F) & \xrightarrow{\cong} & F(K_2) \end{array}$$

- Přirozenost pro F :

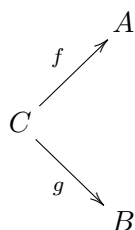
$$\begin{array}{ccc} \text{Hom}(y(K), F) & \xrightarrow{\cong} & F(K_1) \\ \text{Hom}(y(h), F) \downarrow & & \downarrow F(h) \\ \text{Hom}(y(K), G) & \xrightarrow{\cong} & F(K_2) \end{array}$$

5.3 Kartézsky uzavřené kategorie

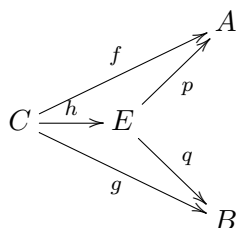
Definice 5.3.1. Buď $\mathcal{K}$ kategorie, $A, B \in \text{ob}(\mathcal{K})$. Součinem A, B rozumíme diagram (tj. objekt spolu s morfismy)



který má univerzální vlastnost, že pokud je dán diagram



pak existuje jediný morfismus $h: C \rightarrow E$ takový, že diagram



komutuje.

Definice 5.3.2. Nechť je $\mathcal{K}$ kategorie s konečnými součiny a nechť pro libovolné objekty $Y, Z \in \text{ob}(\mathcal{K})$ obsahuje též objekt Z^Y spolu s morfismem

$$\text{eval}: Z^Y \times Y \rightarrow Z$$

tak, že libovolnému

$$f: X \times Y \rightarrow Z$$

přiřadíme

$$\tilde{f}: X \rightarrow Z^Y$$

a to jednoznačně. Přitom platí

$$f: X \times Y \xrightarrow{\tilde{f} \times Y} Z^Y \times Y \xrightarrow{\text{eval}} Z$$

$$f: (x, y) \longrightarrow (\tilde{f}(x), y) \longrightarrow f(x, y).$$

Poznámka. Alternativně: Kategorie $\mathcal{K}$ je kartézsky uzavřená právě tehdy, když má konečné součtiny a pro každé $K \in \mathcal{K}$ má funktor

$$_ \times K: \mathcal{A} \rightarrow \mathcal{A}$$

zprava adjungovaný funktor.

Zprava adjungovaný funktor se v tomto případě značí $(_)^K$. Adjungovanost říká, že

$$\mathcal{K}(L \times K, M) \cong \mathcal{K}(L, M^K).$$

přirozeně v L a M .

Příklad.

- Kategorie *Set* je kartézsky uzavřená.
- Nechť C je malá kategorie, pak Set^C , tj. kategorie funktorů $C \rightarrow \text{Set}$, je kartézsky uzavřená.
- Kategorie vektorových prostorů Vect_k nad tělesem k není kartézsky uzavřená. Binární součin je direktní součet $\oplus$. Terminální objekt je triviální vektorový prostor. Pokud by kategorie vektorových prostorů nad tělesem k byla kartézsky uzavřená, pak by $\{0\} \oplus V \cong \{0\}$ pro libovolný vektorový prostor V .

Věta 5.3.3. Buď $\mathcal{K}$ kartézsky uzavřená kategorie s iniciálním objektem 0 taková, že

$$A \cong 0^{(0^A)}$$

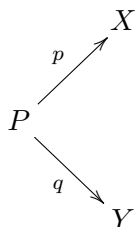
pro libovolné $A \in \text{ob}(\mathcal{K})$. Pak $\mathcal{K}$ je tenká, tj. $|\mathcal{K}(A, B)| \leq 1$.

Kapitola 6

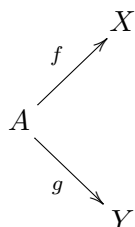
Limity

6.1 Součiny, součty, ekvalizátory, pullbacky, pushouty

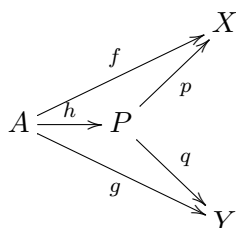
Definice 6.1.1. Buď $\mathcal{K}$ kategorie, $X, Y \in \text{ob}(\mathcal{K})$. *Součinem* X, Y rozumíme diagram (tj. objekt spolu s morfismy)



s univerzální vlastností, že pokud je dán diagram



pak existuje jediný morfismus $h: A \rightarrow P$ takový, že diagram



komutuje. Zobrazení p, q se nazývají projekce. Součin X, Y značíme $X \times Y$.

Věta 6.1.2. *Nechť $\mathcal{K}$ je kategorie. Součin $X, Y \in \text{ob}(\mathcal{K})$ je dán jednoznačně až na izomorfismus.*

Definice 6.1.3. Buď $\mathcal{K}$ kategorie, $X, Y \in \text{ob}(\mathcal{K})$. *Součtem* X, Y rozumíme diagram

$$\begin{array}{ccc} X & & \\ & \searrow i & \\ & & C \\ & \nearrow j & \\ Y & & \end{array}$$

s univerzální vlastností, že pokud je dán diagram

$$\begin{array}{ccc} X & & \\ & \searrow f & \\ & & D \\ & \nearrow g & \\ Y & & \end{array}$$

pak existuje jediný morfismus $h: C \rightarrow D$ takový, že diagram

$$\begin{array}{ccccc} X & & & & \\ & \searrow f & & & \\ & & & & \\ & \searrow i & & \nearrow h & \\ & & C & \xrightarrow{h} & D \\ & \nearrow j & & & \\ Y & & & \nearrow g & \end{array}$$

komutuje. Součet objektů X, Y značíme $X + Y$.

Poznámka. Alternativně bychom mohli říct, že součet je součinem v duální kategorii.

Definice 6.1.4. Buď $\mathcal{K}$ kategorie, $X, Y \in \text{ob}(\mathcal{K})$ a necht' $f, g: X \rightarrow Y$ jsou morfismy mezi nimi. *Ekvalizátorem* morfismů f, g rozumíme diagram

$$E \xrightarrow{e} X \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} Y$$

takový, že $fe = ge$ a je-li dán libovolný objekt A spolu s morfismem $h: A \rightarrow X$, kde $fh = gh$, pak existuje jediný morfismus $t: X \rightarrow E$ tak, že $et = h$, tj. následující diagram komutuje

$$\begin{array}{ccc} E & \xrightarrow{e} & X \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} Y \\ \uparrow t & \nearrow h & \\ A & & \end{array}$$

Poznámka. Koekvalizátorem rozumíme ekvalizátor v duální kategorii.

Definice 6.1.5. Necht' $\mathcal{K}$ je kategorie. Necht' je dán diagram

$$\begin{array}{ccc} & & Z \\ & & \downarrow g \\ Y & \xrightarrow{f} & X \end{array}$$

Pullbackem tohoto diagramu rozumíme $P \in \text{ob}\mathcal{K}$ spolu s morfismy $p_1: P \rightarrow Y$ a $p_2: P \rightarrow Z$ tak, že diagram

$$\begin{array}{ccc} P & \xrightarrow{p_2} & Z \\ p_1 \downarrow & & \downarrow g \\ Y & \xrightarrow{f} & X \end{array}$$

komutuje, přičemž pokud komutuje

$$\begin{array}{ccc} A & \xrightarrow{q_2} & Z \\ q_1 \downarrow & & \downarrow g \\ Y & \xrightarrow{f} & X \end{array}$$

pak existuje jediný morfismus $h: A \rightarrow P$ takový, že diagram

$$\begin{array}{ccccc} A & & & & \\ & \searrow h & \searrow q_2 & & \\ & & P & \xrightarrow{p_2} & Z \\ & \searrow p_1 & \downarrow & & \downarrow g \\ & & Y & \xrightarrow{f} & X \end{array}$$

komutuje.

Definice 6.1.6. *Pushoutem* rozumíme pullback v duální kategorii (tj. otočíme všechny šipky v definici pullbacku).

Příklad. *Uvažme kategorii Set.*

- *Součinem množin X, Y je kartézský součin $X \times Y$.*
- *Součtem množin X, Y je disjunktivní sjednocení $X \sqcup Y$.*
- *Nechť $f, g: X \rightarrow Y$. Ekvalizátorem zobrazení f, g je $E = \{x \in X \mid f(x) = g(x)\}$ spolu s vnořením $E \rightarrow X$.*

6.2 Limity, kolimity

V předchozím jsme představili tři speciální případy limit: součiny, ekvalizátory a pullbacky. Naším cílem bude tento koncept zobecnit. Při konstrukci těchto limit jsme vždy začali s nějakými objekty a morfismy mezi nimi:

- u součinu se jednalo o

$$X$$

$$Y$$

- u ekvalizátoru se jednalo o

$$X \begin{array}{c} \xrightarrow{f} \\ \xRightarrow{g} \end{array} Y$$

- u pullbacku se jednalo o

$$\begin{array}{ccc} & & Z \\ & & \downarrow g \\ Y & \xrightarrow{f} & X \end{array}$$

Objektem v libovolné kategorii $\mathcal{K}$ je funktor $1 \rightarrow \mathcal{K}$, morfismem je funktor $2 \rightarrow \mathcal{K}$, kde 2 je kategorie s dvěma objekty, identitami na nich a jediným dalším morfismem mezi těmito dvěma objekty. V předchozím jsme uvažovali kategorie

$$\mathbb{T} = \bullet \quad \bullet, \quad \mathbb{E} = \bullet \rightrightarrows \bullet, \quad \mathbb{P} = \bullet \rightarrow \bullet \leftarrow \bullet$$

Nyní budeme uvažovat obecně funktor $D: \mathcal{I} \rightarrow \mathcal{K}$, kde $\mathcal{I}$ je malá kategorie.

Definice 6.2.1. Nechť $\mathcal{K}$ je kategorie, $\mathcal{I}$ je malá kategorie. Funktor $\mathcal{I} \rightarrow \mathcal{K}$ se nazývá *diagram* v $\mathcal{K}$ tvaru $\mathcal{I}$.

Definice 6.2.2. Buď $\mathcal{K}$ kategorie, $\mathcal{I}$ malá kategorie a $D: \mathcal{I} \rightarrow \mathcal{K}$ diagram v $\mathcal{K}$. *Kuželem* na D rozumíme objekt $K \in \mathcal{K}$ společně se souborem morfismů $(K \xrightarrow{q_I} D(I))_{I \in \mathcal{I}}$ v $\mathcal{K}$ takových, že pro libovolné zobrazení $I \xrightarrow{u} J$ v $\mathcal{I}$ diagram

$$\begin{array}{ccc} & D(I) & \\ q_I \nearrow & \downarrow D(u) & \\ K & & \\ q_J \searrow & \downarrow & \\ & D(J) & \end{array}$$

komutuje.

Limitou rozumíme terminální kužel, tj. kužel $(L \xrightarrow{p_I} D(I))_{I \in \mathcal{I}}$ s univerzální vlastností, že pro libovolný kužel K na D existuje jediné zobrazení $h: K \rightarrow L$ tak, že $p_I \circ h = q_I$ pro každé $I \in \mathcal{I}$.

Definice 6.2.3. Kolimitou rozumíme limitu v duální kategorii.

Poznámka. Alternativně můžeme udělat podobnou konstrukci jako u limity.

Nechť $\mathcal{K}$ je kategorie a $\mathcal{I}$ malá kategorie, $D: \mathcal{I} \rightarrow \mathcal{K}$ je diagram v $\mathcal{K}$. Duálním kuželem na D rozumíme objekt $K \in \mathcal{K}$ společně s třídou morfismů $(D(I) \rightarrow K)_{I \in \mathcal{I}}$ tak, aby diagram

$$\begin{array}{ccc} D(I) & & \\ \downarrow & q_I \searrow & \\ & K & \\ & q_J \nearrow & \\ D(J) & & \end{array}$$

komutoval. Kolimitou pak rozumíme iniciální duální kužel, tj. takový duální kužel $(D(I) \rightarrow C)_{I \in \mathcal{I}}$, že pro libovolný duální kužel $(D(I) \rightarrow K)_{I \in \mathcal{I}}$ existuje jediné zobrazení $h: C \rightarrow K$ tak, aby $hp_I = q_I$

Definice 6.2.4. Řekneme, že kategorie $\mathcal{K}$ je *kompletní*, jestliže má všechny limity. Řekneme, že kategorie $\mathcal{K}$ je *kokompletní*, jestliže má všechny kolimity.

6.3 Limity pomocí součinů a ekvalizátorů

Věta 6.3.1. *Nechť $\mathcal{K}$ je kategorie.*

1. *Má-li $\mathcal{K}$ všechny součiny a ekvalizátory, pak má $\mathcal{K}$ všechny limity.*
2. *Má-li $\mathcal{K}$ binární součiny, ekvalizátory a terminální objekt, pak má $\mathcal{K}$ má konečné limity.*

Věta 6.3.2. *Funktor $F: \mathcal{A} \rightarrow \mathcal{B}$ zachovává limity právě tehdy, když zachovává součiny a ekvalizátory.*

Kapitola 7

Adjungované funktory

7.1 Definice a příklady

Definice 7.1.1. Necht $\mathcal{A}, \mathcal{B}$ jsou kategorie, $F: \mathcal{A} \rightarrow \mathcal{B}$ a $G: \mathcal{B} \rightarrow \mathcal{A}$ funktory mezi nimi. Jestliže

$$\mathcal{B}(F(A), B) \cong \mathcal{A}(A, G(B))$$

přirozeně v $A \in \mathcal{A}$ a $B \in \mathcal{B}$, řekneme, že F je *zleva adjungovaný* ke G a G je *zprava adjungovaný* k F , píšeme $F \dashv G$. *Adjunkcí* mezi F a G rozumíme volbu přirozeného izomorfismu.

Příklad. *Algebraické struktury: volný $\dashv$ zapomínající*

- *Necht k je těleso. Uvažme následující funktory. Necht U je zapomínající funktor*

$$U: \text{Vect}_k \rightarrow \text{Set}$$

a F je volný funktor

$$F: \text{Set} \rightarrow \text{Vect}_k$$

tj. množině přiřadí vektorový prostor nad tělesem k , kde je tato množina bází. Adjungovanost říká, že je-li dána množina S a vektorový prostor V , pak lineární zobrazení

$$F(S) \rightarrow V$$

je v podstatě to stejné, jako funkce

$$S \rightarrow U(V).$$

- *Necht U je zapomínající funktor $\text{Ab} \rightarrow \text{Gp}$, který posílá abelovkou grupu na sebe samu. Funktor F posílá grupu G na její abelizaci, pak opět $F \dashv U$.*
- *Uvážíme-li kategorii Field těles, kde morfismy jsou homomorfismy okruhů, pak zapomínající funktor $U: \text{Field} \rightarrow \text{Set}$ nemá levou adjunkci.*

7.2 Freydova věta

Definice 7.2.1. Necht $\mathcal{K}$ je kategorie. Řekneme, že objekt $I \in \text{ob}(\mathcal{K})$ je

- *iniciální*, jestliže $\forall X \in \text{ob}(\mathcal{K}) \exists ! f: I \rightarrow X$,
- *slabě iniciální*, jestliže $\forall X \in \text{ob}(\mathcal{K}) \exists I \rightarrow X$,

Řekneme, že množina $J \subseteq \text{ob}(\mathcal{K})$ je *slabě iniciální množina objektů*, jestliže $\forall X \in \text{ob}(\mathcal{K}) \exists I \in J$ a morfismus $f: I \rightarrow X$.

Lemma 7.2.2. *Nechť je $\mathcal{K}$ lokálně malá kategorie se součiny mající slabě iniciální množinu objektů. Pak má $\mathcal{K}$ slabě iniciální objekt.*

Důkaz. Nechť J je slabě iniciální množina objektů. Slabě iniciálním objektem je $\prod J$. Protože pro libovolné $A \in \text{ob}(\mathcal{K})$ existuje $I \in J$ a $J \rightarrow A$, dostáváme složením s projekcí morfismus

$$\prod J \rightarrow I \rightarrow A$$

pro libovolné A .

Lemma 7.2.3. *Je-li F zleva adjungovaný k U , pak je U zprava adjungovaný k F .*

Věta 7.2.4. *Má-li funktor $U: \mathcal{A} \rightarrow \mathcal{B}$ zleva adjungovaný funktor, pak U zachovává limity.*

Poznámka. Obrácená implikace (tj. zachovává limity $\Rightarrow$ má zleva adjungovaný) obecně neplatí

- úplné Booleovy algebry $\rightarrow$ úplné svazy,
- úplné svazy $\rightarrow$ množiny.

Definice 7.2.5. Nechť jsou dány kategorie $\mathcal{A}, \mathcal{B}, \mathcal{C}$ a funktory $P: \mathcal{A} \rightarrow \mathcal{C}$ a $Q: \mathcal{B} \rightarrow \mathcal{C}$. Kategorie $P \downarrow Q$ se sestává z

- objektů: (A, h, B) , kde $A \in \mathcal{A}, B \in \mathcal{B}$ a $h: P(A) \rightarrow Q(B)$ v $\mathcal{C}$,
- morfismů $(A, h, B) \rightarrow (A', h', B')$: dvojic $(f: A \rightarrow A', g: B \rightarrow B')$ tak, že diagram

$$\begin{array}{ccc} P(A) & \xrightarrow{P(f)} & P(A') \\ h \downarrow & & \downarrow h' \\ Q(B) & \xrightarrow{Q(g)} & Q(B') \end{array}$$

komutuje.

Nechť $A \in \mathcal{A}$, $P: \mathcal{B} \rightarrow \mathcal{A}$ je funktor. Kategorii $K \downarrow P$ rozumíme kategorií danou diagramem

$$\begin{array}{ccc} & \mathcal{B} & \\ & \downarrow P & \\ 1 & \xrightarrow{A} & \mathcal{A} \end{array}$$

- objekty: dvojice $(B \in \mathcal{B}, f: A \rightarrow P(B))$
- morfismus $(B, f) \rightarrow (B', f')$ je zobrazení $q: B \rightarrow B'$ takové, že diagram

$$\begin{array}{ccc} A & \xrightarrow{f} & P(B) \\ & \searrow f' & \downarrow P(q) \\ & & P(B') \end{array}$$

komutuje.

Věta 7.2.6 (Freydova věta o adjungovaných funktorech). *Nechť $\mathcal{A}$ je kategorie a $\mathcal{B}$ je úplná a lokálně malá kategorie. Nechť $G: \mathcal{B} \rightarrow \mathcal{A}$ je funktor takový, že pro každé $A \in \text{ob}(\mathcal{A})$ má kategorie $A \downarrow G$ slabě iniciální množinu objektů. Pak G má levou adjunkci právě tehdy, když G zachovává limity.*

Kapitola 8

Rozšíření těles

Definice 8.0.1. Necht K, L jsou tělesa a necht K je podokruh L . Pak řekneme, že K je *podtělesem* tělesa L , též L je *rozšířením* tělesa K .

Necht $\alpha_1, \dots, \alpha_n \in L$. Podtěleso tělesa L generované množinou $K \cup \{\alpha_1, \dots, \alpha_n\}$ budeme značit $K(\alpha_1, \dots, \alpha_n)$.

Věta 8.0.2. Buď K těleso charakteristiky $p \neq 0$. Pak K obsahuje jako svoje podtěleso těleso izomorfní s $\mathbb{Z}/p\mathbb{Z}$. Je-li K těleso charakteristiky 0, pak K obsahuje jako svoje podtěleso těleso izomorfní s $\mathbb{Q}$. Toto podtěleso se nazývá základové těleso.

