

ALGEBRA II PRO INFORMATIKY

OBSAH

1. Booleovy okruhy	1
2. Dělitelnost v komutativních monoidech s krácením	3
3. Obory hlavních ideálů	6
4. Okruhy polynomů	9
5. Kořenová nadtělesa	13
6. Minimální polynomy algebraických prvků	16
7. Rozkladová nadtělesa a algebraický uzávěr	18
8. Úvod do Galoisovy teorie	20
9. Abelova-Ruffiniho věta	23
10. Konečná tělesa po druhé	26
11. Ireducibilní rozklad polynomů	29
12. Volné algebry	32
13. Variety algeber	33

Přednáška Algebra II navazuje na přednášku Algebra I, která proběhla v zimním semestru. Jejím cílem je především prohloubit znalosti o komutativních okruzích včetně úvodu do Galoisovy teorie a strukturální teorie konečných těles. Poslední dvě přednášky budou věnovány základům univerzální algebry.

1. BOOLEOVY OKRUHY

V následující kapitole aplikujeme znalosti komutativních okruhů získané minulý semestr pro algebraický popis Booleových algeber. Podstatou úvahy je pozorování, že každou Booleovu algebru lze chápat jako jistý komutativní okruh. Pro konečné Booleovy algebry tak získáme popis všech kongruencí i podalgeber.

Definice. O okruhu $R(+, \cdot, -, 0, 1)$ řekneme, že je *Booleův*, je-li to komutativní okruh a pro každé $r \in R$ platí, že $r \cdot r = r$ a $r + r = 0$.

Příklad 1.1. Algebra $\mathcal{P}(X)(\div, \cap, \text{Id}_{\mathcal{P}(X)}, \emptyset, X)$, kde \div značí symetrickou diferenci, je pro každou neprázdnou množinu X Booleův okruh. Je-li $Y \subseteq X$, potom je zjevně $\mathcal{P}(Y)$ ideálem okruhu $\mathcal{P}(X)(\div, \cap, \text{Id}_{\mathcal{P}(X)}, \emptyset, X)$. Je-li naopak I ideál, všimněme si, že je uzavřen na konečnou sjednocení svých prvků. Díky indukčnímu argumentu nám stačí ověřit, že $A \cup B \in I$ pro každé $A, B \in I$. Ovšem $A \cup B = (A \div B) \div (A \cap B) \in I$, protože $A \div B, A \cap B \in I$.

Uvažujme X konečnou množinu a buď I ideál. Pak je I konečný, a proto $Y = \bigcup I \in I$. Tudíž $I = \mathcal{P}(Y) = Y \cap \mathcal{P}(X)$ a v okruhu $\mathcal{P}(X)(\div, \cap, \text{Id}_{\mathcal{P}(X)}, \emptyset, X)$ jsou všechny ideály hlavní.

Věta 1.2. (1) Necht' $\mathcal{S}_A = S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ je Booleova algebra. Definujeme-li na S binární operaci $+$ předpisem $a + b = (a \wedge b') \vee (a' \wedge b)$, pak $\mathcal{S}_0 = S(+, \wedge, \text{Id}_S, \mathbf{0}, \mathbf{1})$ je Booleův okruh. Navíc P je podalgebra resp. ρ kongruence \mathcal{S}_A , právě když je P podalgebra resp. ρ kongruence \mathcal{S}_0 .

(2) Necht' $\mathcal{S}_0 = S(+, \cdot, -, 0, 1)$ je Booleův okruh. Definujeme-li na S binární operaci \vee předpisem $a \vee b = a + b + a \cdot b$ a unární operaci $'$ předpisem $a' = 1 + a$, pak $\mathcal{S}_A = S(\vee, \cdot, 0, 1, ')$ je Booleova algebra. Navíc P je podokruh resp. ρ kongruence \mathcal{S}_0 , právě když je P podalgebra resp. ρ kongruence \mathcal{S}_A .