8.1 Algebraická a konečná rozšíření

Definice 8.1.1. Necht $K \subseteq L$ je rozšíření těles. Řekneme, že $\alpha \in K$ je *algebraický nad L* , jestliže existuje nenulový polynom $f \in K[x]$ takový, že $f(\alpha) = 0$. V opačném případě se α nazývá *transcendentní prvek nad K* .

Definice 8.1.2. Necht $K \subseteq L$ je rozšíření těles, $\alpha \in L$ je algebraický nad K . Normovaný polynom $f \in K[x]$, který je ireducibilní nad K a má kořen α nazýváme *minimální polynom prvku α nad K* .

Definice 8.1.3. Necht $K \subseteq L$ je rozšíření těles. *Stupněm rozšíření L nad K* rozumíme dimenzi vektorového prostoru $(L, +)$ nad tělesem K , značíme $[L : K]$.

Definice 8.1.4. Necht $K \subseteq L$ je rozšíření těles. Řekneme, že toto rozšíření je

- *jednoduché*, jestliže existuje $\alpha \in L$ algebraické nad R takové, že $L = K(\alpha)$,
- *konečné*, jestliže stupeň rozšíření $[L : K]$ je konečný,
- *algebraické*, jestliže každý prvek $\alpha \in L$ je algebraický nad R .

Věta 8.1.5. Každé jednoduché rozšíření je konečné.

Každé konečné rozšíření tělesa charakteristiky 0 je jednoduché.

Každé konečné rozšíření je algebraické.

8.2 Rozkladová tělesa a normální rozšíření, algebraický uzávěr

Definice 8.2.1. Řekneme, že těleso K je *algebraicky uzavřené*, jestliže každý nekonstantní polynom $f \in K[x]$ má v K kořen.

Věta 8.2.2. *Nechť K je těleso. Následující podmínky jsou ekvivalentní*

- K je algebraicky uzavřené,
- každý nekonstantní polynom $f \in K[x]$ se v $K[x]$ rozkládá na součin lineárních činitelů,
- každý ireducibilní polynom nad K je lineární,
- pro L konečné rozšíření K platí, že $L = K$,
- pro každé algebraické rozšíření $K \subseteq L$ platí $K = L$.

Definice 8.2.3. Nechť K je těleso. Těleso L se nazývá *algebraický uzávěr tělesa K* , jestliže $K \subseteq L$ je algebraické rozšíření a současně L je algebraicky uzavřené těleso.

Definice 8.2.4. Nechť K je těleso, $f \in K[x]$ nekonstantní polynom. Těleso L se nazývá *rozkladové těleso polynomu f nad K* , jestliže $K \subseteq L$ je rozšíření, f se v $L[x]$ rozkládá na součin lineárních činitelů a pro každé těleso T , $K \subseteq T \subset L$ platí, že f se v $T[x]$ nerozkládá na součin lineárních činitelů.

Definice 8.2.5. Rozšíření K/F se nazývá *normální*, jestliže existuje množina $M \subseteq F[x]$ nekonstantních polynomů taková, že každý polynom z M se v $K[x]$ rozkládá na lineární činitele, ale pro každé podtěleso $F \subseteq L \subset K$ existuje $f \in M$, který se na lineární činitele nerozloží.

Poznámka. Rozšíření K/F je tedy normální právě tehdy, když K je rozkladové těleso nějaké množiny polynomů z $F[x]$.

Věta 8.2.6. *Každé těleso F lze vnořit do algebraicky uzavřeného tělesa.*

Důkaz. Pro každý normovaný polynom $f \in F[x]$ uvažme proměnnou x_f . Označme $R = F[\dots, x_f, \dots]$. Nechť I je ideál generovaný všemi x_f pro $f \in F[x]$ normovaný. Ukažme, že ideál I je vlastní. Předpokládejme sporem, že tomu tak není, pak $1 \in I$, tj. $1 = g_1 f_1(x_1) + \dots + g_n f_n(x_n)$, přitom v rozkladovém tělese $f_1 \dots f_n$ existují α_i takové, že $f_i(\alpha_i) = 0$. Odtud

$$1 = g_1(\alpha_1, \dots, \alpha_n, 0, \dots, 0) f_1(\alpha_1) + \dots + g_n(\alpha_1, \dots, \alpha_n, 0, \dots, 0) f_n(\alpha_n) = 0,$$

spor. I je tedy vlastní, lze jej vnořit do maximálního ideálu M . Pak $F_1 = R/M$ je těleso. Stejnou konstrukcí z F_1 obdržíme F_2 . Označme

$$T = \bigcup_{i=1}^{\infty} F_n.$$

Pak T je algebraicky uzavřené těleso obsahující F (jistě každý polynom $g \in T$ pochází z nějakého F_n a v F_{n+1} má kořen).

Důsledek 8.2.7. *Ke každému tělesu existuje jeho algebraický uzávěr.*

Důkaz. Algebraický uzávěr je množina všech algebraických prvků algebraicky uzavřeného tělesa.

8.3 Separabilní a neseperabilní rozšíření

Definice 8.3.1. Necht K je těleso. Nekonstantní polynom $f \in K[x]$ se nazývá *separabilní*, jestliže nemá ve svém rozkladovém tělese násobný kořen.

Věta 8.3.2. Necht K je těleso, $f \in K[x]$ nekonečtní polynom. Pak f je separabilní právě tehdy, když $(f, f') = 1$.

Věta 8.3.3. Necht K je těleso charakteristiky nula, pak každý ireducibilní polynom $f \in K[x]$ je separabilní.

Definice 8.3.4. Řekneme, že rozšíření těles K/F je *separabilní*, jestliže

1. K/F je algebraické
2. pro každé $a \in K$ platí, že minimální polynom prvku a je separabilní.

Definice 8.3.5. Necht K je těleso, $\text{char} K = p > 0$. Zobrazení $\varphi: K \rightarrow K$ určené předpisem $\varphi(a) = a^p$ pro každé $a \in K$ se nazývá *Frobeniův endomorfismus*.

Příklad. Je-li K konečné těleso, pak je Frobeniův endomorfismus dokonce automorfismem.

Definice 8.3.6. Těleso K se nazývá *perfektní*, jestliže platí některá z podmínek

- $\text{char} K = 0$,
- $\text{char} K = p > 0$ a Frobeniův endomorfismus je automorfismem.

Věta 8.3.7. Necht K/F je algebraické rozšíření a F perfektní těleso, pak K/F je separabilní.

Příklad. Uvažujme následující rozšíření:

- $\mathbb{R}/\mathbb{Q}$ není algebraické $\Rightarrow$ není separabilní,
- $\mathbb{C}/\mathbb{R}$ je separabilní,
- $\bar{\mathbb{Q}}/\mathbb{Q}$, kde $\bar{\mathbb{Q}}$ je algebraický uzávěr $\mathbb{Q}$, je separabilní rozšíření,
- K konečné těleso charakteristiky p , pak $K/\mathbb{Z}_p$ je separabilní,
- Buď p prvočíslo, $\mathbb{Z}_p(y)$ těleso racionálních funkcí nad $\mathbb{Z}_p$. Položme $t = y^p$, pak

$$\mathbb{Z}_p(y)/\mathbb{Z}_p(t)$$

je algebraické rozšíření (minimální polynom prvku y nad $\mathbb{Z}_p(t)$ je $x^p - t$, což je neseperabilní polynom. Toto rozšíření tedy je algebraické, ale není separabilní.

- Necht F/L a L/K jsou rozšíření těles. Je-li F/K separabilní, pak jsou separabilní i L/K a F/L .

8.4 Klasické konstrukce pravítkem a kružítkem

Nechť 1 udává délku, kterou máme danou. Budeme chtít určit, která další čísla $a \in \mathbb{R}$ jsme schopni sestavit, tedy které vzdálenosti můžeme z 1 získat poze s využitím pravítka a kružítká. Bod $(x, y) \in \mathbb{R}^2$ je zkonstruovatelný právě tehdy, pokud jsou zkonstruovatelné jeho souřadnice $x, y \in \mathbb{R}$. Množinu všech prvků $a \in \mathbb{R}$, které můžeme zkonstruovat, spolu s prvky opačnými budeme nazývat *zkonstruovatelné prvky* $\mathbb{R}$. Přitom můžeme

1. vést přímku dvěma body,
2. narýsovat kružnici, když máme daný poloměr a střed,
3. nalézt průsečík dvou přímek, dvou kružnic či kružnice a přímky.

Máme-li dány délky $a, b \in \mathbb{R}$, jsme schopni zkonstruovat:

1. $a \pm b$, ab a pro $b \neq 0$ též $\frac{a}{b}$,
2. $\sqrt{a}$ (uvážíme Thaletovu kružnici o poloměru $a + 1$, zbytek plyne z Euklidovy věty o výšce: $v^2 = a \cdot 1$, tj. $v = \sqrt{a}$).

Díky tomu, že tyto konstrukce umožňují čísla sčítat, odčítat, násobit a můžeme i dělit nenulovým číslem, tvoří zkonstruovatelné prvky těleso, které je podtělesem reálných čísel. Protože můžeme konstruovat druhé odmocniny, je $\mathbb{Q}$ vlastním podtělesem hledaného tělesa.

Pokud řešíme průnik dvou přímek, dostáváme soustavu dvou lineárních rovnic tvaru

$$ax + by + c = 0$$

pro $a, b, c \in F$. Takto nezískáme žádný bod, který by ležel mimo F . Kružnice je zadána rovnicí

$$(x - h)^2 + (y - k)^2 = r^2$$

pro $h, k, r \in F$. Řešíme-li průnik kružnice a přímky, můžeme dosadit z lineární rovnice. Obdržíme kvadratickou rovnici v jednom proměnné. Získáme tak nejvýše kvadratické rozšíření F . Konečně uvažme, co lze získat, když budeme uvažovat průnik dvou kružnic.

$$\begin{aligned}(x - h)^2 + (y - k)^2 &= r^2, \\ (x - h')^2 + (y - k')^2 &= r'^2.\end{aligned}$$

Odečtením druhé rovnice od první dostáváme

$$\begin{aligned}(x - h)^2 + (y - k)^2 &= r^2, \\ 2(h' - h)x + 2(k' - k)y &= r^2 - h^2 - k^2 - r'^2 + h'^2 + k'^2,\end{aligned}$$

což opět zadává průsečík přímky s kružnicí. Vidíme, že každá z operací vytvoří nejvýše kvadratické rozšíření. Je-li prvek $\alpha \in \mathbb{R}$ zkonstruovatelný, musí ležet v tělese F takovém, že $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ pro nějaké $n \in \mathbb{N}_0$. Navíc se k tomuto tělesu musíme postupně dostat z $\mathbb{Q}$ pomocí rozšíření, která jsou stupně právě 2. To nám dává následující tvrzení:

Věta 8.4.1. *Žádný z klasických Řeckých problémů (zdvojení krychle, kvadratura kruhu, trisekce úhlu) není řešitelný pomocí pravítka a kružítká.*

Důkaz. Zdvojení krychle o hraně délky 1 vyžaduje vytvoření krychle o hraně délky $\sqrt[3]{2}$. Přitom $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q})] = 3$.

Kvadratura kruhu o poloměru 1 vyžaduje vytvoření čtverce o straně délky $\sqrt{\pi}$, přitom π není algebraické číslo.

Trisekci některých speciálních úhlů (například přímý úhel či pravý úhel) jsme schopni udělat. Musíme nalézt úhel, u kterého toto není možné. Ekvivalentně můžeme tento problém zadat takto: je-li dán $\cos \theta$ zkonstruujte $\cos \frac{\theta}{3}$. Zvolme $\theta = \frac{\pi}{3}$. Víme, že $\cos \frac{\pi}{3} = \frac{1}{2}$. Vyjdeme ze vzorce

$$\cos \theta = 4 \cos^3 \frac{\theta}{3} - 3 \cos \frac{\theta}{3}$$

Položme $\beta = \cos \frac{\pi}{9}$, dostáváme

$$4\beta^3 - 3\beta - \frac{1}{2} = 0,$$

což můžeme přepsat pomocí substituce $\alpha = 2\beta$ jako

$$\alpha^3 - 3\alpha - 1 = 0.$$

Protože polynom $x^3 - 3x - 1$ nemá kořen v $\mathbb{Q}$, je ireducibilní, je to tedy minimální polynom α . Proto $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = 3$.

Věta 8.4.2. *Pravidelný n -úhelník jde sestavit pravítkem a kružítkem právě tehdy, když $\varphi(n)$ je mocnina dvou.*

Kapitola 9

Galoisova teorie

Definice 9.0.1. Nechť K je těleso. Označme $\text{Aut}(K)$ množinu automorfismů tělesa K , tj. izomorfismů $K \rightarrow K$. Nechť K/F je rozšíření těles. Řekneme, že $\sigma \in \text{Aut}(K)$ *fixuje* F , jestliže $\forall a \in F: \sigma(a) = a$. Množinu automorfismů tělesa K fixujících F označíme $\text{Aut}(K/F)$.

Lemma 9.0.2. Nechť K/F je rozšíření, pak $(\text{Aut}(K), \circ)$ je grupa, $(\text{Aut}(K/F), \circ)$ její podgrupa.

Lemma 9.0.3. Nechť K/F je rozšíření těles, $\alpha \in K$ je algebraický nad F , $f \in F[x]$ minimální polynom prvku α . Pak $\forall \sigma \in \text{Aut}(K/F): f(\sigma(\alpha)) = 0$.

Důsledek 9.0.4. Je-li K/F rozšíření těles, pak $\sigma \in \text{Aut}(K/F)$ permutuje množinu kořenů $f \in F[x]$ v K .

Lemma 9.0.5. Nechť K je těleso, $H \leq \text{Aut}(K)$. $\text{Fix}(H) = \{a \in K \mid \forall \sigma \in H: \sigma(a) = a\}$ je podtěleso tělesa K .

Lemma 9.0.6. Nechť K je těleso.

- Pro každé dvě podtělesa $F_1 \subseteq F_2 \subseteq K$ platí $\text{Aut}(K/F_2) \leq \text{Aut}(K/F_1)$.
- Pro každé dvě podgrupy $H_1 \leq H_2 \leq \text{Aut}(K)$ platí $\text{Fix}(H_1) \supseteq \text{Fix}(H_2)$.

Věta 9.0.7. Nechť F je těleso, $f \in F[x]$ nekonstantní polynom. Nechť K je rozkladové těleso polynomu f nad F . Pak platí

$$|\text{Aut}(K/F)| \leq [K : F]$$

přičemž rovnost nastává, jestliže polynom f je separabilní.

Definice 9.0.8. Nechť K/F je konečné rozšíření. Řekneme, že toto rozšíření je *Galoisovo*, jestliže

$$|\text{Aut}(K/F)| = [K : F].$$

V takovém případě budeme psát $\text{Gal}(K/F)$ místo $\text{Aut}(K/F)$, abychom tento fakt zdůraznili. Grupa $\text{Gal}(K/F)$ se nazývá *Galoisova grupa*.

Definice 9.0.9. Nechť K/F je Galoisovo rozšíření s Galoisovou grupou $G = \text{Gal}(K/F)$, $\alpha \in K$. Prvky $\sigma(\alpha)$ pro $\sigma \in G$ nazýváme *konjugované* s α nad F . Je-li E podtěleso K obsahující F (takovým tělesům budeme říkat *meztělesa*), pak podtěleso $\sigma(E)$, $\sigma \in G$ nazýváme podtěleso konjugované s E nad F .

Definice 9.0.10. Rozšíření K/F se nazývá *normální*, jestliže je K rozkladové těleso nějaké množiny polynomů z $F[x]$.

Věta 9.0.11. *Buď K/F rozšíření těles. Následující podmínky jsou ekvivalentní*

1. K/F je Galoisovo (tj. $|\text{Aut}(K/F)| = [K : F]$),
2. K je rozkladové těleso vhodného separabilního polynomu $f \in F[x]$ nad F ,
3. $F = \text{Fix}(\text{Aut}(K/F))$, kde K/F je konečné,
4. K je konečné, normální, separabilní rozšíření tělesa F .

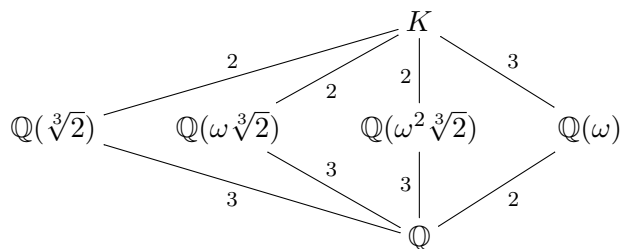
Příklad.

- $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ není Galoisovo. $|\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1 < 3[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}]$. Minimální polynom $x^3 - 2$ má nereálné kořeny, přitom $\mathbb{Q}(\sqrt[3]{2})$ obsahuje pouze reálná čísla. $\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\text{id}\}$ a $\text{Fix}(\text{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})) = \mathbb{Q}(\sqrt[3]{2})$.
- Uvažme polynom $x^3 - 2$. Označme $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$ jeho rozkladové těleso ($\omega = \frac{1}{2} - i\frac{\sqrt{3}}{2}$). Protože $[K : \mathbb{Q}] = 6$, má je $|\text{Gal}(K/\mathbb{Q})| = 6$.

$$\forall \sigma \in \text{Gal}(K/\mathbb{Q}) : \sigma(\sqrt[3]{2}) \in \{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\},$$

$$\sigma(\omega) \in \{\omega, \omega^2\}.$$

Protože má Galoisova grupa 6 prvků, každá z těchto voleb zadává nějaký automorfismus.



Každé $\sigma \in \text{Gal}(K/\mathbb{Q})$ zadává jednu permutaci množiny $\{\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}\}$, proto

$$\text{Gal}(K/\mathbb{Q}) \cong S_3$$

9.1 Základní věta Galoisovy teorie

Věta 9.1.1 (Hlavní věta Galoisovy teorie). *Nechť K/F je Galoisovo rozšíření s Galoisovou grupou G . Pak máme bijekci mezi množinami*

$$\{H \mid H \subseteq G\} \rightarrow \{E \mid E \text{ těleso}, F \subseteq E \subseteq K\},$$

$$H \mapsto \text{Fix}(H),$$

$$\text{Aut}(K/E) \leftarrow E.$$

Pro libovolné mezitěleso E a jím určenou $H = \text{Aut}(K/E)$ platí

- K/E je Galoisovo, $\text{Gal}(K/E) = H$,
 $[K : E] = |H|$, $[E : F] = [G : H]$.
- E/F je Galoisovo právě tehdy, když H je normální podgrupa grupy G . V tomto případě je $\text{Gal}(E/F) \cong G/H$, přičemž izomorfismus je dán restrikcí. Obecně (H nemusí být normální) restrikce určí bijekci mezi rozkladem G/H na levé třídy rozkladu a množinou všech vnoření tělesa E do prvně zvoleného algebraického uzávěru tělesa K nechávající na místě všechny prvky v F .

- Jsou-li E_1, E_2 libovolná mezitělesa a H_1, H_2 jimi určené podgrupy, pak

$$E_1 \subseteq E_2 \Leftrightarrow H_2 \Leftrightarrow H_1.$$

Tedy popisovaná bijekce je izomorfismus svazu $(\{H \mid H \leq G\}, \subseteq)$ a svazu duálního k $(\{E \mid E \text{ těleso}, F \subseteq E \subseteq K\}, \subseteq)$.

Věta 9.1.2. Necht F, K_1, K_2 jsou podtělesa daného tělesa T taková, že K_1/F a K_2/F jsou Galoisova rozšíření. Pak platí

- $(K_1 \cap K_2)/F$ je Galoisovo,
- $K_1 K_2/F$ je Galoisovo, navíc $\text{Gal}(K_1 K_2/F)$ je izomorfní s následující podgrupou součinu grup $\text{Gal}(K_1/F) \times \text{Gal}(K_2/F)$, totiž s podgrupou

$$H = \{(\sigma, \tau) \mid \sigma_{K_1 \cap K_2} = \tau_{K_1 \cap K_2}\}$$

Zejména je-li $K_1 \cap K_2 = F$, pak

$$\text{Gal}(K_1 K_2/F) = \text{Gal}(K_1/F) \times \text{Gal}(K_2/F).$$

Důsledek 9.1.3. Necht K/F je konečné separabilní rozšíření, pak ve zvoleném algebraickém uzávěru tělesa K existuje těleso E obsahující K takové, že E/F je Galoisovo.

Definice 9.1.4. Nejmenší takové E v rámci zvoleného algebraického uzávěru nazveme *Galoisův uzávěr* rozšíření K/F .

Věta 9.1.5. Necht K/F je konečné rozšíření. Pak platí, že K/F je jednoduché právě tehdy, když existuje jen konečně mnoho mezitěles.

Důsledek 9.1.6. Každé konečné separabilní rozšíření je jednoduché.

9.2 Kruhová a abelovská rozšíření tělesa racionálních čísel

Definice 9.2.1. Rozšíření těles K/F nazveme abelovské, jestliže je Galoisovo a má komutativní Galoisovu grupu.

Věta 9.2.2. Pro libovolné $n \in \mathbb{N}$ je $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ abelovské.

Důsledek 9.2.3. Pro libovolné podtěleso $K \subseteq \mathbb{Q}(\zeta_n)$ platí, že $K/\mathbb{Q}$ i $\mathbb{Q}(\zeta_n)/K$ jsou abelovská.

Věta 9.2.4 (Kroneckerova-Weberova). Je-li $K \subseteq \mathbb{C}$ takové, že $K/\mathbb{Q}$ je abelovské, pak existuje $n \in \mathbb{N}$ takové, že $K \subseteq \mathbb{Q}(\zeta_n)$.

Příklad. Necht $m, n \in \mathbb{N}$. Pak platí

$$\begin{aligned}\mathbb{Q}(\zeta_n) \cap \mathbb{Q}(\zeta_m) &= \mathbb{Q}(\zeta_{(m,n)}), \\ \mathbb{Q}(\zeta_n) \cdot \mathbb{Q}(\zeta_m) &= \mathbb{Q}(\zeta_{[m,n]})\end{aligned}$$

Definice 9.2.5. Rozšíření K/F se nazývá *cyklické*, jestliže je Galoisovo a jeho Galoisova grupa je cyklická.

9.3 Řešitelná a radikálová rozšíření, Galoisova grupa polynomu, řešitelné grupy, souvislost s vyjadřováním kořenů polynomů v radikálech

Definice 9.3.1. Rozšíření K/F nazveme *jednoduché radikálové*, jestliže existuje $\alpha \in K$ tak, že $K = F(\alpha)$ a $\alpha^n \in F$ pro vhodné $n \in \mathbb{N}$.

Rozšíření K/F nazveme *radikálové*, jestliže existují tělesa $F_0 = F \subseteq F_1 \subseteq \dots \subseteq F_r = K$ tak, že $\forall i \in \{1, \dots, r\}$ je F_i/F_{i-1} jednoduché radikálové.

Definice 9.3.2. Necht F je těleso, $g \in F[x]$ nekonstantní polynom. Řekneme, že polynom g je *řešitelný v radikálech*, jestliže existuje radikálové rozšíření K/F takové, že v $K[x]$ se g rozkládá na lineární činitele.

Definice 9.3.3. Grupa G se nazývá *jednoduchá*, jestliže její jediné normální podgrupy jsou $\{1\}$ a G .

Definice 9.3.4. Necht G je grupa. Posloupnost jejích podgrup

$$G = G_0 \geq G_1 \geq \dots \geq G_r = \{1\}$$

se nazývá

- *normální řada*, jestliže $\forall i = 1, \dots, r$ je $G_i \trianglelefteq G$,
- *subnormální řada*, jestliže $\forall i = 1, \dots, r$ je $G_i \trianglelefteq G_{i-1}$.

Definice 9.3.5. Subnormální řada $G = G_0 \trianglerighteq G_1 \trianglerighteq \dots \trianglerighteq G_r = \{1\}$ grupy G se nazývá *kompoziční řada* grupy G , jestliže pro každé $i = 1, \dots, r$ je G_{i-1}/G_i jednoduchá. Faktorgrupy G_{i-1}/G_i se nazývají *kompoziční faktory*.

Věta 9.3.6. Každá konečná grupa má kompoziční řadu.

Má-li G kompoziční řadu, pak libovolná její normální podgrupa má kompoziční řadu.

Definice 9.3.7. Řekneme, že dvě kompoziční řady téže grupy G jsou *ekvivalentní*, pokud mají stejnou délku r a po případné permutaci mají izomorfní kompoziční faktory.

Definice 9.3.8. Necht G je grupa, $x, y \in G$. Definujeme *komutátor* $[x, y] = xyx^{-1}y^{-1}$. *Komutátorovou podgrupou* G' grupy G rozumíme podgrupu generovanou komutátory, tj.

$$G' = \langle \{[x, y] \mid x, y \in G\} \rangle.$$

Poznámka. Zřejmě $G' = \{1\} \Leftrightarrow G$ je komutativní.

Věta 9.3.9. Necht G je grupa, $N \trianglelefteq G$. Pak G/N je komutativní právě tehdy, když $N \geq G'$.

Definice 9.3.10. Necht G je grupa. Položme $G^{(1)} = G'$ a $G^{(i)} = (G^{(i-1)})'$. Grupa G se nazývá *řešitelná*, jestliže existuje $r \in \mathbb{N}$ takové, že $G^{(r)} = \{1\}$.

Věta 9.3.11. Následující podmínky jsou pro grupu G ekvivalentní

- G je řešitelná,
- G má normální řadu s komutativními faktory,
- G má subnormální řadu s komutativními faktory,

je-li navíc G konečná, pak

- G má subnormální řadu s cyklickými faktory,
- G má subnormální řadu s faktory prvočíselného řádu.

Věta 9.3.12.

- G řešitelná, $H \leq G \Rightarrow H$ řešitelná,
- G řešitelná, $N \trianglelefteq G \Rightarrow G/N$ řešitelná,
- G grupa, $N \trianglelefteq G$, $N, G/N$ řešitelné $\Rightarrow G$ řešitelná,
- G, H řešitelné $\Rightarrow G \times H$ řešitelná.

Věta 9.3.13. Grupa mající kompoziční řadu je řešitelná právě tehdy, když její faktory jsou konečné prvočíselného řádu.

Zejména žádná nekonečná řešitelná grupa nemá kompoziční řadu.

Poznámka.

- Každá konečná grupa lichého řádu je řešitelná.
- Necht p, q jsou prvočísla. Každá grupa řádu $p^c q^d$, kde $c, d \in \mathbb{N}$, je řešitelná.
- Necht G je konečná grupa. Jestliže pro každé $m \in \mathbb{N}$ takové, že $m \mid |G|$, $(m, \frac{|G|}{m}) = 1$ existuje v G prvek řádu m , pak je G řešitelná.
- Konečná grupa G není řešitelná právě tehdy, když existují prvky $x, y, z \in G$ takové, že $xy = z$ a řady prvků x, y, z jsou po dvou nesoudělné.

Věta 9.3.14. Polynom $f(x)$ je řešitelný v radikálech právě tehdy, když je jeho Galoisova grupa řešitelná.

Důsledek 9.3.15. Obecný polynom stupně $n \geq 5$ není řešitelný v radikálech.

Příklad. Uvažme $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. Tento polynom je ireducibilní podle Eisensteinova kritéria pro 3. Buď K rozkladové těleso polynomu f . Snadno se rozmyslí, že f má právě tři reálné kořeny. Jistě $\text{Gal}(K/\mathbb{Q}) \subseteq S_5$. Buď $\alpha \in K$ kořen f , pak $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$, tedy $5 \mid |\text{Gal } K/\mathbb{Q}|$. Galoisova grupa tedy obsahuje prvek řádu 5, navíc obsahuje komplexní konjugovanost. Proto

$$H = \langle (1, 2), (1, 2, 3, 4, 5) \rangle \subseteq \text{Gal}(K/\mathbb{Q}),$$

přitom $H = S_5$. Protože S_5 není řešitelná, není $f(x)$ řešitelný v radikálech.

Kapitola 10

Základy teorie modulů

10.1 Moduly, homomorfismy, základní konstrukce

Definice 10.1.1. Buď $(R, \boxplus, \cdot)$ okruh. *Levým R -modulem* rozumíme komutativní grupu $(M, +)$ spolu s akcí R na M , tj. zobrazením $R \times M \rightarrow M$ (kde obraz (r, m) značíme rm), splňující pro všechna $r, s \in R$ a $m, n \in M$ následující podmínky:

1. $r(m + n) = rm + rn$,
2. $(r \boxplus s)m = rm + sm$,
3. $(r \cdot s)m = r(sm)$,
4. $1_R m = m$.

Akci R na M nazýváme *násobení* prvky z okruhu R . Využíváme navíc konvenci, že násobení má přednost před sčítáním.

Definice 10.1.2. Necht R je okruh a M je levý R modul. *Podmodulem* modulu M rozumíme podgrupu N grupy M , která je uzavřená na násobení prvky z okruhu R , tj. pro všechna $r \in R$ a $n \in N$ je $rn \in N$.

Definice 10.1.3. Necht R je okruh a M, N levé R -moduly.

1. Zobrazení $f: M \rightarrow N$ se nazývá *homomorfismus R -modulů*, jestliže
 - (a) $\forall x, y \in M$ platí $f(x + y) = f(x) + f(y)$,
 - (b) $\forall x \in M, \forall r \in R$ platí $f(rx) = rf(x)$.
2. Homomorfismus R -modulů se nazývá *izomorfismus R -modulů*, jestliže je injektivní i surjektivní. Řekneme, že moduly M, N jsou izomorfní, píšeme $M \cong N$, jestliže existuje izomorfismus R -modulů $f: M \rightarrow N$.
3. Necht $f: M \rightarrow N$ je homomorfismus R -modulů. *Jádrem homomorfismu f* rozumíme množinu $\ker f = \{m \in M \mid f(m) = 0\}$.
4. Necht $f: M \rightarrow N$ je homomorfismus R -modulů. *Obrazem homomorfismu f* rozumíme množinu $\operatorname{im} f = \{n \in N \mid \exists m \in M: f(m) = n\}$. Obraz homomorfismu budeme někdy značit též $f(M)$.

Věta 10.1.4. Buď R okruh, M levý R -modul a N jeho podmodul. Na faktorgrupě M/N lze zavést strukturu R -modulu tak, že definujeme násobení prvky z R předpisem

$$r(x + N) = rx + N \quad \forall r \in R, x + N \in M/N.$$

Kanonická projekce $p: M \rightarrow M/N$ definovaná vztahem $p(x) = x + N$ je homomorfismem R -modulů s jádrem N .

Definice 10.1.5. Modul M/N z předchozí věty se nazývá *faktorový modul*. Homomorfismus p se nazývá *kanonická projekce na faktoromodul*.

Definice 10.1.6. Buď R okruh, M levý R -modul, $N_1, N_2, \dots, N_n$ jeho podmoduly.

1. Součtem (též *vnitřním součtem*) podmodulů $N_1, N_2, \dots, N_n$ rozumíme množinu

$$N_1 + N_2 + \dots + N_n = \{a_1 + a_2 + \dots + a_n \mid a_i \in N_i \text{ pro každé } i = 1, 2, \dots, n\}.$$

2. Nechť $A \subseteq M$ je libovolná podmnožina. Pro $A \neq \emptyset$ definujeme

$$RA = \{r_1 a_1 + r_2 a_2 + \dots + r_m a_m \mid r_i \in R, a_i \in A, m \in \mathbb{N}\},$$

pro $A = \emptyset$ klademe $RA = \{0\}$. Je-li $A = \{a_1, \dots, a_n\}$ konečná množina, píšeme

$$RA = Ra_1 + Ra_2 + \dots + Ra_n.$$

Množina RA je podmodulem modulu M a nazývá se *podmodul generovaný množinou A* . Množinu A nazýváme *množinou generátorů* podmodulu RA . Snadno lze rozmyslet, že RA je nejmenší podmodul obsahující množinu A .

3. Podmodul N se nazývá *konečně generovaný*, jestliže existuje konečná množina $A \subseteq M$ taková, že $N = RA$.
4. Podmodul N se nazývá *cyklický*, jestliže existuje $a \in M$ takové, že $N = Ra$.
5. Je-li podmodul N konečně generovaný, pak existuje $d \in \mathbb{N}_0$ takové, že N je generovaný d prvky, ale už není generovaný žádnými $d - 1$ prvky. Číslo d se nazývá *minimální počet generátorů*.

Definice 10.1.7. Buď R okruh, I neprázdná indexová množina a pro každé $j \in I$ buď M_j levý R -modul.

1. Součinem R -modulů $(M_j, +_j)$ pro $j \in I$ rozumíme modul

$$\prod_{j \in I} M_j,$$

s operacemi definovanými po složkách.

$\prod_{j \in I} M_j$ je množina všech výběrových funkcí $f: I \rightarrow \bigcup_{j \in I} M_j$, $f(j) \in M_j$. Operace sčítání a násobení prvky okruhu z R zavádíme následujícím způsobem. Pro $f, g \in \prod_{j \in I} M_j$, kde $f(j) = a_j$ a $g(j) = b_j$ pro každé $j \in I$, tedy definujeme

$$f + g: I \rightarrow \bigcup_{j \in I} M_j,$$

$$f + g: j \mapsto a_j + b_j$$

a

$$rf: I \rightarrow \bigcup_{j \in I} M_j,$$

$$rf: j \mapsto r \cdot a_j.$$

V případě součinu konečného počtu modulů, tj. $I = \{1, 2, \dots, n\}$ pro nějaké $n \in \mathbb{N}$, budeme standardním způsobem ztotožňovat $f = (a_1, \dots, a_n)$.

2. Příímým součtem R -modulů M_j pro $j \in I$ rozumíme modul

$$\bigoplus_{j \in I} M_j \subseteq \prod_{j \in I} M_j$$

všech prvků majících jen konečně mnoho nenulových složek.

Dostáváme

$$\bigoplus_{j \in I} M_j = \{f: I \rightarrow \bigcup_{j \in I} M_j \mid f(j) \in M_j \text{ a } f(j) \neq 0 \text{ jen pro konečně mnoho } j \in I\}.$$

Je-li tedy I konečná množina, pak $\prod_{j \in I} M_j = \bigoplus_{j \in I} M_j$.

3. Homomorfismus modulů $i_k: M_k \rightarrow \bigoplus_{j \in I} M_j$ (respektive $M_k \rightarrow \prod_{j \in I} M_j$), který posílá $\alpha \in M_k$ na prvek mající na k -té složce α a ostatní složky nulové, nazýváme *kanonickým vnořením* (též *kanonickou injekcí*).

4. Homomorfismus modulů $p_k: \bigoplus_{j \in I} M_j \rightarrow M_k$ (respektive $\prod_{j \in I} M_j \rightarrow M_k$), který posílá každý prvek na jeho k -tou složku, nazýváme *kanonickou projekcí*.

Definice 10.1.8. Necht R je okruh, I neprázdná indexová množina a M, M_i jsou R -moduly pro každé $i \in I$. Necht jsou dále dány homomorfismy R -modulů

$$\varphi_i: M_i \rightarrow M.$$

Příímým součtem homomorfismů φ_i rozumíme homomorfismus

$$\bigoplus_{i \in I} \varphi_i: \bigoplus_{i \in I} M_i \rightarrow M$$

definovaný pro $f \in \bigoplus_{i \in I} M_i$ předpisem

$$\bigoplus_{i \in I} \varphi_i(f) = \sum_{i \in I} \varphi_i(f(i)),$$

což je korektní zápis, neboť v sumě na pravé straně je jen konečně mnoho nenulových sčítanců.

Definice 10.1.9. Buď R okruh. R -modul F se nazývá *volný* nad množinou $A \subseteq F$, jestliže pro každý nenulový prvek $x \in F$ existuje $n \in \mathbb{N}$ a jednoznačně daná n -prvková podmnožina $\{a_1, a_2, \dots, a_n\} \subseteq A$ a jednoznačně dané nenulové prvky $r_1, r_2, \dots, r_n \in R$ takové, že $x = r_1 a_1 + r_2 a_2 + \dots + r_n a_n$. Množina A se nazývá *báze* modulu M .

10.2 Projektivní moduly a krátké exaktní posloupnosti

Definice 10.2.1. Buď R okruh. R -modul P nazýváme *projektivní*, jestliže pro libovolné R -moduly M, N a libovolné homomorfismy $h: M \rightarrow N$ a $f: P \rightarrow N$, kde h je surjektivní, existuje homomorfismus $g: P \rightarrow M$ takový, že $hg = f$, tj. existuje homomorfismus g takový, že diagram

$$\begin{array}{ccc} & P & \\ \exists g \swarrow & & \searrow f \\ M & \xrightarrow{h} & N \end{array}$$

komutuje.

Definice 10.2.2. 1. Řekneme, že posloupnost

$$A \xrightarrow{f} B \xrightarrow{g} C$$

R -modulů (případně grup) a homomorfismů mezi nimi je *exaktní v B* , jestliže $\ker g = \operatorname{im} f$.

2. Posloupnost

$$\cdots \rightarrow X_{n-1} \rightarrow X_n \rightarrow X_{n+1} \rightarrow \cdots$$

se nazývá *exaktní*, jestliže je exaktní ve všech svých členech, kde je tento pojem definován (tj. ve všech členech mezi dvěma homomorfismy).

3. *Krátkou exaktní posloupností* rozumíme exaktní posloupnost tvaru

$$0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0.$$

Věta 10.2.3. Nechť je dán R -modul P . Následující podmínky jsou ekvivalentní:

1. R -modul P je projektivní.
2. Je-li posloupnost $0 \rightarrow A \rightarrow B \rightarrow P \rightarrow 0$ exaktní, pak $A \oplus P \cong B$.
3. R -modul P je přímým sčítancem vhodného volného R -modulu.

10.3 Tenzorový součin

Definice 10.3.1. Buď K komutativní okruh, M, N, L jsou K -moduly. *Bimorfismem* rozumíme zobrazení $f: M \times N \rightarrow L$ splňující

1. $f(a + b, c) = f(a, c) + f(b, c)$,
2. $f(a, c + d) = f(a, c) + f(a, d)$,
3. $f(ra, c) = f(a, rc) = rf(a, c)$.

Modul $M \otimes N$ z něhož vychází univerzální bimorfismus f takový, že

$$\begin{array}{ccc} M \times N & \xrightarrow{f} & M \otimes N \\ & \searrow h & \swarrow \exists! g \\ & L & \end{array}$$

pro libovolný bimorfismus h existuje jediný homomorfismus g takový, že $h = g \circ f$, tj. diagram výše komutuje, nazýváme *tenzorovým součinem* modulů M a N . Tenzorový součin je touto vlastností určen jednoznačně.