Důkaz. Nejprve si všimněme, že jakmile oběma směry složíme konstrukci operací Booleova okruhu a Booleovy algebry, dostaneme se k původní struktuře. Označíme-li $\tilde{\vee}$ spojení na Booleově algebře definovaný pomocí operací Booleova okruhu a operace na Booleově okruhu jsou naopak definovány pomocí struktury původní Booleovy algebry spočítáme

$$\begin{aligned} a \tilde{\vee} b &= a + b + a \cdot b = (a \wedge b') \vee (a' \wedge b) + a \wedge b = \\ &= (((a \wedge b') \vee (a' \wedge b)) \wedge [a' \vee b']) \vee (((a' \vee b) \wedge (a \vee b')) \wedge [a \wedge b]) = \\ &= (a' \wedge b) \vee (a \wedge b') \vee (a \wedge b) \vee (a \wedge b) = a \vee b. \end{aligned}$$

Výpočet pro komplement je snadný a podobně jako v předchozí úvaze, označíme-li $\tilde{+}$ sčítání na Booleově okruhu definované pomocí operací Booleovy algebry, dostaneme:

$$\begin{aligned} a \tilde{+} b &= (a \wedge b') \vee (a' \wedge b) = a \cdot (1 + b) + (1 + a) \cdot b + a \cdot (1 + b) \cdot (1 + a) \cdot b \\ &= a + a \cdot b + b + a \cdot b + a \cdot b + a \cdot a \cdot b + a \cdot b \cdot b + a \cdot b \cdot a \cdot b = a + b. \end{aligned}$$

Proto stačí, abychom u obou ekvivalence ztotožňující podalgebry a kongruence dokázali jen přímou implikaci.

(1) Přímou z definice vidíme, že jsou operace $+$ resp. \wedge komutativní s neutrálními prvky $\mathbf{0}$ resp. $\mathbf{1}$. Dále \wedge je asociativní, $a \wedge a = a$ a $a + a = (a \wedge a') \vee (a' \wedge a) = \mathbf{0} \vee \mathbf{0} = \mathbf{0}$, tedy každý prvek $a \in S$ je sám k sobě opačný. Zbývá ověřit asociativitu operace $+$ a distributivitu \vee vzhledem k $+$. Vezměme libovolné $a, b, c \in S$. Potom díky distributivitě Booleovy algebry

$$\begin{aligned} (a + b) + c &= (((a \wedge b') \vee (a' \wedge b)) \wedge c') \vee ((a' \vee b) \wedge (a \vee b') \wedge c) = \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge a \wedge c) \vee (a' \wedge b' \wedge c) \vee (b \wedge a \wedge c) \vee (b \wedge b' \wedge c) = \\ &= (a \wedge b' \wedge c') \vee (a' \wedge b \wedge c') \vee (a' \wedge b' \wedge c) \vee (b \wedge a \wedge c). \end{aligned}$$

Protože $a + (b + c) = (c + b) + a$, dostáváme z předchozího výpočtu

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

Konečně

$$\begin{aligned} a \wedge c + b \wedge c &= (a \wedge c \wedge (b' \vee c')) \vee ((a' \vee c') \wedge b \wedge c) = \\ &= (a \wedge c \wedge b') \vee (a' \wedge b \wedge c) = [(a \wedge b') \vee (a' \wedge b)] \wedge c = (a + b) \wedge c. \end{aligned}$$

Vezměme nyní podalgebry P a kongruenci ρ Booleovy algebry $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$. Potom pro každé $a, b \in P$ a $(c_i, d_i) \in \rho$, $i = 1, 2$ máme $a', b', a + b = (a \wedge b') \vee (a' \wedge b) \in P$ a podobně (c'_i, d'_i) , $(c_1 \wedge c'_2, d_1 \wedge d'_2)$, $(c'_1 \wedge c_2, d'_1 \wedge d_2)$, $(c_1 + c_2, d_1 + d_2) \in \rho$. Uzavřenost a slučitelnost s dalšími operacemi je zřejmá.

(2) Dokážeme, že je $S(\cdot, \vee)$ distributivní svaz. Zvolme libovolně $a, b, c \in S$. Komutativita \cdot je zaručena předpoklady a komutativita \vee plyne okamžitě z definice. Dále $a \cdot a = a$ podle předpokladu a $a \vee a = a + a + a \cdot a = 0 + a = a$. Asociativita operace \cdot opět plyne z předpokladu, že $S(+, \cdot, -, 0, 1)$ je (Booleův) okruh a

$a \vee (b \vee c) = a + (b + c + b \cdot c) + a \cdot (b + c + b \cdot c) = a + b + c + a \cdot b + a \cdot c + b \cdot c + a \cdot b \cdot c = (a \vee b) \vee c$.
Dále ověříme axiom (S4):

$$a \vee (b \cdot a) = a + b \cdot a + a \cdot b \cdot a = a + a \cdot b + a \cdot b = a,$$

$$a \cdot (b \vee a) = a \cdot (b + a + b \cdot a) = a \cdot b + a \cdot a + a \cdot b \cdot a = a.$$