Poznámka. Alternativně můžeme definovat tenzorový součin takto

$$M \otimes N = F(M \times N)/A,$$

kde $F(M \times N)$ je volný modul nad množinou $M \times N$ a modul A je generovaný rovnostmi

$$\begin{aligned}(a+b, c) &= (a, c) + (b, c), \\ (ra, c) &= r(a, c), \\ (a, rc) &= r(a, c), \\ (a, c+d) &= (a, c) + (a, d).\end{aligned}$$

Poznámka. Je-li R podokruh okruhu S , pak každý S -modul můžeme chápat též jako R -modul. Tenzorový součin nám umožní učinit opačný postup. Máme-li R -modul M , pak $M \otimes S$ má dokonce strukturu S -modulu (díky tomu, že v druhé složce máme prvky okruhu S). Tato konstrukce zadává v jistém smyslu nejlepší možné rozšíření skalárů.

10.4 Ploché moduly, Lazardova věta

Poznámka. Nechť $h: N_1 \rightarrow N_2$ je surjektivní homomorfismus K -modulů, pak

$$\text{id}_M \otimes h: M \otimes N_1 \rightarrow M \otimes N_2$$

je surjektivní. Podobné tvrzení však obecně neplatí pro injektivní homomorfismy.

Definice 10.4.1. R -modul M se nazývá *plochý*, jestliže $M \otimes _$ zachovává monomorfismy, tj.

$$h: N_1 \hookrightarrow N_2 \quad \Rightarrow \quad \text{id}_M \otimes h: M \otimes N_1 \hookrightarrow M \otimes N_2.$$

Definice 10.4.2. *Direktní uspořádanou množinou* (též usměrněnou množinou) rozumíme uspořádanou množinu, kde libovolná konečná podmnožina má horní zavoru.

Definice 10.4.3. Nechť I je direktní uspořádaná množina, $M_i, i \in I$ jsou R -moduly, $f_{ij}: M_i \rightarrow M_j$ pro $i \leq j$ takové, že

$$f_{jk} \circ f_{ij} = f_{ik} \text{ pro } i \leq j \leq k, \quad f_{ii} = \text{id}_{M_i}.$$

Direktní kolimitou M_i rozumíme modul $\text{colim} M_i$ daný jako univerzální kompatibilní kužel, tj.

$$\begin{array}{ccc} & M_j & \\ & \uparrow & \searrow u_j \\ f_{ij} & & \text{colim} M_i \\ & \uparrow & \nearrow u_i \\ & M_i & \end{array}$$

kde $u_j \circ f_{ij} = u_i$ ($\text{colim} M_i$ je kompatibilní). Pro libovolný kompatibilní kužel $g_i: M_i \rightarrow M$ existuje právě jeden homomorfismus $g: \text{colim} M_i \rightarrow M$ tak, že $gu_i = g_i$ ($\text{colim} M_i$ je univerzální), tj.

$$\begin{array}{ccc} M_i & \xrightarrow{u_i} & \text{colim} M_i \\ & \searrow g_i & \swarrow g \\ & M & \end{array}$$

komutuje.

Věta 10.4.4 (Lazardova). *Ploché R -moduly jsou právě direktní kolimity volných (projektivních) R -modulů.*

10.5 Injektivní moduly a injektivní obal

Definice 10.5.1. R -modul E se nazývá *injektivní*, jestliže pro libovolný injektivní homomorfismus R -modulů $f: M \rightarrow N$ a pro libovolný homomorfismus $g: M \rightarrow E$ existuje homomorfismus $h: N \rightarrow E$ takový, že $hf = g$.

$$\begin{array}{ccc} M & \xrightarrow{f} & N \\ & \searrow g & \swarrow \exists h \\ & E & \end{array}$$

Věta 10.5.2. *Součin injektivních modulů je injektivní. Přímý sčítanec injektivního modulu je injektivní.*

Věta 10.5.3 (Baerovo kritérium). *R -modul E je injektivní právě tehdy, když pro libovolný levý ideál I v R lze libovolný homomorfismus $I \rightarrow E$ rozšířit na R .*

Věta 10.5.4. *Libovolný R -modul lze vnořit do injektivního R -modulu.*

Definice 10.5.5. Řekneme, že podmodul L modulu M je *podstatný*, jestliže $L \cap N \neq 0$ pro libovolný $0 \neq N \subseteq M$. V tomto případě říkáme, že M je *podstatné rozšíření* L .

Lemma 10.5.6. *Jsou-li $L \subseteq N$ a $N \subseteq M$ podstatná rozšíření, pak $L \subseteq M$ je podstatné rozšíření.*

Definice 10.5.7. Buď $L \subseteq M$. Řekneme, že N je *podstatný komplement* L , pokud $L \cap N = 0$ a $L + N \subseteq M$ je podstatný.

Věta 10.5.8. *Buď M podmodul modulu E . Následující podmínky jsou ekvivalentní.*

1. E je maximální podstatné rozšíření,
2. E je injektivní modul a podstatné rozšíření M ,
3. E je minimální injektivní modul obsahující M

navíc libovolný modul M je obsažen v takovém E (tj. takové E existuje).

Definice 10.5.9. Modul E splňující podmínky z předchozí věty se nazývá *injektivní obal* modulu M .

Věta 10.5.10. *Injektivní obal E modulu M je určen jednoznačně až na izomorfismus.*

Věta 10.5.11. *Buď $M \subseteq E$, E injektivní. Pak E je injektivní obal M právě tehdy, když libovolný homomorfismus $f: E \rightarrow E$ takový, že $f|_M = \text{id}_M$, je izomorfismus.*

Kapitola 11

Komutativní algebra a algebraická geometrie

11.1 Rezultant polynomu, polynomy více proměnných

Lemma 11.1.1. *Nechť k je těleso, $f, g \in k[x]$. Polynomy f, g mají společný faktor právě tehdy, když existují nenulové polynomy $k, l \in k[x]$ takové, že*

$$kf + lg = 0,$$

kde navíc $\deg l < \deg f$ a $\deg k < \deg g$.

Definice 11.1.2. Nechť $f, g \in A[x]$ jsou polynomy nad okruhem A , označme

$$f = a_n x^n + \cdots + a_1 x + a_0, \quad g = b_m x^m + \cdots + b_1 x + b_0.$$

Definujeme *Sylvesterovou matici* jako matici $(n+m) \times (n+m)$ pomocí koeficientů f a g :

$$Syl(f, g) = \begin{pmatrix} a_n & 0 & \cdots & 0 & b_m & 0 & \cdots & 0 \\ a_{n-1} & a_n & \cdots & 0 & b_{m-1} & b_m & \cdots & 0 \\ \vdots & a_{n-1} & \ddots & 0 & \vdots & b_{m-1} & \ddots & 0 \\ a_1 & \ddots & \ddots & a_n & b_1 & \ddots & \ddots & b_m \\ a_0 & a_1 & \ddots & a_{n-1} & b_0 & b_1 & \ddots & b_{m-1} \\ 0 & a_0 & \ddots & \vdots & 0 & b_0 & \ddots & \vdots \\ \vdots & & \ddots & a_1 & \vdots & & \ddots & b_1 \\ 0 & 0 & \cdots & a_0 & 0 & 0 & \cdots & b_0 \end{pmatrix}$$

Determinant Sylvesterovy matice nazýváme *rezultantou* polynomů f, g a značíme $Res(f, g)$.

Věta 11.1.3. *Nechť k je těleso, $f, g \in k[x]$ nekonstantní polynomy. Potom f, g mají společný faktor právě tehdy, když $Res(f, g) = 0$.*

Věta 11.1.4. *Nechť $f = a_n(x - \alpha_1) \cdots (x - \alpha_n)$ a $g = b_m(x - \beta_1) \cdots (x - \beta_m)$. Pak*

$$Res(f, g) = a_n^m b_m^n \prod_{i,j} (\alpha_i - \beta_j).$$

Věta 11.1.5. *Nechť $f, g \in k[x_1, \dots, x_r]$. Chápejme f, g jako polynomy v proměnné x_r nad okruhem $k[x_1, \dots, x_{r-1}]$. Jsou-li f, g nekonstantní, pak mají společný faktor s kladným stupněm v proměnné x_r právě tehdy, když $Res(f, g; x_r) = 0$.*

Poznámka. Víme, že $\text{Res}(f, g; x_r) \in k[x_1, \dots, x_{r-1}]$. Kořenem $\text{Res}(f, g; x_r)$ je bod $(p_1, \dots, p_{r-1})$ takový, že buď

- $f(p_1, \dots, p_{r-1}, -)$ a $g(p_1, \dots, p_{r-1}, -)$ mají společný kořen, nebo
- vedoucí koeficient f či g je nulový.

Druhá možnost nenastane, pokud je vedoucí člen f (respektive g) x_r^n (respektive x_r^m), čehož lze změnou souřadnic dosáhnout.

Důsledek 11.1.6. *Nechť je k algebraicky uzavřené těleso. Pokud f, g nemají společný faktor, mají rovnice $f(x, y) = 0$, $g(x, y) = 0$ pouze konečně mnoho společných řešení, a to nejvýše $\deg f \cdot \deg g$.*

11.2 Lokalizace okruhu, noetherovské okruhy a moduly, Hilbertova věta o bázi a Gröbnerova báze

Definice 11.2.1. Nechť R je okruh. Řekneme, že $S \subseteq R$ je *multiplikativní podmnožina*, jestliže

1. $1 \in S$,
2. pro všechna $a, b \in S$ platí $a \cdot b \in S$.

Definice 11.2.2. Nechť R je komutativní okruh, $S \subseteq R$ jeho multiplikativní podmnožina. Na množině $R \times S$ definujeme relaci ekvivalence $\sim$ předpisem

$$(r_1, s_1) \sim (r_2, s_2) \iff \exists s \in S: s(r_1 s_2 - r_2 s_1) = 0.$$

Rozklad $R \times S$ podle ekvivalence $\sim$ budeme značit $S^{-1}R$. Třidu obsahující (r, s) budeme značit $\frac{r}{s}$. Na množině $S^{-1}R$ zavedeme operace $+$ a $\cdot$ následujícím předpisem:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}.$$

Množina $S^{-1}R$ tvoří spolu s těmito operacemi komutativní okruh, který budeme nazývat *lokalizací okruhu R vzhledem k množině S* .

Věta 11.2.3. *Nechť R je netriviální komutativní okruh, S jeho multiplikativní podmnožina neobsahující nulu a $S^{-1}R$ lokalizace okruhu R vzhledem k množině S . Pak zobrazení*

$$\begin{aligned} \lambda: R &\rightarrow S^{-1}R, \\ \lambda: r &\rightarrow \frac{r}{1} \end{aligned}$$

je homomorfismus okruhů. Navíc platí, že

1. λ je injektivní právě tehdy, když S neobsahuje nulu ani žádného dělitele nuly okruhu R .
2. Nechť S neobsahuje nulu ani žádného dělitele nuly, pak λ je surjektivní právě tehdy, když S obsahuje pouze jednotky okruhu R .

Věta 11.2.4. *Buď R komutativní okruh a S jeho multiplikativní podmnožina. Nechť $\varphi: R \rightarrow T$ je homomorfismus okruhů takový, že $\varphi(r) \in T$ je jednotka pro každé $r \in S$. Pak existuje jediný homomorfismus okruhů $\psi: S^{-1}R \rightarrow T$ takový, že $\varphi = \psi \circ \lambda$.*

Poznámka. Speciální případy lokalizace

- $S = \{1, a, a^2, \dots\}$, pak $S^{-1}R$ vznikne z R přidáním inverze k prvku a .
- $S = R \setminus P$, kde P je nějaký prvoideál. Potom $S^{-1}R$ značíme R_P a nazýváme *lokalizací v prvoideálu P* .
- Je-li R obor integrity, pak 0 je prvoideál a R_0 je podílové těleso okruhu R .

Definice 11.2.5. Řekneme, že R -modul M je noetherovský, jestliže neexistuje nekonečná rostoucí posloupnost podmodulů

$$M_0 \subset M_1 \subset \dots \subset M_n \subset \dots$$

Řekneme, že okruh R je noetherovský, je-li noetherovský jako R -modul, tj. neexistuje nekonečná rostoucí posloupnost ideálů.

Lemma 11.2.6. *Nechť R je okruh. Následující podmínky jsou ekvivalentní*

1. R je noetherovský,
2. každý ideál okruhu R je konečně generovaný,
3. každá neprázdná množina ideálů okruhu R obsahuje maximální prvek.

Věta 11.2.7. *Nechť $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$ je krátká exaktní posloupnost R -modulů. Pak M je noetherovský právě tehdy, když M' a M'' jsou noetherovské.*

Důsledek 11.2.8. *Je-li R noetherovský okruh, pak je každý konečně generovaný R -modul noetherovský.*

Věta 11.2.9 (Hilbertova věta o bázi). *Je-li R noetherovský okruh, pak je také $R[x]$ noetherovský.*

Důkaz. Sporem předpokládejme, že existuje ideál I , který není konečně generovaný. Uvažme polynom $0 \neq f_1 \in I$ nejmenšího stupně. Následně uvažme polynom $f_2 \in I \setminus (f_1)$ nejmenšího stupně, pak $f_3 \in I \setminus (f_1, f_2)$ atd. Protože I není konečně generovaný, lze toto vždy udělat. Dostáváme posloupnost

$$(f_1) \subset (f_1, f_2) \subset \dots \subset (f_1, f_2, \dots, f_n) \subset \dots$$

Přitom platí $\deg f_1 \leq \deg f_2 \leq \dots$. Uvažme ideály $J_i \subseteq R$ generované vedoucími koeficienty. Protože R je noetherovský, bude platit $J_{i-1} = J_i$ pro vhodné i . Pak jsme ale schopni nalézt místo polynomu f_i polynom menšího stupně, což je spor s výběrem f_i . Okruh $R[x]$ je proto noetherovský.

Definice 11.2.10. Nechť $I \subseteq k[x_1, \dots, x_r]$ je ideál, nechť je dáno uspořádání na monomech. Vedoucí monom polynomu f značíme $\text{LM } f$. Definujeme

$$\text{LT } I = \{\text{LM } f \mid f \in I\}.$$

Věta 11.2.11 (Gröbnerova báze). *Nechť $I \subseteq k[x_1, \dots, x_r]$ je ideál a $g_1, \dots, g_k \in I$. Jestliže $\text{LT } I = (\text{LM } g_1, \dots, \text{LM } g_k)$, pak $I = (g_1, \dots, g_k)$. Množina prvků $g_1, \dots, g_k \in I$ s touto vlastností vždy existuje a nazývá se Gröbnerova báze.*

Důkaz. Zřejmě $(g_1, \dots, g_k) \subseteq I$. Předpokládejme, že inkluze je ostrá. Existuje tedy $f \in I \setminus (g_1, \dots, g_k)$ nejmenšího stupně. Protože jsme v okruhu polynomů nad tělesem, můžeme pro jednoduchost předpokládat, že všechny polynomy jsou normované. Protože $\text{LM } f \in \text{LT } I$ a $\text{LM } f$ je monom, musí být $\text{LM } f = x^\alpha \text{LM } g_i$. Pak ale

$$f - x^\alpha g_i \in I \setminus \{g_1, \dots, g_k\}$$

je menšího stupně než I . To je spor s minimalitou $\deg f$.

Nechť $\text{LT } I = (h_1, \dots, h_l)$. Pak každý člen h_j je vedoucím členem nějakého polynomu $g_i \in I$. Uvážením všech těchto g_i dostáváme Gröbnerovu bázi.

11.3 Afinní a projektivní variety

Definice 11.3.1. Nechť $S \subseteq k[x_1, \dots, x_n]$ je libovolná podmnožina. *Afinní varietou* rozumíme libovolnou množinu tvaru

$$V(S) = \{x \in \mathbb{A}^n \mid \forall f \in S: f(x) = 0\}.$$

Poznámka. $V(S)$ je množina bodů, kde se nulují všechny polynomy $f \in S$. Zřejmě je-li $I = (S)$ ideál generovaný množinou S , tak

$$V(S) = V(I).$$

Definice 11.3.2. Definujeme

$$I(X) = \{f \in k[x_1, \dots, x_n] \mid \forall x \in X: f(x) = 0\}.$$

Definice 11.3.3. Varieta V se nazývá *ireducibilní*, jestliže nelze psát jako sjednocení $V = V_1 \cup V_2$, kde $V_1 \subset V$, $V_2 \subset V$ jsou afinní variety.

Věta 11.3.4. Varieta V je ireducibilní právě tehdy, když $I(V)$ je prvoideál.

Věta 11.3.5. Každou varietu lze psát jako konečné sjednocení ireducibilních variet.

Definice 11.3.6. Na $\mathbb{A}^n$ definujeme *Zariského topologii* tak, že uzavřené množiny jsou právě afinní variety.

Topologický prostor se nazývá *noetherovský*, jestliže neexistuje nekonečná klesající posloupnost uzavřených množin.

Definice 11.3.7. Buď $f \in k[x_0, \dots, x_n]$ homogenní polynom. Definujeme

$$V(f) = \{(x_0 : x_1 : \dots : x_n) \in \mathbb{P}^n \mid f(x_0, \dots, x_n) = 0\}.$$

Buď $S \subseteq k[x_0, \dots, x_n]$ množina homogenních polynomů. *Projektivní varietou* rozumíme podmnožinu $\mathbb{P}^n$ tvaru

$$V(S) = \bigcap_{f \in S} V(f).$$

11.4 Radikál ideálu, Hilbertova věta o nulách, vztah mezi ideály a algebraickými podmnožinami afinního prostoru, věta o Noetherovské normalizaci

Definice 11.4.1. Nechť $J \subseteq R$ je ideál. *Radikál* ideálu J definujeme předpisem

$$\sqrt{J} = \{f \in R \mid \exists k \in \mathbb{N}: f^k \in J\}.$$

Ideál J se nazývá *radikálový*, jestliže $J = \sqrt{J}$.

Věta 11.4.2 (Hilbertova věta o nulách). *Nechť k je algebraicky uzavřené těleso.*

- *Maximální ideály $k[x_1, \dots, x_n]$ jsou v bijekci s body $\mathbb{A}^n$. Bodu $P = (p_1, \dots, p_n) \in \mathbb{A}^n$ odpovídá ideál $m_P = (x_1 - p_1, \dots, x_n - p_n)$.*
- *Ideál $J \subset k[x_1, \dots, x_n]$ je vlastní právě tehdy, když $V(J) \neq \emptyset$.*
- *Pro ideál $J \subset k[x_1, \dots, x_n]$ platí $IV(J) = \sqrt{J}$.*

Definice 11.4.3. *Nechť A je podokruh okruhu B , pak B nazveme A -algebrou.*

Řekneme, že B je konečná A -algebra, jestliže B je konečně generovaný A -modul.

Řekneme, že B je konečně generovaná A -algebra, jestliže existují $b_1, \dots, b_r \in B$ takové, že $B = A[b_1, \dots, b_r]$, tj. B je generovaný jako okruh okruhem A a jen konečně mnoha dalšími generátory.

Věta 11.4.4 (o noetherovské normalizaci). *Nechť A je konečně generovaná k -algebra. Existuje podalgebra $B \subseteq A$ izomorfní $k[t_1, \dots, t_r]$ taková, že A je konečná B -algebra.*

Poznámka. Věta o noetherovské normalizaci říká

$$\begin{array}{c} A \\ \left| \begin{array}{l} \text{konečné rozšíření} \\ \text{konečně generované} \\ \text{volné rozšíření} \end{array} \right. \\ B \\ \left| \right. \\ k \end{array}$$

Definice 11.4.5. *Nechť B je podokruh okruhu A . Řekneme, že A je integrální nad B , jestliže každý prvek $z \in A$ je kořenem normovaného polynomu $f \in B[x]$.*

Věta 11.4.6. *Nechť je A konečně generovaná B -algebra. Pak A je integrální nad B právě tehdy, když A je konečná B -algebra.*

Věta 11.4.7. *Nechť B je podokruh tělesa A . Nechť A je integrální nad B , pak B je také těleso.*

Kapitola 12

Algebraická topologie

Definice 12.0.1. Zobrazení $f, g: X \rightarrow Y$ se nazývají *homotopická*, píšeme $f \sim g$, jestliže existuje zobrazení $h: X \times I \rightarrow Y$ takové, že

$$h(x, 0) = f(x), \quad h(x, 1) = g(x).$$

Zobrazení h se nazývá *homotopií* mezi f a g .

Prostory X, Y se nazývají homotopicky ekvivalentní, jestliže existují spojitá zobrazení $f: X \rightarrow Y$ a $g: Y \rightarrow X$ tak, že jejich složení jsou identity

Definice 12.0.2. Necht X je topologický prostor, $A \hookrightarrow X$. Řekneme, že A je retraktem X , jestliže existuje spojitě zobrazení

$$r: X \rightarrow A$$

takové, že $ri = \text{id}_A$. Zobrazení r nazýváme *retrakcí*.

12.1 Definice singulárních homologií a kohomologií a jejich aplikace

Definice 12.1.1. Řetězcovým komplexem $\{C_n, \partial\}$ rozumíme posloupnost abelovských grup (či modulů nad okruhem R) a jejich homomorfismů, které indexujeme celými čísly

$$\dots \xrightarrow{\partial_{n+2}} C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \dots$$

tak, že $\partial_{n-1}\partial_n = 0$, to znamená, že $\text{im } \partial_n \subseteq \ker \partial_{n-1}$. Homomorfismus ∂_n se nazývá *hraniční operátor*.

Řetězcovým homomorfismem řetězcových komplexů $(C, \partial^C), (D, \partial^D)$ rozumíme posloupnost homomorfismů abelovských grup (či modulů nad okruhem R) $f_n: C_n \rightarrow D_n$, který komutuje s hraničním operátorem, tj. pro každé n diagram

$$\begin{array}{ccc} C_n & \xrightarrow{\partial_n^C} & C_{n-1} \\ f_n \downarrow & & \downarrow f_{n-1} \\ D_n & \xrightarrow{\partial_n^D} & D_{n-1} \end{array}$$

komutuje.

Definice 12.1.2. Necht (C, ∂) je řetězcový komplex. Jeho n -tou *homologickou grupu* definujeme jako

$$H_n(C) = \ker \partial_n / \operatorname{im} \partial_{n+1}.$$

Prvky $\ker \partial_n = Z_n$ se nazývají *cykly* dimenze n a prvky $\operatorname{im} \partial_{n+1} = B_n$ *hranice* dimenze n .

Komponenta f_n řetězcového homomorfismu zobrazuje cykly na cykly a hranice na hranice. Můžeme proto definovat

$$\begin{aligned} H_n(f): H_n(C) &\rightarrow H_n(D), \\ [c] &\mapsto [f_n(c)]. \end{aligned}$$

Poznámka. Je-li řetězcový komplex exaktní, pak jsou všechny homologické grupy triviální.

Definice 12.1.3. Řekneme, že posloupnost řetězcových homomorfismů $\cdots \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow \cdots$ je *exaktní*, jestliže pro každé $n \in \mathbb{Z}$ je

$$\cdots \rightarrow A_n \xrightarrow{f_n} B_n \xrightarrow{g_n} C_n \rightarrow \cdots$$

exaktní posloupnost abelovských grup.

Věta 12.1.4. Necht $0 \rightarrow A \xrightarrow{i} B \xrightarrow{j} C \rightarrow 0$ je krátká exaktní posloupnost řetězcových komplexů, pak existuje svazující homomorfismus $\delta_*: H_n(C) \rightarrow H_{n-1}(A)$ takový, že

$$\cdots \xrightarrow{\delta_*} H_n(A) \xrightarrow{H_n(i)} H_n(B) \xrightarrow{H_n(j)} H_n(C) \xrightarrow{\delta_*} H_{n-1}(A) \xrightarrow{H_{n-1}(i)} \cdots$$

je exaktní.

Podívejme se nyní na duální pojem k pojmu homologie

Definice 12.1.5. *Kořetězcovým komplexem* (C, δ) rozumíme posloupnost abelovských grup (či modulů) a homomorfismů indexovaných celými čísly

$$\cdots \xrightarrow{\delta^{n-2}} C^{n-1} \xrightarrow{\delta^{n-1}} C^n \xrightarrow{\delta^n} C^{n+1} \xrightarrow{\delta^{n+1}} \cdots$$

takovou, že $\delta^n \delta^{n-1} = 0$. Zobrazení δ se nazývá kohraniční operátor.

Kořetězcovým homomorfismem kořetězcových komplexů (C, δ_C) a (D, δ_D) rozumíme posloupnost homomorfismů abelovských grup (modulů) $f^n: C^n \rightarrow D^n$ tak, že f komutuje s kohraničním operátorem, tj. diagram

$$\begin{array}{ccc} C^n & \xrightarrow{\delta_C^n} & C^{n+1} \\ f^n \downarrow & & \downarrow f^{n+1} \\ D^n & \xrightarrow{\delta_D^n} & D^{n+1} \end{array}$$

komutuje.

Definujeme n -tou kohomologickou grupu kořetězcového komplexu (C, δ) jako

$$H^n(C) = \ker \delta^n / \operatorname{im} \delta^{n-1}.$$

Nášim cílem bude nyní popsat, jak můžeme topologickým prostorům přiřadit homologické grupy. Využívají se dva postupy: *simpliciální homologie* a *singulární homologie*. V tomto textu se budeme zabývat singulárními homologiemi.

Definice 12.1.6. *Standardním n -simplexem rozumíme n -simplex*

$$\Delta^n = \{(t_0, \dots, t_n) \in \mathbb{R}^{n+1} \mid \sum_{i=0}^n t_i = 1, t_i \geq 0\}.$$

Singulárním n -simplexem v topologickém prostoru X rozumíme spojitě zobrazení $\Delta^n \rightarrow X$.

Poznámka. Definujme zobrazení

$$\begin{aligned} j_n: \quad \Delta^{n-1} &\rightarrow \Delta^n \\ (t_0, \dots, t_{n-1}) &\mapsto (t_0, \dots, t_{j-1}, 0, t_j, \dots, t_{n-1}). \end{aligned}$$

Lemma 12.1.7. *Platí*

$$\varepsilon_{n+1}^k \varepsilon_n^j = \varepsilon_{n+1}^{j+1} \varepsilon_n^k$$

pro $k < j$.

Definice 12.1.8. Označme volnou abelovskou grupu generovanou všemi singulárními n -simplexy $C_n(X)$ a definujme hraniční operátor

$$\begin{aligned} \partial_n: C_n &\rightarrow C_{n-1} \\ \sigma &\mapsto \sum_{i=0}^n (-1)^i \sigma \varepsilon_n^i \end{aligned}$$

pro $n \geq 0$. Položme $C_n(X) = 0$ pro $n < 0$.

Řetězcový komplex (C_n, ∂_n) se nazývá *singulární řetězcový komplex* topologického prostoru X . *Singulárními homologickými grupami* rozumíme homologické grupy singulárního řetězcového komplexu.

Definice 12.1.9. Redukované singulární homologie nazveme homologie singulárního řetězcového komplexu doplněného v dimenzi -1 grupou $\mathbb{Z}$. Značíme je $\bar{H}_n(X)$.

Věta 12.1.10. *Jsou-li X, Y homotopicky ekvivalentní prostory, pak $H_n(X) = H_n(Y)$.*

Příklad. *Bud' $n \in \mathbb{N}$, pak platí*

$$\begin{aligned} H_k(S^0) &\cong \begin{cases} \mathbb{Z} \oplus \mathbb{Z} & k = 0 \\ 0 & k > 0 \end{cases} \\ H_k(S^n) &\cong \begin{cases} \mathbb{Z} & k = 0, n \\ 0 & \text{jinak.} \end{cases} \\ H_n(T) &\cong \begin{cases} \mathbb{Z} & n = 0, 2 \\ \mathbb{Z}^2 & n = 1 \\ 0 & \text{jinak} \end{cases} \\ H_k(\mathbb{P}^n) &\cong \begin{cases} \mathbb{Z} & p = 0 \text{ a } n \text{ pro } n \text{ liché} \\ \mathbb{Z}/2\mathbb{Z} & p \text{ liché, } 0 < p < n \\ 0 & \text{jinak} \end{cases} \end{aligned}$$

Uvedme si některé aplikace homologií

Příklad.

- S^{n-1} není retrakt D^n ,

$$\begin{array}{ccc}
 S^{n-1} \hookrightarrow D^n & & \\
 \searrow \text{id} & \downarrow r & \\
 & S^{n-1} &
 \end{array}
 \quad \text{indukuje} \quad
 \begin{array}{ccc}
 \mathbb{Z} = H_{n-1}(S^{n-1}) & \longrightarrow & H_{n-1}(D^n) = 0 \\
 \searrow \text{id} & & \downarrow \\
 & H_{n-1}(S^{n-1}) = \mathbb{Z} &
 \end{array}$$

což je spor.

- Browerova věta o pevném bodu: každé spojitě zobrazení $D^n \rightarrow D^n$ má pevný bod.
Nechť f nemá pevný bod. Pak můžeme definovat zobrazení $D^n \rightarrow \partial D^n$ tak, že bod x pošleme na průsečíky polopřímky danou body $x, f(x)$ s hranicí. Toto zobrazení je prosté a je retrakcí, což je spor.
- $U \subseteq \mathbb{R}^n, V \subseteq \mathbb{R}^m$ jsou otevřené a homeomorfní, pak $n = m$.
- Na S^n existuje nenulové tečné vektorové pole právě tehdy, když n je liché.

Definice 12.1.11. Uvažme dvojici topologických prostorů (X, A) (tj. máme vnoření A do X). Pak $C_n(A) \trianglelefteq C_n(X)$. To nám dává krátkou exaktní posloupnost

$$0 \rightarrow C_n(A) \xrightarrow{i} C_n(X) \xrightarrow{j} C_n(X)/C_n(A) \rightarrow 0.$$

Protože je hraniční operátor $C_n(A)$ restrikce hraničního operátoru $C_n(X)$, můžeme definovat

$$\partial_n: C_n(X)/C_n(A) \rightarrow C_{n-1}(X)/C_{n-1}(A)$$

Tento řetězcový komplex budeme značit $(C(X, A), \partial)$ a jeho homologické grupy $H_n(X, A)$.

12.2 Výpočet pro CW-komplexy

Definice 12.2.1. Buď $f: S^n \rightarrow S^n$. Uvažme $f_*: \bar{H}_n(S^n) \rightarrow H_n(S^n)$

$$f_*(x) = ax, \quad a \in \mathbb{Z}.$$

Číslo a se nazývá *stupeň zobrazení f* .

Věta 12.2.2. *Stupeň zobrazení má následující vlastnosti*

- $\deg \text{id} = 1$
- homotopická zobrazení mají stejný stupeň
- pokud f není surjektivní, má stupeň 0
- $\deg(fg) = \deg f \cdot \deg g$
- $f(x_0, x_1, \dots, x_n) = (-x_0, x_1, \dots, x_n)$ má stupeň -1
- $f(x) = -x$ má stupeň $(-1)^{n+1}$
- pokud f nemá pevný bod, pak $\deg f = (-1)^{n+1}$

Stupeň zobrazení je často výhodné počítat pomocí tzv. lokálního stupně. Jeho definici zde však uvádět nebudeme.

Definice 12.2.3. CW-komplekem rozumíme prostor, který lze obdržet následující konstrukcí.

1. Začneme s diskretním prostorem X^0 . Body X^0 se nazývají *buňky dimenze 0*.
2. Předpokládejme, že jsme zkonstruovali X^{n-1} . Pro každý prvek α indexové množiny J_n uvažme zobrazení

$$f_\alpha: S^{n-1} = \partial D_\alpha^n \rightarrow X^{n-1}$$

a položíme

$$X^n = \bigcup_{\alpha} (X^{n-1} \cup_{f_\alpha} D_\alpha^n).$$

Vnitřky disků D_α^n se nazývají *n-dimenzionální buňky* a značí se e_α^n .

3. Tuto konstrukci lze provádět do nějakého $n \in \mathbb{N}$, pak pokládáme $X = X^n$, ale i do nekonečna, v takovém případě klademe $X = \bigcup_{n \in \mathbb{N}} X^n$.

V druhém případě je topologie na X následující: $A \subseteq X$ je otevřená (resp. uzavřená) je-li $A \cap X^n$ otevřená (resp. uzavřená) v X^n pro všechna n .

Příklad. Sféra S^n je CW-komplex s jednou buňkou e^0 dimenze 0 a jednou buňkou e^n dimenze n spolu s konstantním lepicím zobrazením $f: S^{n-1} \rightarrow e^0$.

Reálný projektivní prostor dimenze n je CW-komplex mající jednu buňku ve všech dimenzích $0, \dots, n$.

Nechť máme daný prostor X u něhož známe jeho strukturu jakožto CW-komplexu. Uvažme následující posloupnost grup a homomorfismů mezi nimi

$$(H_n(X^n, X^{n-1}), d_n),$$

kde

$$d_n: H_n(X^n, X^{n-1}) \xrightarrow{\partial_n} H_n(X^{n-1}) \xrightarrow{j_{n-1}} H_{n-1}(X^{n-1}, X^{n-2})$$

Věta 12.2.4. Je-li X CW-komplex, pak $(H_n(X^n, X^{n-1}), d_n)$ je řetězový komplex a pro jeho homologie platí

$$H_n^{CW}(X) \cong H_n(X).$$

Platí

$$H_k(X^n, X^{n-1}) = \begin{cases} \oplus_{\alpha} \mathbb{Z} & n = k, \\ 0 & n \neq k. \end{cases}$$

Zabývejme se nyní výpočtem d_n .

Nechť e_α^n a e_β^{n-1} jsou buňky dimenze n a $n-1$ CW-komplexu X . Zobrazení d_n je dáno kompozicí

$$H_n(X^n, X^{n-1}) \xrightarrow{\partial_n} H_n(X^{n-1}) \xrightarrow{j_{n-1}} H_{n-1}(X^{n-1}, X^{n-2}),$$

přítom

$$H_n(X^n, X^{n-1}) = \bigoplus_{\alpha} \mathbb{Z}, \quad H_{n-1}(X^{n-1}, X^{n-2}) = \bigoplus_{\beta} \mathbb{Z}.$$

Buňky e_α^n a e_β^{n-1} proto můžeme považovat za generátory těchto grup. Uvažme

$$\varphi_\alpha: \partial D_\alpha^n \rightarrow X^{n-1}$$

lepicí zobrazení pro buňku e_α^n . Pak

$$d_n(e_\alpha^n) = \sum_{\beta} d_{\alpha\beta} e_\beta^{n-1},$$

kde $d_{\alpha\beta}$ je stupeň kompozice

$$S^{n-1} = \partial D_\alpha^n \xrightarrow{\varphi_\alpha} X^{n-1} \rightarrow X^{n-1}/X^{n-2} \rightarrow X^{n-1}/(X^{n-2} \cup \bigcup_{\gamma \neq \beta} e_\gamma^{n-1}) = S^{n-1}.$$

Příklad. Víme, že sféra S^n má jako CW-komplex jednu buňku dimenze 0 a jednu další buňku dimenze n . Řetězcový komplex pro $n \geq 2$ je tvaru

$$0 \rightarrow \cdots \rightarrow 0 \rightarrow \mathbb{Z} \xrightarrow{d_n} 0 \rightarrow \cdots \rightarrow 0 \rightarrow \mathbb{Z} \xrightarrow{d_0} 0$$

$$\quad \quad \quad [e^n] \quad \quad \quad [e^0]$$

zřejmě tedy

$$H_k(S^n) = \begin{cases} \mathbb{Z} & k = n, 0 \\ 0 & \text{jinak} \end{cases}$$

Pro S^0 je komplex tvaru

$$0 \rightarrow \cdots \rightarrow 0 \rightarrow \mathbb{Z} \oplus \mathbb{Z} \rightarrow 0$$

$$\quad \quad \quad [e_a^0, e_b^0]$$

Zřejmě tedy

$$H_k(S^0) = \begin{cases} \mathbb{Z} \oplus \mathbb{Z} & k = 0 \\ 0 & \text{jinak} \end{cases}$$

Zbývá rozebrat případ jednodimenzionální sféry (tj. dvou bodů). Řetězcový komplex je tvaru

$$0 \rightarrow \mathbb{Z} \xrightarrow{d_1} \mathbb{Z} \rightarrow 0,$$

$$\quad \quad [e^1] \quad [e^0]$$

musíme proto určit stupeň zobrazení d_1 . Máme $X^1 = \{e^0\}$ a $X^0 = \{e^0\}$. Stupeň kompozice

$$S^0 \rightarrow X^0 \rightarrow X^0/\emptyset \rightarrow X^0/\emptyset = X^0 \cup \{*\}$$

je nula, vždyť tato kompozice není surjektivní, proto všechny hraniční operátory jsou triviální, tj. $\text{im } d_i = 0$. Odtud

$$H_k(S^1) = \begin{cases} \mathbb{Z} & k = 0, 1, \\ 0 & \text{jinak.} \end{cases}$$

12.3 Homotopické grupy a jejich základní vlastnosti

Definice 12.3.1. Nechť X je topologický prostor s význačným bodem x_0 , $I = [0, 1]$. Nechť $\pi_n(X, x_0)$ homotopické třídy zobrazení

$$(I^n, \partial I^n) \rightarrow (X, x_0)$$

Pro $n \geq 1$ definujeme na $\pi_n(X, x_0) = [(I^n, \partial I^n), (X, x_0)]$ operaci

$$(f + g)(t_1, \dots, t_n) = \begin{cases} f(2t_1, t_2, \dots, t_n) & t_1 \in [0, \frac{1}{2}], \\ g(2t_1 - 1, t_2, \dots, t_n) & t_1 \in [\frac{1}{2}, 1]. \end{cases}$$

Tato operace dává na $\pi_n(X, x_0)$ strukturu grupy. Tuto grupu nazýváme n -tou homotopickou grupou.

Poznámka. Platí

- $\pi_0(X, x_0)$ je množina komponent křivkové souvislosti s význačným prvkem, tj. komponentou obsahující x_0
- $\pi_1(X, x_0)$ grupa jejíž prvky jsou třídy: smyčky začínající (a končící) v x_0 / homotopie, obecně nemusí být komutativní
- $\pi_2(x, x_0)$ je pro $n \geq 2$ komutativní grupa

Definice 12.3.2. *Totálně nespojitou akcií* grupy G na prostoru Y rozumíme akci

$$\begin{aligned} G \times Y &\rightarrow Y \\ (g, y) &\mapsto gy \end{aligned}$$

přítom

- $g_2(g_1)y(g_2g_1)y$ a $1y = y$ (je to akce)
- $\forall y \in Y \exists U \ni y$ tak, že $g_1(U) \cap g_2(U) \neq \emptyset \Rightarrow g_1 = g_2$ (je totálně nespojitá)

Věta 12.3.3. *Nechť Y je křivkově souvislý prostor s totálně nespojitou akcií grupy G , pak*

- $Y \rightarrow Y/G$ je nakrytí
- $G \cong \pi_1(Y/G, p(Y))/\pi_1(Y, y)$.