Zbývá ověřit jednu distributivitu:

$$a \cdot (b \vee c) = a \cdot (b + c + b \cdot c) = a \cdot b + a \cdot c + a \cdot b \cdot c = (a \cdot b) \vee (a \cdot c).$$

Konečně $a \vee 0 = a \cdot 1 = a$, $a \vee a' = a + (1 + a) + a \cdot (1 + a) = 1 + a + a \cdot a = 1$ a $a \cdot a' = a \cdot (1 + a) = a + a = 0$, tedy $S(\vee, \cdot, 0, 1, ')$ je Booleova algebra.

Vezmeme-li nyní podalgebru a kongruenci Booleova okruhu $S(+, \cdot, -, 0, 1)$, potom díky tomu, že jsou nové operace definovány výlučně pomocí operací původních, stejně přímočarou argumentací jako v (1) dokazuje, že se jedná o podalgebru a kongruenci příslušné Booleovy algebry $S(\vee, \cdot, 0, 1, ')$. \square

Důsledek 1.3. *Svaz všech kongruencí konečné Booleovy algebry $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ je izomorfní svazu všech podmnožin $\mathcal{P}(A)(\cap, \cup)$, kde A je množina všech atomů S .*

Důkaz. Podle Věty 4.13 je Booleova algebra $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ izomorfní Booleově algebře $\mathcal{P}(A)(\cup, \cap, \emptyset, A, ')$ a díky popisu kongruencí okruhu z minulého semestru stačí popsat svaz ideálů příslušného Booleova okruhu $\mathcal{P}(A)(\div, \cap, \text{Id}_{\mathcal{P}(A)}, \emptyset, A)$. V příkladu 1.1 jsme zjistili, že ideály jsou právě tvaru $\mathcal{P}(Y)$ pro $Y \in \mathcal{P}(A)$. Konečně snadno nahlédneme, že $\mathcal{P}(Y) \vee \mathcal{P}(Z) = \mathcal{P}(Y \cup Z)$ a $\mathcal{P}(Y) \wedge \mathcal{P}(Z) = \mathcal{P}(Y \cap Z)$, tedy svaz ideálů (a tedy i svaz kongruencí původní Booleovy algebry) je izomorfní svazu $\mathcal{P}(A)(\cap, \cup)$. \square

Příklad 1.4. (1) Bud' $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ konečná Booleova algebra. Víme, že je S izomorfní potenční Booleově algebře nad množinou všech atomů A . To mimo jiné znamená, že $|S| = |\mathcal{P}(A)| = 2^{|A|}$. Podle 1.3 existuje na $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, ')$ právě $2^{|A|} = |S|$ kongruencí.

(2) Bud' X konečná množina a $\mathcal{P}(X)(\cup, \cap, \emptyset, X, ')$ Booleova algebra všech podmnožin množiny X a uvažujme na ní nějakou kongruenci ρ . Tato kongruence je podle 1.2 kongruencí na okruhu $\mathcal{P}(X)(\div, \cap, \text{Id}_{\mathcal{P}(X)}, \emptyset, X)$. Označme $Y = \bigcup [\emptyset]_{\rho}$. Využijeme-li popis kongruencí na okruzích pomocí ideálů a připomeneme, že podle 1.1 je ideál $[\emptyset]_{\rho} = \mathcal{P}(Y)$, vidíme, že $(A, B) \in \rho$, právě když $A \div B \subseteq Y$.

Cvičení:

- (1) Popište všechny podalgebry konečné Booleovy algebry.
- (2) Je faktor Booleova okruhu (Booleovy algebry) opět Booleův okruh (Booleova algebra)?
- (3) Najděte nekonečnou Booleovu algebra, která nemá žádné atomy.

2. DĚLITELNOST V KOMUTATIVNÍCH MONOIDECH S KRÁCENÍM

Všimněme si, že definitorická podmínka Booleova okruhu $a \cdot a = a$ Booleova okruhu je ekvivalentní podmínce $(1 - a) \cdot a = 0$. To znamená, že Booleův okruh obsahující více než prvky 0 a 1 má netriviální dělitele nuly a není tedy oborem. V následujících několika kapitolách se budeme zabývat obecnou dělitelností, které je zajímavá právě nad obory, tedy nad zcela jiným typem komutativního okruhu než tvoří Booleovy okruhy.