Příklad. *Uvažme $Y = \mathbb{R}$, $G = \mathbb{Z}$ a akci $(n, x) \mapsto x + n$, pak $\mathbb{R}/\mathbb{Z} \cong S^1$. Věta říká, že*

$$\mathbb{Z} \cong \pi_1(S^1).$$

Pro $Y = \mathbb{R}^2$, $G = \mathbb{Z} \times \mathbb{Z}$ uvažme akci $((n, m), (x, y)) \mapsto ((n + x), (m + y))$. Pak $\mathbb{R}^2/\mathbb{Z} \times \mathbb{Z}$ je torus. Dostáváme, že

$$\pi_1(T) \cong \mathbb{Z} \times \mathbb{Z}.$$

Definice 12.3.4. Prostor X se nazývá n -souvislý, jestliže $\forall x_0 \in X$ je

$$\pi_i(X, x_0) = 0$$

pro $0 \leq i \leq n$.

Věta 12.3.5. *Nechť X je $n - 1$ souvislý prostor, pak pro každé $k \leq n$, $n \geq 2$ platí*

$$H_n(X) = \pi_n(X)$$

a $H_1(X)$ je abelizace $\pi_1(X)$.

Kapitola 13

Teorie grafů

13.1 Orientované a neorientované grafy a jejich reprezentace

Definice 13.1.1. *Neorientovaný grafem* rozumíme uspořádanou dvojici $G = (V, E)$, kde V je množina vrcholů a E je množina hran, tj. množina vybraných dvouprvkových podmnožin množiny vrcholů. Je-li $u, v \in V$ značíme hranu $\{u, v\}$ jen uv . Vrcholy spojené hranou nazýváme *sousední*.

Orientovaný grafem rozumíme uspořádanou dvojici $D = (V, E)$, kde V je množina vrcholů a $E \subseteq V \times V$ je množina hran. Množinu vrcholů grafu G značíme $V(G)$, množinu hran $E(G)$.

Poznámka. Alternativně můžeme definovat hrany neorientovaného grafu jako ireflexivní symetrickou relaci na $V \times V$. V případě orientovaného grafu odstraníme podmínky ireflexivity (umožníme smyčky) a symetrie (hrany nemusí být oboustranné).

Definice 13.1.2. Buď $G = (V, E)$ (neorientovaný) graf.

- *Stupněm vrcholu* $v \in V(G)$ rozumíme počet hran vycházejících z v , značíme $d_G(v)$.
- *Sledem délky* n v grafu G rozumíme posloupnost vrcholů a hran $v_0, e_1, v_1, e_2, v_2, \dots, e_n, v_n$, kde $e_i = v_{i-1}v_i$.
- *Cestou* délky n rozumíme sled délky n , ve kterém se neopakují vrcholy.

Podobně bychom mohli definovat orientovaný sled, cestu (i tah). V případě stupňů rozlišujeme výstupní stupeň $d_D^+(u)$ vrcholu u a vstupní stupeň $d_D^-(u)$.

Poznámka. Další možnost pohledu na graf je tzv. *incidenční model*, kde hrany jsou samostatné objekty (tj. ne relace $R \subseteq V \times V$, množina $E \subseteq 2^V$, kde $e \in E$ má dva prvky či dvojice $E \subseteq V \times V$). Místo relace sousednosti mezi dvojicemi vrcholů pak tento model zavádí relaci *incidence* mezi dvojicí vrchol-hrana.

Poznámka. Zabývejme se nyní reprezentací v počítači. Je-li graf hustý (tj. má-li hodně hran), může být výhodné zadat graf *maticí sousednosti*. Řádek zde reprezentuje výchozí vrchol a sloupec cílový vrchol (na pozici i, j je 1, pokud existuje hrana z i do j , 0 jinak). Snadno můžeme tuto matici upravit tak, aby hodnoty v ní udávaly vzdálenost vrcholů (∞ respektive nějaká maximální konstanta udává neexistenci hrany). Je-li naopak graf řídký, je často výhodné reprezentovat graf seznamem následníků, kde máme seznam vrcholů a ke každému z nich máme seznam sousedních vrcholů. Další možnost je uložení celé relace incidence jakožto incidenční matice.

Podívejme se na časovou složitost některých operací při jednotlivých reprezentacích. Označme $n = |V|$ a $m = |E|$.

Operace	Seznam následníků	Matice sousednosti	Incidenční matice
Ulož graf	$O(m + n)$	$O(n^2)$	$O(mn)$
Přidání vrcholu	$O(1)$	$O(n^2)$	$O(mn)$
Přidání hrany	$O(1)$	$O(1)$	$O(mn)$
Odebrání vrcholu	$O(m)$	$O(n^2)$	$O(mn)$
Odebrání hrany	$O(m)$	$O(1)$	$O(mn)$
Dotaz na sousednost	$O(n)$	$O(1)$	$O(m)$

13.2 Eulerovské a hamiltonovské grafy

Definice 13.2.1. *Tahem* rozumíme sled, ve kterém se neopakují hrany.

Řekneme, že tah je *uzavřený*, jestliže končí ve stejném vrcholu, ve kterém začíná. V opačném případě řekneme, že tah je *otevřený*.

Řekneme, že tah je *eulerovský*, jestliže je uzavřený a obsahuje všechny hrany grafu G .

Graf G se nazývá *eulerovský*, jestliže v něm existuje eulerovský tah.

Věta 13.2.2. *Graf G je eulerovský právě tehdy, když je souvislý a všechny vrcholy v G jsou sudého stupně.*

Důkaz. „ $\Rightarrow$ “: Je-li graf eulerovský, pak je jistě souvislý a každý vrchol má sudý stupeň, neboť uzavřený tah každým průchodem „ubere“ dvě hrany.

„ $\Leftarrow$ “: Uvažme nejdelší uzavřený tah T v grafu G . Sporem ukažme, že T je eulerovský tah. Necht tedy T není eulerovský. Uvažme graf G' takový, že $V(G) = V(G')$ a $E(G') = E(G) \setminus E(T)$. Protože G' má všechny stupně vrcholů sudé, lze libovolně jeho komponenta C (z indukčního předpokladu) nakreslit jedním uzavřeným tahem T_C . Protože G je souvislý, protíná každá komponenta $C \subseteq G'$ tah T v některém vrcholu w . Tah T lze prodloužit o tah T_C (připojíme ho ve vrcholu w). To je spor s maximalitou T .

Důsledek 13.2.3. *Graf G lze nakreslit jedním uzavřeným tahem právě tehdy, když je G souvislý a všechny vrcholy v G až na dva jsou sudého stupně.*

Definice 13.2.4. Necht G je graf.

- *Cesta* se nazývá *hamiltonovská*, jestliže navštíví každý vrchol grafu G právě jednou.
- *Kružnice* se nazývá *hamiltonovská*, jestliže navštíví každý vrchol grafu G právě jednou.
- Graf G se nazývá *hamiltonovský*, jestliže obsahuje hamiltonovskou kružnici.

Věta 13.2.5 (Dirac 1952). *(Neorientovaný) graf G mající alespoň 3 vrcholy je hamiltonovský, jestliže je každý vrchol stupně alespoň $n/2$.*

Věta 13.2.6 (Ore 1960). *Graf G mající alespoň 3 vrcholy je hamiltonovský, jestliže pro každou dvojici nesousedních vrcholů platí, že součet jejich stupňů je alespoň n .*

Poznámka. Na rozdíl od eulerovských grafů je rozhodovací problém, zda je graf hamiltonovský, velice obtížný. Jedná se o NP -úplný problém.

13.3 Míry souvislosti grafu

Definice 13.3.1. Buď G neorientovaný graf. Relace $\sim \subseteq V \times V$ definovaná tak, že $u \sim v \Leftrightarrow$ existuje sled z u do v , je relace ekvivalence. Třídy této relace se nazývají *komponenty souvislosti* grafu G .

Definice 13.3.2. Graf G se nazývá *souvislý*, jestliže je tvořen jedinou komponentou souvislosti, tj. pokud jsou v něm každé dva vrcholy spojené cestou.

Definice 13.3.3. Graf G se nazývá *hranově k -souvislý*, $k > 1$, jestliže zůstane souvislý i po odebrání libovolných (nejvýše) $k - 1$ hran.

Graf G se nazývá *vrcholově k -souvislý*, $k > 1$, jestliže zůstane souvislý i po odebrání libovolných (nejvýše) $k - 1$ vrcholů.

Poznámka. Hovoříme-li o k -souvislém grafu, máme na mysli vrcholově k -souvislý graf. Graf je souvislý právě tehdy, když je 1-souvislý.

Věta 13.3.4. Buď G neorientovaný graf.

- G je hranově k -souvislý $\Leftrightarrow$ mezi libovolnými dvěma vrcholy lze vést alespoň k hranově disjunktních cest (vrcholy mohou být sdílené).
- G je vrcholově k -souvislý $\Leftrightarrow$ mezi libovolnými dvěma vrcholy lze vést alespoň k disjunktních cest (různých až na dva spojované vrcholy).

Definice 13.3.5. Buď D orientovaný graf. Slabě souvislou komponentou rozumíme komponentu souvislosti grafu, který vznikne z D zapomenutím orientace.

Relace $\approx \subseteq V \times V$ definovaná tak, že $u \approx v \Leftrightarrow$ existují orientované sledy z u do v a z v do u , je relace ekvivalence. Třídy této ekvivalence se nazývají *silně souvislé komponenty*.

13.4 Rovinné grafy: Eulerův vzorec a jeho důsledky, obarvení rovinného grafu pěti barvami

Definice 13.4.1. *Rovinným nakreslením* grafu G rozumíme zobrazení, ve kterém jsou vrcholy znázorněny jako různé body v rovině a hrany jako oblouky spojující body svých koncových vrcholů. Přitom hrany se nesmí nikde křížit ani procházet jinými vrcholy než svými koncovými body.

Řekneme, že graf G je rovinný, jestliže existuje jeho rovinné nakreslení.

Definice 13.4.2. *Stěnami* rovinného nakreslení grafu nazýváme (topologicky) souvislé oblasti roviny ohraničené tímto nakreslením.

Definice 13.4.3. *Duální (multi)graf* rovinného nakreslení grafu G získáme tak, že stěny nahradíme vrcholy a hranami spojíme sousedící dvojice stěn.

Věta 13.4.4. Buď G souvislý rovinný graf. Označme f počet stěn nějakého rovinného nakreslení grafu G . Pak

$$|V(G)| + f - E(G) = 2.$$

Důkaz. Označme h počet hran, v počet vrcholů. Důkaz povedeme indukcí k počtu vrcholů. Je-li G strom, pak $h = v - 1$ a stěna je jediná. Platí tedy $v + 1 - (h - 1) = 2$. Uvažme nějaké rovinné nakreslení. Vypuštěním jedné hrany se sníží počet stěn o 1, počet vrcholů se nezmění. Zbytek z indukčního předpokladu.

Důsledek 13.4.5. *Jednoduchý rovinný graf na $v \geq 3$ vrcholech má nejvýše $3v - 6$ hran. Jednoduchý rovinný graf na $v \geq 3$ vrcholech bez trojúhelníků má nejvýše $2v - 4$ hran.*

Důkaz. Můžeme předpokládat, že graf G je souvislý, jinak bychom přidali hrany. Každá stěna má v libovolném nakreslení na obvodu alespoň 3 hrany, každá hrana se započítá do dvou přilehlých stěn. Proto $h \geq \frac{3}{2}f$, tj. $\frac{2}{3}h \geq f$. Víme $v + f - h = 2$, dostáváme

$$2 = v + f - h \leq v + \frac{2}{3}h - h = v - \frac{1}{3}h,$$

tedy $h \leq 3v - 6$.

Podobně druhé tvrzení. Protože graf neobsahuje trojúhelníky, platí $h \geq \frac{4}{2}f$, tj. $\frac{1}{2}h \geq f$. Opět dosadíme

$$2 = v + f - h \leq v + \frac{1}{2}h - h = v - \frac{1}{2}h,$$

tedy $h \leq 2v - 4$.

Důsledek 13.4.6. *Každý jednoduchý rovinný graf obsahuje vrchol stupně nejvýše 5. Každý jednoduchý rovinný graf obsahuje vrchol stupně nejvýše 3.*

Důsledek 13.4.7. K_5 a $K_{3,3}$ nejsou rovinné.

Definice 13.4.8. *Podrozdělením grafu G rozumíme graf, který vznikne z G nrahažením některých hran novými cestami libovolné (kladné) délky.*

Věta 13.4.9. *Graf G je rovinný právě tehdy, když neobsahuje podrozdělení grafů K_5 nebo $K_{3,3}$.*

Věta 13.4.10. *Každý rovinný graf (bez smyček) lze (vrcholově) obarvit čtyřmi barvami.*

Poznámka. Důkaz této věty je velice složitý. K jeho úplnému provedení bylo využito počítače (a doposud není znám žádný jednodušší důkaz). Uvedeme si proto slabší tvrzení, které i dokážeme.

Věta 13.4.11. *Každý rovinný graf (bez smyček) lze (vrcholově) obarvit pěti barvami.*

Důkaz. Indukcí vzhledem k velikosti grafu. Protože G je rovinný, existuje vrchol v stupně nejvýše 5. Uvažme graf G' vzniklý odebráním vrcholu v . Ten lze z indukčního předpokladu obarvit pěti barvami. Pokud všichni sousedi v jsou obarveni dohromady nejvýše čtyřmi barvami, můžeme v obarvit zbývající barvou a jsme hotovi. Předpokládejme tedy, že $v_1, \dots, v_5$ (zapsány v cyklickém pořadí, jak jsou okolo v nakresleny) jsou všechny obarveny postupně barvami $1, 2, \dots, 5$.

Uvažme indukovaný podgraf $G_{1,3} \subseteq G'$ sestávající se jen z těch vrcholů, které jsou obarveny barvami 1 a 3. Pokud vrcholy v_1, v_3 leží v různých komponentách souvislosti, můžeme v komponentě obsahující v_1 zaměnit obarvení a uvolněnou barvu 1 přiřadit vrcholu v . V opačném případě leží v_1, v_3 ve stejné komponentě souvislosti, lze je tedy spojit cestou (na které se střídají barvy 1 a 3).

Podobně uvažme podgraf $G_{2,4} \subseteq G'$. Nyní však nemůže existovat dvoubarevná cesta z v_2 do v_4 , protože by protínala cestu z v_1 do v_3 . Proto v_2, v_4 leží v různých komponentách. V jedné z nich můžeme prohodit obarvení a uvolněnou barvu přiřadit vrcholu v .

13.5 Prohledávání grafu do šířky a do hloubky

Všem vrcholům budeme přiřazovat tři stavy podle toho, zda jsme je už našli a zpracovali či nikoli. Těmi budou

- FRESH - ještě nenalezený
- OPEN - nalezený, ale nezpracovaný
- CLOSED - zpracovaný

Dále si pro každý vrchol v budeme pamatovat

- předchůdce $p[v]$,
- vzdálenost od počátečního vrcholu $d[v]$.

V průběhu celého algoritmu budeme využívat datovou strukturu, která nám bude držet nalezené vrcholy. Touto úschovnou bude v případě

- prohledávání do šířky *fronta*,
- prohledávání do hloubky *zásobník*.

Pro jednoduchost budeme tuto úschovnu nazývat Q . Operace vkládání bude push, vybírání pop (striktně vzato se jedná o operace zásobníku, u fronty se nazývají jinak, nebudeme to však rozlišovat).

VSTUP: Graf G , vrchol s

```
1      foreach( $v \in V(G)$ ){
2          stav[v] = FRESH; d[v] =  $\infty$ ; p[u] = null;
3      }
4      stav[s] = OPEN; d[s] = 0; p[s] = null;
5      Q.push(s);
6      while(!Q.Empty()){
7          u = U.pop();
8          for( $(u,v) \in E(G)$ ){
9              if (stav[v] == FRESH){
10                 stav[v] = OPEN;
11                 d[v] = d[u]+1;
12                 p[v] = u;
13                 Q.push(v);
14             }
15         }
16         stav[u] = CLOSED;
17     }
```

VÝSTUP: Strom procházení zadaný seznamem následníků spolu se vzdáleností od kořene.

Kapitola 14

Grafové algoritmy

14.1 Minimální kostry: algoritmy Kruskala a Prima

V této části budeme značit $m = |E|$ a $n = |V|$.

Definice 14.1.1. *Kostrou* souvislého grafu G rozumíme podgraf grafu G , který je stromem a obsahuje všechny vrcholy grafu G .

Nechť je dána funkce $w: E \rightarrow \mathbb{R}$. *Minimální kostrou* grafu G rozumíme takovou kostru T , pro kterou je hodnota $\sum_{e \in E(T)} w(e)$ minimální.

Kruskalův algoritmus:

1. Seřaď hrany vzestupně podle ohodnocení, tj. $w(e_1) \leq w(e_2) \leq \dots \leq w(e_m)$.
2. Začneme s prázdnou množinou hran T .
3. Pro $i = 1, 2, \dots, m$ vezmeme hranu e_i . Pokud $T \cup \{e_i\}$ nevytvoří kružnici, přidáme ji do T . Jinak ji zahodíme.
4. Na konci množina T obsahuje hrany minimální kostry váženého grafu G, w .

Časová složitost tohoto algoritmu je $O(m \log m) = O(m \log n)$. Čas potřebný na seřazení hran dominuje čas na zbytek algoritmu.

Jarníkův-Primův algoritmus:

1. Vyber náhodný vrchol $v \in G$ a přidej ho do T .
2. V každém kroku vyber nejmenší hranu z T do zbytku grafu a tu přidej.

Časová složitost tohoto algoritmu je $O(m + n \log n)$ při použití Fibonacciho haldy (n extract min, m decrease key operací).

Borůvkův algoritmus je podobný algoritmu Jarníka a Prima, přičemž hledá nejkratší cestu ze všech komponent souvislosti, které doposud našel, současně. V takovém případě potřebuje čas $O(m \log n)$ (po každé fázi klesne počet komponent na nejvýše polovinu, potřebný čas pro každou fázi je $O(m)$).

Borůvkův algoritmus s kontrakcemi, kde po každé fázi vezme komponentu a udělá z ní jeden vrchol, má časovou složitost $O(\min(m \log n, n^2))$.

Kombinací Jarníkova a Borůvkova algoritmu s kontrakcemi (tj. na začátku se provede několik fází Borůvkova algoritmu, byl-li graf řídký, tak se zahustí a pak se využije efektivita Jarníkova algoritmu) obdržíme Tarjanův algoritmus s časovou složitostí $O(m \log \log n)$.

14.2 Nejkratší cesty z jednoho vrcholu: Dijkstrův algoritmus, Bellmanův-Fordův algoritmus

Cílem této části je dát popis algoritmů, které naleznou nejkratší cestu (respektive vzdálenost) z pevně daného vrcholu $s \in G$ do všech ostatních dosažitelných vrcholů $v \in G$. Předpokládejme, že délka hrany je dána funkcí $w: E \rightarrow \mathbb{R}$.

Bellman-Fordův algoritmus: funguje pro libovolné ohodnocení hran. Má-li graf dosažitelný záporný cyklus, algoritmus to rozpozná a skončí. Jinak vypočítá vzdálenost nejkratší cesty z daného vrcholu do všech ostatních dosažitelných vrcholů.

Označme $d[u]$ doposud nejlepší vzdálenost od počátečního vrcholu do vrcholu u . Cílem bude postupně zlepšovat hodnoty $d[u]$.