Nejprve prozkoumáme základní pojmy, které známe z kontextu dělitelnosti v přirozených číslech.

Definice. Řekneme, že $S(\cdot)$ je *komutativní monoid s krácením*, je-li $S(\cdot)$ monoid s komutativní operací \cdot splňující pro každé $a, b, c \in S$ podmínku $a \cdot c = b \cdot c \Rightarrow a = b$.

Příklad 2.1. (1) $\mathbb{N}(\cdot)$ a $\mathbb{Z} \setminus \{0\}(\cdot)$ jsou zřejmě komutativní monoidy s krácením.

(2) Je-li $R(+, \cdot, -, 0, 1)$ obor, pak je $R \setminus \{0\}(\cdot)$ komutativní monoid s krácením. Vezmeme-li totiž prvky $a, b, c \in R \setminus \{0\}$, pro něž $a \cdot c = b \cdot c$, potom díky distributivitě dostáváme $0 = a \cdot c - b \cdot c = (a - b) \cdot c$, a proto $a - b = 0$.

Poznamenejme, že komutativní monoid s krácením $R \setminus \{0\}(\cdot)$ oboru $R(+, \cdot, -, 0, 1)$ bude v následujícím nejvýznamnějším příkladem tohoto pojmu.

Definice. Bud' $S(\cdot)$ komutativní monoid s krácením (nebo $S(+, \cdot, -, 0, 1)$ obor) a necht' $a, b \in S$. Řekneme, že a *dělí* b (píšeme $a|b$), pokud existuje takové $c \in S$, že $b = a \cdot c$. Řekneme že a je *asociován s* b (píšeme $a||b$), pokud $a|b$ a zároveň $b|a$.

Všimněme si, že prvek komutativního monoidu s krácením je asociován s 1, právě když je invertibilní.

Poznámka 2.2. Bud' $R(+, \cdot, -, 0, 1)$ obor. Pak $a|b$ právě když $bR \subseteq aR$ a $a||b$ právě když $bR = aR$.

Důkaz. Jestliže $b = a \cdot r$ pro $r \in R$, pak $b \in aR$ a proto $bs \in aR$ pro každé $s \in R$.

Platí-li $bR \subseteq aR$, pak i $b = b1 \in aR$, proto $a|b$.

Druhou ekvivalenci dostaneme dvojím použitím první ekvivalence právě dokázaného kritéria. \square

Poznámka 2.3. Necht' $S(\cdot)$ je komutativní monoid s krácením.

- (1) Pro každé $a, b \in S$ existuje nejvýše jeden takový prvek $c \in S$, že $a = b \cdot c$.
- (2) Necht' $a, b \in S$. Pak $a||b$ právě tehdy, když existuje invertibilní prvek $u \in S$ tak, že $a = b \cdot u$.
- (3) $||$ je kongruence na $S(\cdot)$.
- (4) $S/||(\cdot)$ je komutativní monoid s krácením a relace dělení na něm tvoří uspořádání.

Důkaz. (1) Jestliže $(a =)b \cdot c_0 = b \cdot c_1$, pak stačí krátit hodnotou b , abychom dostali $c_0 = c_1$.

(2) Pro dvojici asociovaných prvků $a||b$ existuje dvojice prvků $u, v \in S$, pro něž $a = b \cdot u$ a $b = a \cdot v$. Dosadíme-li do prvního vztahu za b , máme $a = a \cdot v \cdot u$, a krátíme-li prvkem a dostáváme, že $1 = v \cdot u$, tj. u a v jsou vzájemně inverzní.

Naopak je-li $a = b \cdot u$ pro invertibilní $u \in S$, je $b = a \cdot u^{-1}$, tedy $a|b$ i $b|a$.

(3) Zřejmě je $||$ reflexivní a symetrická relace. Jestliže $a|b$ a $b|c$, existují x a y , pro něž $b = a \cdot x$ a $c = b \cdot y$, proto $c = a \cdot (x \cdot y)$, tedy $a|c$ a odtud vidíme, že relace $|$ i $||$ jsou ekvivalence. Mějme $a_0||b_0$ a $a_1||b_1$. Pak podle (2) existují invertibilní prvky u_0, u_1 pro které $a_i = b_i \cdot u_i$, kde $i = 1, 2$. Nyní $a_0 \cdot a_1 = (b_0 \cdot b_1) \cdot (u_0 \cdot u_1)$, kde $u_0 \cdot u_1$ je opět invertibilní prvek. Tedy $(a_0 \cdot a_1)||b_0 \cdot b_1$ podle (2).