Jestliže selepší $d[u]$, je nutné přezkoumat, zda pomocí u nemůžeme zlepšit $d[v]$ pro $(u, v) \in E$.

```

Inicializace( $G, s$ );
  for  $v \in V$  {
     $d[v] = \infty$ ;
     $p[v] = \text{null}$ ;
  }
   $d[s] = 0$ ;

Relaxace( $u, v, w$ )
  if ( $d[v] > d[u] + w(u, v)$ ) {
     $d[v] = d[u] + w(u, v)$ ;
     $p[v] = u$ ;
  }

Bellman-Ford( $G, w, s$ )
  for ( $i=1, i < |V|, i++$ )
    foreach ( $(u, v) \in E$ )
      Relaxace( $u, v, w$ );
  foreach ( $(u, v) \in E$ )
    if ( $d[v] > d[u] + w(u, v)$ ) return false;

```

Časová složitost je $O(mn)$.

Dijkstrův algoritmus: vyžaduje nezáporné ohodnocení hran. Jedná se o algoritmus velice podobný *BFS* a *DFS* s tím rozdílem, že nepoužíváme klasickou frontu ani zásobník, ale Fibonacciho haldu, ze které bereme ten nezpracovaný vrchol, který je nejbliž výchozího vrcholu.

Časová složitost je dána $O(m + n \log n)$ (n -insert, n -extract min, m -decrease key).

14.3 Nejkratší cesty mezi všemi dvojicemi vrcholů: nejkratší cesty a násobení matic, Floydův-Warshallův algoritmus

Mějme nyní graf G zadaný maticí sousednosti $W = (w_{ij})$, tj.

$$w_{ij} = \begin{cases} 0 & i = j \\ \text{délka hrany } ij & i \neq j, (i, j) \in E \\ \infty & i \neq j, (i, j) \notin E \end{cases}$$

Označme $\delta(i, j)$ délku nejkratší cesty z i do j . Předpokládejme, že graf neobsahuje záporné cykly.

Algoritmus násobení matic:

Označme $l_{ij}^{(c)}$ minimální délku cesty z i do j , která má nejvýše c hran. Platí

$$l_{ij}^{(0)} = \begin{cases} 0 & i = j \\ \infty & i \neq j \end{cases}$$

$$l_{ij}^{(c)} = \min\{l_{ij}^{(c-1)}, \min_{k \in V} \{l_{ik}^{(c-1)} + z_{kj}\}\} = \min_{k \in V} \{l_{ik}^{(c-1)} + z_{kj}\}$$

Protože nejkratší cesta nemůže mít více než $|V| - 1$ hran, platí $\delta i, j = l_{ij}^{(n-1)}$. Počítáme matice $L^{(1)}, \dots, L^{(n-1)}$.

Nyní popíšeme algoritmus. Jedná se o algoritmus velice podobný algoritmu násobení matic (odtud název algoritmu). Vyjdeme z matice $L^{(1)} = W$ a děláme

$$L^{(1)} \bullet L^{(1)} \bullet \dots \bullet L^{(1)},$$

kde $\bullet$ se počítá jako součin matic s tím rozdílem, že prvek na dané pozici nepočítáme jako součet součinů, ale jako minimum součtů. Protože je tato operace asociativní, můžeme místo „přínásobování“ matice $L^{(1)}$ využít již existující matice $L^{(c)}$ a aplikovat tuto operaci na ni. Získáváme tedy $L^{(1)}, L^{(2)}, L^{(4)}, \dots$. Těchto kroků nám stačí jen $O(\log n)$.

Složitost tohoto algoritmu je $O(n^3 \log n)$.

Warshallův-Floydův algoritmus:

- Nejkratší cesta p z vrcholu i do vrcholu j obsahuje jako svoje vnitřní vrcholy libovolné vrcholy z V , označme je $\{1, 2, \dots, k\}$.
- Vyberme vrchol k cesty p .
- Cesta p se rozpadá na nejkratší cesty z i do k a z k do j . Ani jedna z těchto cest neobsahuje jako vnitřní vrchol k (to by dávalo existenci nekladného cyklu, je-li cyklus délky 0, tak ho můžeme vypustit).
- Algoritmus využívá vztah mezi množinou cest z i do j obsahující vrcholy $\{1, \dots, k\}$ a množinou cest z i do j , jejichž vnitřní vrcholy jsou jen z množiny $\{1, \dots, k-1\}$.

Popíšeme si postup algoritmu:

1. Označme $d_{ij}^{(k)}$ délku nejkratší cesty z i do j s vnitřními vrcholy z množiny $\{1, 2, \dots, k\}$.
2. Platí

$$d_{ij}^{(k)} = \begin{cases} w_{ij} & k = 0 \\ \min\{d_{ij}^{(k-1)}, d_{ik}^{(k-1)} + d_{kj}^{(k-1)}\} & k \geq 1 \end{cases}$$

3. $d_{ij}^{(n)} = \delta i, j$, zvolíme-li vhodné pořadí, můžeme každou z hodnot $d_{ij}^{(k)}$ vypočítat v konstantním z hodnot, které jsme již spočítali dříve (postupně zvyšujeme k)

Časová složitost Warshallova-Floydova algoritmu je $O(n^3)$.

14.4 Maximální toky v sítích: sítě, Fordova-Fulkersonova metoda, maximální párování v bipartitních grafech

Definice 14.4.1. *Sítí* rozumíme čtveřici $S = (G, z, s, w)$, kde G je graf, $z, s \in V(G)$ jsou vrcholy, které nazýváme *zdroj* a *stok*. Funkce $w: E(G) \rightarrow \mathbb{R}^+$ je kladné ohodnocení hran, které nazýváme *kapacitou hran*.

Tokem v síti $S = (G, z, s, w)$ rozumíme funkci $f: E(G) \rightarrow \mathbb{R}_0^+$ splňující

- $\forall e \in E(G): 0 \leq f(e) \leq w(e)$ - respektuje kapacitu hrany,
- $\forall v \in V(G) \setminus \{s, z\}: \sum_{e \rightarrow v} f(e) = \sum_{e \leftarrow v} f(e)$ - zachování substance

Velikostí toku f rozumíme hodnotu $|f| = \sum_{e \leftarrow z} f(e) - \sum_{e \rightarrow z} f(e)$.

Fordův-Fulkersonův algoritmus pro hledání maximálního toku:

Definice 14.4.2. Reziduální síť pro tok f je dána

- Reziduálním grafem $G_f = (V, E_f)$, kde pro každou hranu $e = (u, v) \in E$ obsahuje E_f
 - hranu (u, v) je-li $f(e) < w(e)$,
 - hranu (v, u) , je-li $f(e) > 0$.
- a reziduálními kapacitami c_f

$$w_f(uv) = \begin{cases} w(uv) - f(uv) & uv \in E \\ f(uv) & vu \in E \end{cases}$$

V průběhu algoritmu pak hledáme cestu ze zdroje do stoku v reziduálním grafu. Jakmile takovou cestu najdeme, zvýšíme tok f o tolik, kolik je minimální reziduální kapacita.

Edmonsův-Karpův algoritmus je založen na podobné myšlence, jen cestu v reziduálním grafu berou nejkratší možnou (myšleno co do počtu projitých vrcholů), tj. využívají BFS. Protože se délka této cesty nikdy nezkrátí a navíc je zaručeno, že se po nejvýše m krocích zvýší, musí tento algoritmus skončit.

Časová složitost Edmonsova-Karpova algoritmu je $O(m^2n)$.

Další vylepšení této myšlenky nabízí Dinicův algoritmus. Cílem je v reziduálním grafu nasytit všechny možné cesty současně. Hledá tedy tok v reziduálním grafu takový, že každá cesta ze zdroje do stoku obsahuje plně nasycenou hranu tímto tokem.

Časová složitost Dinicova algoritmu je $O(mn^2)$.

Dalším známým algoritmem, který staví na podobné myšlence je *MPM* algoritmus (též *three Indians algorithm*). Hlavní myšlenkou je plně nasítit všechny vstupní či výstupní hrany určitého vrcholu (s nejmenší kapacitou) v jednom kroku. Díky tomu má tento algoritmus časovou složitost $O(n^3)$.

Definice 14.4.3. Necht G je graf, množinu $M \subseteq E$ nazveme *párováním*, jestliže žádné dvě hrany z M nemají společný vrchol. *Maximálním párováním* rozumíme párování s největší kardinalitou.

Nechť G je bipartitní graf. Můžeme tedy uvážit rozklad množiny jeho vrcholů V na dvě podmnožiny V_1, V_2 , kde mezi libovolnými dvěma vrcholy z téže podmnožiny nevede v G hrana. Přidejme ke G dva vrcholy - z, s . Každé hraně grafu G přidáme orientaci a to tak, aby vedla z V_1 do V_2 . Přidejme hrany ze zdroje do každého vrcholu ve V_1 a hrany do stoku z každého vrcholu ve V_2 . Všem hranám dejme kapacitu 1. Maximální tok zadává maximální párování bipartitního grafu G .

Kapitola 15

Lineární programování

15.1 Úlohy lineárního programování, dualita v lineárním programování

Definice 15.1.1. Buďte b, c reálné vektory, A reálná matice. Úlohu

- $\max\{cx \mid Ax = b, x \geq 0\}$ nazýváme *úlohou lineárního programování ve standardním tvaru*,
- $\max\{cx \mid Ax \leq b, x \geq 0\}$ nazýváme *úlohou lineárního programování v kanonickém tvaru*,

přitom v teorii se často využívá úloha lineárního programování ve tvaru

$$\max\{cx \mid Ax \leq b\}.$$

Funkce cx se nazývá *účelová funkce*, x *přípustné řešení*. *Optimálním řešením* x^* rozumíme takové přípustné řešení, že $cx \leq cx^*$ pro každé přípustné řešení x . Hodnotu cx^* nazýváme *optimální hodnotou* účelové funkce.

Lemma 15.1.2. Všechny úlohy lineárního programování z předchozí definice jsou ekvivalentní.

Definice 15.1.3. Duální úlohou k úloze lineárního programování

- $\max\{cx \mid Ax = b, x \geq 0\}$ rozumíme úlohu

$$\min\{yb \mid yA \geq c\},$$

- $\max\{cx \mid Ax \leq b, x \geq 0\}$ rozumíme úlohu

$$\min\{yb \mid yA \geq c, y \geq 0\},$$

- $\max\{cx \mid Ax \leq b\}$ rozumíme úlohu

$$\min\{yb \mid yA = c, y \geq 0\}.$$

Věta 15.1.4 (Farkasovo lemma). *Soustava lineárních nerovnic $Ax \leq b$ má řešení právě tehdy, když $\forall y \geq 0: yA = 0 \Rightarrow yb \geq 0$.*

Věta 15.1.5 (o dualitě v lineárním programování). *Nechť $\max\{cx \mid Ax \leq b, x \geq 0\}$ a $\min\{yb \mid yA \geq c, y \geq 0\}$ jsou vzájemně duální úlohy lineárního programování. Pak pro všechna přípustná řešení x a y platí $cx \leq yb$. Přitom nastává právě jedna z následujících podmínek*

1. Obě úlohy mají optimální řešení a optimální hodnoty jsou si rovny.
2. Jedna z úloh nemá přípustné řešení a druhá úloha má přípustné řešení, ale nemá optimální řešení kvůli neohraničenosti účelové funkce.
3. Ani jedna úloha nemá přípustné řešení.

15.2 Geometrie polyedrů

Definice 15.2.1. Polyedrem rozumíme množinu tvaru $P = \{x \mid Ax \leq b\}$.

Dimenzí polyedru $P = \{x \mid Ax \leq b\}$ rozumíme dimenzi jeho afinního obalu.

Definice 15.2.2. Necht P je polyedr a c libovolný nenulový vektor takový, že úloha

$$\max\{cx \mid Ax \leq b\}$$

má optimální řešení s optimální hodnotou δ . Afinní nadrovina $\{x \mid cx = \delta\}$ se nazývá *opěrná nadrovina* polyedru P .

Stěnou polyedru P rozumíme sám P nebo jeho průnik s opěrnou nadrovinou.

Věta 15.2.3. Steny polyedru P jsou právě neprázdné množiny tvaru

$$\{x \mid Ax \leq b, A'x = b'\},$$

kde $A'x \leq b'$ je podsystém $Ax \leq b$ (tj. některé nerovnice prohlásíme za rovnice).

Věta 15.2.4. Každá stěna krom P samého je průnikem maximálních stěn.

Každá stěna krom P samého je obsažena ve stěně dimenze o 1 vyšší.

Věta 15.2.5. Buď $P = \{x \mid Ax \leq b\}$ polyedr dimenze n , pak každá minimální stěna je afinním podprostorem dimenze $n - h(A)$ se zaměřením $\{x \mid Ax = 0\}$.

Definice 15.2.6. Polyedr se nazývá *bodovaný*, jestliže $h(A) = n$.

Minimální stěny mají dimenzi 0, nazývají se *vrcholy*.

Stěny dimenze 1 se nazývají *hrany*, jsou to úsečky a polopřímky.

15.3 Simplexová metoda a dopravní problém

Simplexová metoda se používá k řešení úlohy lineárního programování ve standardním tvaru

$$\max\{cx \mid Ax = b, x \geq 0\}.$$

Základní myšlenka:

- Nalézt nějaký vrchol polyedru P
- Postupovat po hranách z vrcholu do vrcholu a přitom zlepšovat účelovou funkci.

Označme hodnotu $h(A) = m$, $A = (a_1, a_2, \dots, a_n)$, tj. a_i je i -tý sloupec matice A , $\bar{x}$ řešení soustavy $Ax = b$. Položme

$$M_{\bar{x}} = \{j \in \{1, 2, \dots, n\} \mid \bar{x}_j \neq 0\}.$$

Vektor $\bar{x}$ nazveme *bazické řešení* soustavy $Ax = b$, jestliže sloupce a_j pro $j \in M_{\bar{x}}$ jsou lineárně nezávislé.

Je-li $\bar{x}$ bazické řešení, kde $|M_{\bar{x}}| < m$, nazveme toto řešení *degenerované*.

Příklad. Uvažme

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Aby mohl být nějaký vektor bazickým řešením, musí mít některou složku nulovou. Snadno získáme dvě možnosti:

$$\begin{aligned} \bar{x} &= (1, 0, 0) \Rightarrow M_{\bar{x}} = \{1\}, \\ \bar{y} &= (0, 1, 1) \Rightarrow M_{\bar{y}} = \{2, 3\} \end{aligned}$$

přičemž jeden nenulový sloupec je jistě lineárně nezávislý a sloupce $(1, 0)^T$ a $(0, 1)^T$ jsou také lineárně nezávislé. Vektory $\bar{x}$, $\bar{y}$ jsou tedy bazická řešení. Přitom $\bar{x}$ je degenerované bazické řešení.

Definice 15.3.1. Přípustným bazickým řešením rozumíme bazické řešení splňující $\bar{x} \in P$.

Lemma 15.3.2. Přípustná bazická řešení jsou právě vrcholy polyedru.

Buď $\bar{x}$ přípustné bazické řešení. Předpokládejme, že $M_{\bar{x}} \subseteq M \subset \{1, 2, \dots, n\}$ tak, že sloupce a_j pro $j \in M$ tvoří bázi m -dimenzionálního vektorového prostoru

$$M = \{\mu_1, \dots, \mu_m\}, \quad A_M = (a_{\mu_1}, \dots, a_{\mu_m})$$

s pevně daným pořadím indexů $\mu_1, \dots, \mu_m$. Zvolme $k \in \{1, 2, \dots, n\} \setminus M$. Uvažme soustavu

$$Ax = b, \quad x_j = 0 \text{ pro } j \notin M \cup \{k\}.$$

Tato soustava má hodnotu $n - 1$. Pokud přidáme předpoklad $x_k \geq 0$, dostáváme polopřímku

$$h = \{x \mid Ax = b, x \geq 0, x_j = 0 \text{ pro } j \notin M \cup \{k\}\},$$

která je stěnou polyedru P . Pokud $\bar{x}$ není degenerované bazické řešení, je h hrana, po které se můžeme posunout k lepšímu řešení.

Příklad (Dopravní problém). Uvažme následující problém

- p zdrojů
- a_i pro $i = 1, \dots, p$ je množství surovin v i -tém zdroji
- q spotřebičů
- b_j pro $j = 1, \dots, q$ je množství suroviny, které máme dodat do j -tého spotřebiče
- c_{ij} cena za dopravu jednotkového množství suroviny z i -tého zdroje do j -tého spotřebiče
- x_{ij} hledané množství dopravené z i -tého zdroje do j -tého spotřebiče

$$\min \sum_{i=1}^p \sum_{j=1}^q c_{ij} x_{ij}$$

$$\text{za podmíněk } \sum_{j=1}^q x_{ij} = a_i \quad \text{pro } i = 1, \dots, p$$

$$\sum_{i=1}^p x_{ij} = b_j \quad \text{pro } j = 1, \dots, q$$

$$x_{ij} \geq 0 \quad \forall i, j$$

přitom předpokládáme, že ze zadání je $a_i, b_j > 0$.

Úloha má přípustné řešení $\Leftrightarrow$ úloha má optimální řešení $\Leftrightarrow \sum_{i=1}^p a_i = \sum_{j=1}^q b_j$.

Kapitola 16

Hry v normální formě

16.1 Hry n hráčů v normální formě: koncepty rovnováhy

Definice 16.1.1. Necht $n \in \mathbb{N}$, $n \geq 2$ a $N = \{1, 2, \dots, n\}$ je množina všech hráčů. Buď $i \in N$.

- Neprázdná množina X_i se nazývá *množina strategií* i -tého hráče.
- Funkce $u_i: \prod_{j \in N} X_j \rightarrow \mathbb{R}$ se nazývá *výherní funkce* i -tého hráče.

Uspořádanou dvojici $G = ((X_i)_{i \in N}, (u_i)_{i \in N})$ nazýváme *hrou* n hráčů *v normální formě*. Prvky množiny $X = \prod_{j \in N} X_j$ nazýváme *situace*.

Poznámka. Abychom se vyhnuli zbytečným technickým detailům, budeme se v dalším vyjadřovat méně formálně, stále však přesně.

Porovnání dvou situací z pohledu daného hráče znamená porovnání hodnot jeho výherní funkce (vyšší = lepší). Porovnání dvou strategií daného hráče v dané situaci znamená, že zafixujeme strategie všech ostatních hráčů a porovnáváme situace, kdy se mění jen dvě strategie daného hráče.

Definice 16.1.2. Řekneme, že strategie $x_i \in X_i$ *dominuje* strategii $y_i \in X_i$, jestliže je alespoň tak dobrá v každé situaci a existuje situace v níž je x_i ostře lepší než y_i .

Strategie $x_i \in X_i$ se nazývá *nedominovaná*, jestliže neexistuje strategie ji dominující.

Řekneme, že situace $x \in X$ *dominuje podle Pareta* situaci $y \in X$, jestliže je x není horší pro žádného hráče než y , přitom pro některého z hráčů je x lepší než y .

Situace $x \in X$ se nazývá *optimální podle Pareta*, jestliže není dominovaná podle Pareta.

Poznámka. Vidíme, že Paretoovo optimum nám nabízí globální pohled na výhry všech hráčů. To je však z hlediska teorie her velice slabý pojem. Chceme se zabývat zejména tím, jak může hráč maximalizovat vlastní zisk bez ohledu na zisky ostatních.

Definice 16.1.3. Situace $x \in X$ se nazývá *rovnovážná podle Nashe*, jestliže se žádnému hráči nevyplatí změnit svou strategii při zachování strategií ostatních hráčů.

Poznámka. Situace v Nashově rovnováze se někdy považují za řešení hry. Jejich výhodou je, že jsou stabilní, tj. jakmile se jednou ustanoví, nikdo nemá důvod strategii měnit. Nevýhodou tohoto konceptu řešení je fakt, že těchto rovnovážných poloh může existovat více a výhry pro jednotlivé hráče se v nich mohou lišit (dokonce mohou být pro všechny zúčastněné vyšší v jedné rovnovážné poloze než v jiné). Nashovo equilibrium navíc nedovoluje žádné dohody mezi jednotlivými hráči, což je při aplikacích poměrně podstatný požadavek.

Definice 16.1.4. Necht $G = ((X, Y), (u, v))$ je hra dvou hráčů v normální formě. Pro tuto hru definujeme *Stackelbergův model* $G' = ((X, Y'), (u', v'))$, kde

$$Y' = \{g: X \rightarrow Y\}, \quad u'(x, g) = u(x, g(x)), \quad v'(x, g) = v(x, g(x)).$$

Řekneme, že situace $(x, g(x)) \in X \times Y$ (respektive $(x, g) \in X \times Y'$) je v *silné Stackelbergově rovnováze*, jestliže

1. $\forall x' \in X: u(x, g(x)) \geq u(x', g(x'))$,
2. $\forall y \in Y: v(x, g(x)) \geq v(x, y)$,
3. $\forall y \in Y: v(x, g(x)) = v(x, y) \Rightarrow u(x, g(x)) \geq u(x, y)$.

Poznámka. Výhodou Stackelbergova equilibria oproti Nashovu je mimo jiné to, že existuje na větší třídě her. Navíc hodnota v každém Stackelbergova equilibriu je pro prvního hráče stejná a vždy alespoň tak dobrá jako při libovolném Nashově equilibriu (pokud toto existuje).

Poznámka. Je-li hra G konečná (tj. množina strategií každého hráče je konečná), pak definujeme tzv. *pravděpodobnostní rozšíření* hry G . Strategiemi je pak pravděpodobnostní rozložení na strategiích původní hry G (tzv. čistých strategiích). Výherní funkce je pak přirozené rozšíření původní výherní funkce (vážený součet přes výhry ze všech situací, které nastaly, kde váhy jsou pravděpodobnosti, s jakou tyto situace nastaly).

Všimněme si, že lze předpokládat, že strategie druhého hráče ve Stackelbergově modelu bude čistá. To často zjednoduší úvahy, které vedou k řešení hry.

16.2 Hry 2 hráčů v normální formě: antagonistické hry, optimální strategie

Definice 16.2.1. Řekneme, že hra G je antagonistická, jestliže $\forall x, y \in X \times Y$ platí

$$u(x) \leq u(y) \Leftrightarrow v(x) \geq v(y).$$

Je-li navíc $u = -v$, pak řekneme, že hra G je s *nulovým součtem*.

Poznámka. Hra je tedy antagonistická, jestliže zvýšení výhry jednoho hráče nastává právě tehdy, když se sníží výhra hráče druhého.

V antagonistických hrách platí, že všechny situace v Nashově equilibriu dávají stejnou výhru všem hráčům.

Definice 16.2.2. Necht $G = ((X, Y), (u, v))$ je hra dvou hráčů v normální formě. *Dolní hodnotu* hry pro prvního hráče definujeme vztahem

$$h_1^- = \sup_{x \in X} \inf_{y \in Y} u(x, y)$$

a *horní hodnotu* hry vztahem

$$h_1^+ = \inf_{y \in Y} \sup_{x \in X} u(x, y).$$

Analogicky pro druhého hráče.

Definice 16.2.3. Strategie $x \in X$ se nazývá *optimální*, jestliže existuje $y \in Y$ takové, že (x, y) je rovnovážná situace (podle Nashe). Analogicky pro druhého hráče.

Věta 16.2.4. *Nechť G je antagonistická hra, (x, y) rovnovážná situace. Pak platí*

$$h_1^- = h_1^+ = u(x, y) = \inf_{y' \in Y} u(x, y') = \sup_{x' \in X} u(x', y).$$

Definice 16.2.5. Strategie $x \in X$ se nazývá *opatrná*, jestliže

$$\inf_{y \in Y} u(x, y) = h_1^-.$$

Poznámka. V každé hře si může hráč ε -zajistit hodnotu h_1^- v tom smyslu, že pro libovolné $\varepsilon > 0$ existuje strategie taková, že ať soupeři zahrají cokoli, jeho výhra bude alespoň $h_1^- - \varepsilon$. Strategie je opatrná, jestliže s její pomocí hráč zajistí dokonce h_1^- .

V případě, že antagonistická hra má Nashovo equilibritum, platí opatrná = optimální.

16.3 Řešení maticových her

Definice 16.3.1. Nechť je dána matice $A = (a_{ij})$ typu $m \times n$. *Maticovou hrou* s maticí A rozumíme hru dvou hráčů s nulovým součtem, kde

- $X = \{1, \dots, m\}$,
- $Y = \{1, \dots, n\}$,
- $u(i, j) = a_{ij} = -v(i, j)$.

V pravděpodobnostním rozšíření je $u(x, y) = x^T A y$.

Věta 16.3.2 (von Neumann). *Pravděpodobnostní rozšíření libovolné maticové hry má rovnovážnou situaci.*

Příklad (Řešení maticových her). *Nechť $A = (a_{ij})$ je matice $m \times n$. Bez újmy na obecnosti můžeme předpokládat, že $A > 0$. V opačném případě bychom přičetli ke všem prvkům matice nějakou konstantu, o kterou se zvýší výhra prvního hráče a po vyřešení hry (strategie zůstanou stejné) tuto hodnotu zase odečteme, abychom získali skutečné výhry prvního hráče. Předpokládáme tedy, že výhra prvního hráče je kladná.*

Nechť $x = (x_1, \dots, x_m)$ je optimální strategie prvního hráče. Pak si tento hráč pomocí x zajistí hodnotu hry v proti jakékoli strategii y druhého hráče, zejména proti každé čisté strategii druhého hráče. To dává soustavu

$$\sum_{i=1}^m a_{ij} x_i \geq v \quad \text{pro } j \in \{1, \dots, n\}.$$

Abychom se zbavili neznámého v na pravé straně, uvažme substituci $t_i = \frac{x_i}{v}$. Protože $v > 0$, můžeme obě strany všech nerovnic vydělit v . Dostáváme

$$\sum_{i=1}^m a_{ij} t_i \geq 1 \quad \text{pro } j \in \{1, \dots, n\}.$$

Přitom platí

$$1 = \sum x_i = \sum v t_i = v \sum t_i.$$

Cílem je nalézt takovou strategii x abychom maximalizovali v . Ekvivalentně se na to můžeme dívat tak, že chceme minimalizovat $\frac{1}{v}$. Přitom

$$\frac{1}{v} = \sum_{t_i}.$$

Dostáváme tedy následující problém lineárního programování:

$$\begin{aligned} \min \quad & t_1 + \dots + t_m \\ \text{za podmínek} \quad & tA = \mathbf{1}, \\ & t \geq 0. \end{aligned}$$

16.4 Neantagonistické hry 2 hráčů: bimaticové hry, teorie užitečnosti, úlohy o dohodě, vyhrožování

Definice 16.4.1. Necht jsou dány matice A, B tvaru $m \times n$. Bimaticovou hrou s maticemi A, B rozumíme hru dvou hráčů, kde

- $X = \{1, \dots, m\}$,
- $Y = \{1, \dots, n\}$,
- $u(i, j) = a_{ij}$,
- $v(i, j) = b_{ij}$.

V pravděpodobnostním rozšíření můžeme psát $u(x, y) = x^T A y$ a $v(x, y) = x^T B y$.

Poznámka. Ekvivalentně můžeme říci, že bimaticové hry jsou právě konečné hry dvou hráčů. Je-li $A = -B$ jedná se vlastně o maticovou hru s maticí A .

Je vidět, že v tomto případě nemusí být hra antagonistická (natož s nulovým součtem).

Necht U je množina událostí, která je uzavřená na formální konvexní kombinace. Na U uvažujeme vzájemně inverzní relace $<, >$ a relaci $\parallel$. Relace $A < B$ chápeme jako dává přednost události B před událostí A . Relaci $\parallel$ že nedáváme přednost žádné události. Necht jsou splněny následující axiomy

1. $\forall A, B \in U$ nastává právě jedna z možností: $A < B, A > B, A \parallel B$.
2. $\parallel$ je relací ekvivalence
3. $<$ je tranzitivní
4. jestliže $A < B \parallel C$, pak $A < C$
jestliže $A \parallel B < C$, pak $A < C$
5. $1 \cdot A + 0 \cdot B = A$
6. $r_1 A_1 + \dots + r_n A_n = r_{\sigma(1)} A_{\sigma(1)} + \dots + r_{\sigma(n)} A_{\sigma(n)}$ pro každou permutaci σ
7. $rA + (1-r)(sB + (1-s)C) = rA + (1-r)sB + (1-r)(1-s)C$
8. $rA + (1-r)A = A$
9. jestliže $A \parallel C$, pak pro $r \in [0, 1]$ a $B \in U$ platí $rA + (1-r)B \parallel rC + (1-r)B$
10. jestliže $A < C$, pak pro $r > 0$ a $B \in U$ platí $rA + (1-r)B < rC + (1-r)B$
11. jestliže $A < B < C$, pak existuje $r \in [0, 1]$ takové, že $rA + (1-r)C \parallel B$

Věta 16.4.2. *Existuje funkce $u: U \rightarrow \mathbb{R}$ taková, že $\forall A, B \in U, r \in [0, 1]$ platí*

- $A < B \Leftrightarrow u(A) < u(B)$,
- $u(rA + (1-r)B) = r \cdot u(A) + (1-r) \cdot u(B)$

Je-li v jiná taková funkce, pak existují $\alpha > 0, \beta \in \mathbb{R}$ taková, že $\forall A \in U$ platí

$$v(A) = \alpha \cdot u(A) + \beta$$

Funkci u nazýváme funkcí užitečnosti.

Definice 16.4.3. *Úlohou o dohodě rozumíme uspořádanou trojici (S, u^*, v^*) , kde $S \subseteq \mathbb{R}^2$ je konvexní a kompaktní množina a $(u^*, v^*) \in S$.*

Poznámka. Úloha o dohodě je vlastně množina všech výher, které mohou dva hráči získat vhodnou kombinací jejich strategií (příčemž nepožadujeme, aby volili strategie nezávisle na sobě), příčemž bod $(u^*, v^*) \in S$ je dvojice výher, kterou si mohou oba hráči samostatně zaručit (tj. hodnoty h_1^- a h_2^-).

Poznámka. Necht D je množina všech úloh o dohodě. Axiomaticky definujeme funkci $\varphi: D \rightarrow \mathbb{R}^2$, která každé úloze o dohodě přiřadí výhry obou hráčů. Dá se ukázat, že existuje jediná. Řešením hry dohodou pak znamená uvážit hru jako hru o dohodě a následně na ni aplikovat tuto funkci. Přitom platí

- Uváží se konvexní obal množiny všech dvojic výher hráčů ve všech situacích a bodu $(h_1^-, h_2^-) = (u^*, v^*)$. Toto je naše množina S .
- Cílem je zlepšit tuto hodnotu pro oba hráče co nejvíce, přitom
 - Pokud není možné se pohnout doprava či nahoru, je (u^*, v^*) řešením
 - Pokud je možné se pohnout jen do jednoho směru, tak se do něj pohneme (co nejdál to jde).
 - Pokud je možné se pohnout doprava i nahoru, tak funkce φ dá bod (u, v) maximalizující $(u - u^*) \cdot (v - v^*)$ na množině S .

Definice 16.4.4. *Uvažujme bimaticovou hru dvou hráčů danou maticemi A, B . Strategie hry $G = ((X^*, Y^*), (u, v))$, kde*

$$(u, v): X^* \times Y^* \rightarrow \mathbb{R}^2, \\ (x, y) \mapsto \varphi(Sx Ay^T, x By^T)$$

pro $S = \text{conv}\{(a_{ij}, b_{ij}) \mid (i, j) \in X \times Y\}$, se nazývají *vyhrožovací strategie*.

Poznámka. Zabýváme-li se vyhrožováním, tak podobně jako v úloze o dohodě povolujeme komunikaci mezi oběma hráči. Intuitivně, každý z hráčů zvolí strategii tak, aby získal pod pohružkou této strategie co nejlepší vyjednávací pozici. Tato strategie nemusí být ani zdaleka optimální. Jakmile si oba své strategie vyloží, řeší výslednou situaci dohodou.

Kapitola 17

Hry ve tvaru charakteristické funkce

Nechť $n \in \mathbb{N}$, $n \geq 2$, $N = \{1, \dots, n\}$.

Definice 17.0.1. Hrou n hráčů ve tvaru charakteristické funkce rozumíme zobrazení

$$v: 2^N \rightarrow \mathbb{R}$$

splňující

1. $v(\emptyset) = 0$ (personálnost),
2. pro libovolné koalice $S, T \subseteq N$ takové $S \cap T = \emptyset$ platí

$$v(S \cup T) \geq v(S) + v(T) \quad \text{superaditivita.}$$

Číslo $v(S)$ nazýváme *výhrou koalice* S .

Poznámka. Hry ve tvaru charakteristické funkce vznikají přirozeně z her v normální formě, když výhru koalice S budeme definovat jako dolní hodnotu hry pro koalici S , tj.

$$v(S) = \sup_{\substack{C \text{ } x_i \in X_i \\ C \text{ } i \in S}} \inf_{\substack{C \text{ } x_i \in X_i \\ C \text{ } i \notin S}} \sum_{i \in S} u_i(x_1, \dots, x_n).$$

Definice 17.0.2. Rozdělení hry v nazýváme libovolné $x \in \mathbb{R}^n$ takové, že

- $\sum_{i=1}^n x_i = v(N)$,
- $\forall i \in N: x_i \geq v(\{i\})$. (V dalším budeme pro přehlednost psát jen $v(i)$.)

Množinu všech rozdělení hry značíme $E(v)$.

Poznámka. Definice rozdělení hry říká, že každý dostane alespoň tolik, co si může zaručit sám, a dohromady si hráči rozdělí vše.

Díky superaditivitě lze očekávat, že všichni hráči vytvoří jedinou koalici a v rámci ní se nějak rozdělí o $v(N)$. Pokud platí

$$\sum_{i \in N} v(i) < v(N)$$

nazveme hru v *podstatnou*. To je právě tehdy, když $|E(v)| > 1$ a otázka, jaké rozdělení mají hráči zvolit, dává smysl.

Definice 17.0.3. Nechť $\emptyset \neq S \subseteq N$. Nechť $x, y \in E(v)$ jsou rozdělení hry v . Řekneme, že x *domínuje pro koalici* S rozdělení y , píšeme $x >_S y$, jestliže

- $\forall i \in S: x_i > y_i$,
- $\sum_{i \in S} x_i \leq v(S)$.

Řekneme, že rozdělení x *dominuje* y , píšeme $x > y$, jestliže existuje koalice S , pro kterou x dominuje y .

Poznámka. Jestliže rozdělení x dominuje pro koalici S rozdělení y , znamená to, že při rozdělení y se koalici S vyplatí „trhnout“ a zisky $v(S)$ si přerozdělit jako je tomu v x , tj. tak, aby každý dostal více.

Rozdělení x tedy dominuje rozdělení y , jestliže pro rozdělení y existuje koalice, které se vyplatí trhnout.

17.1 Jádro a jeho existence, aplikace v ekonomii

Definice 17.1.1. Necht v je hra ve tvaru charakteristické funkce. Množinu všech nedominovaných rozdělení nazýváme *jádrem* a značíme ji $C(v)$.

Věta 17.1.2. Pro libovolnou hru v ve tvaru charakteristické funkce platí

$$C(v) = \{x \in \mathbb{R}^n \mid \forall S \subseteq N: \sum_{i \in S} x_i \geq v(S), \sum_{i \in N} x_i = v(N)\}.$$

Příklad (Přiřazovací hra). Necht $M = \{1, \dots, m\}$ je množina prodejců, $M' = \{m+1, \dots, 2m\}$ množina kupců. Označme $N = M \cup M'$.

- Hráč $i \in M$ vlastní dům, který si cení na a_i .
- Hráč $m+j \in M'$ chce koupit některý z domů, i -tý dům si hodnotí na b_{ij} .
- Necht

$$c_{ij} = v(i, m+j) = \begin{cases} b_{ij} - a_i & b_{ij} > a_i \\ 0 & \text{jinak} \end{cases}$$

Hodnotu c můžeme chápat jako výdělek, kterého lze dosáhnout, pokud se hráči i a $m+j$ dohodnou na obchodu. Výdělek koalice je pak maximum přes veškeré výdělky, které se mohou uskutečnit prodejem a odkupem domů v dané koalici (přitom každý kupec chce koupit jediný dům).

Věta 17.1.3. Přiřazovací (i produkční hra, kterou zde nebudeme uvádět) mají neprázdné jádro.

17.2 Von Neumannovo-Morgensternovo řešení

Definice 17.2.1. Množina $V \subseteq E(v)$ se nazývá *von Neumannovo-Morgensternovo řešení*, jestliže

1. $x, y \in V \Rightarrow x \not> y$,
2. $x \in E(v) \setminus V \Rightarrow \exists y \in V: x < y$.

Poznámka. Von Neumannovo-Morgensternovo řešení V se někdy nazývá *stabilní množina*. První podmínka pak říká, že V je stabilní vnitřně, druhá, že V je stabilní zvnějšku.

17.3 Shapleyho hodnota

Další možné řešení kooperačních her kromě jádra a von Neumannova-Morgensternova řešení nabízí Shapleyho vektor.

Definice 17.3.1. Buď $\mathcal{V}$ množina všech her ve tvaru charakteristické funkce n hráčů. Pro $u, v \in \mathcal{V}$, $\alpha \in \mathbb{R}^+$ a permutaci π množiny N definujeme

- $(u + v)(S) = u(S) + v(S)$,
- $(\alpha u)(S) = \alpha \cdot u(S)$,
- $(\pi u)(S) = u(\pi^{-1}S)$.

Hráč i se nazývá *podstatný*, jestliže existuje koalice S , $i \notin S$ taková, že $v(S \cup \{i\}) > v(S) + v(i)$. V opačném případě hovoříme o *balvanu*. Definujme funkci

$$\begin{aligned} \varphi: \mathcal{V} &\rightarrow \mathbb{R}^n \\ \varphi: v &\mapsto (\varphi_1[v], \dots, \varphi_n[v]). \end{aligned}$$

pomocí axiomů:

1. $\varphi_i[u + v] = \varphi_i[u] + \varphi_i[v]$,
2. $\varphi_i[\alpha u] = \alpha \varphi_i[u]$,
3. $\varphi_i[\pi u] = \varphi_{\pi^{-1}(i)}[u]$,
4. pro libovolnou množinu obsahující všechny podstatné hráče je $\sum_{i \in S} \varphi_i[u] = u(S)$.

Věta 17.3.2. *Existuje jediná funkce φ splňující tyto axiomy a je tvaru*

$$\varphi_i[v] = \sum_{i \in T \subseteq N} \frac{(|T| - 1)! \cdot (n - |T|)!}{n!} \cdot (v(T) - v(T \setminus \{i\})).$$