(4) Je zřejmé, že $S/||(\cdot)$ je komutativní monoid. Mějme $[a]_{||} \cdot [b]_{||} = [a]_{||} \cdot [c]_{||}$, potom $[a \cdot b]_{||} = [a \cdot c]_{||}$, tedy podle (2) existuje invertibilní prvek $u \in S$, pro který $a \cdot b = a \cdot c \cdot u$. Nyní můžeme krátit, tudíž $b = c \cdot u$ a opětovným použitím (2) máme $[b]_{||} = [c]_{||}$.

Uvážíme-li, že reflexivita relace "dělí" na faktorovém monoidu plyne okamžitě z definice faktorové operace, zbývá ověřit tranzitivitu a slabou antisymetrii. Nechť $[a]_{\parallel} \cdot [x]_{\parallel} = [b]_{\parallel}$ a $[b]_{\parallel} \cdot [y]_{\parallel} = [c]_{\parallel}$. Potom existují takové invertibilní prvky u a v , pro něž $a \cdot x \cdot u = b$ a $b \cdot y \cdot v = c$, a proto $(a \cdot x \cdot y) \cdot (u \cdot v) = a \cdot x \cdot u \cdot y \cdot v = c$. Protože $u \cdot v$ je invertibilní prvek dokázali jsme, že $[a]_{\parallel} \cdot [x \cdot y]_{\parallel} = [c]_{\parallel}$. Konečně jestliže $[a]_{\parallel} \cdot [x]_{\parallel} = [b]_{\parallel}$ a $[b]_{\parallel} \cdot [y]_{\parallel} = [a]_{\parallel}$, pak máme invertibilní w , pro které $a \cdot x \cdot y \cdot w = a$, tedy $x \cdot y \cdot w = 1$ a x (stejně jako y) je invertibilní prvek. Tím jsme ověřili, že $[a]_{\parallel} = [b]_{\parallel}$. \square

Příklad 2.4. Komutativní monoidy $\mathbb{N}(\cdot)$ a $\mathbb{Z} \setminus \{0\} / \parallel (\cdot)$ jsou izomorfní.

Definice. Bud' $S(\cdot)$ komutativní monoid s krácením (nebo $S(+, \cdot, -, 0, 1)$ obor) a necht' $a, b, c, a_1, \dots, a_n \in S$. Prvek c nazveme *největší společný dělitel prvků* a_1, \dots, a_n (píšeme $NSD(a_1, \dots, a_n)$), jestliže c/a_i pro všechna i , a každý prvek $d \in S$, který dělí všechna a_i , dělí i prvek c . Prvek c nazveme *ireducibilním* prvkem, jestliže c není invertibilní (ani nulový v oboru) a $c = a \cdot b \Rightarrow c \parallel a$ nebo $c \parallel b$. Prvek c nazveme *prvočinitelem*, jestliže c není invertibilní (ani nulový) a $c/a \cdot b \Rightarrow c/a$ nebo c/b .

Poznamenejme, že každé prvočíslo je určitě ireducibilní prvek v oboru celých čísel.

Poznámka 2.5. Necht' $S(\cdot)$ je komutativní monoid s krácením a $a, b, c, d, e \in S$.

- (1) Necht' d je $\text{GCD}(a, b)$ a e je $\text{GCD}(a \cdot c, b \cdot c)$. Potom $(d \cdot c) \parallel e$
- (2) Necht' 1 je $\text{GCD}(a, b)$ a $a/b \cdot c$. Existuje-li $\text{GCD}(a \cdot c, b \cdot c)$, pak a/c .

Důkaz. (1) Protože dc/ac , dc/bc a e je $\text{GCD}(a \cdot c, b \cdot c)$, dc/e , tj. existuje u , pro něž $e = dcu$. To znamená, že dcu/ac a dcu/bc a krátíme-li du/a a du/b , a proto du/d , tudíž $u \parallel 1$ a $(d \cdot c) \parallel e$ podle 2.3.

(2) Necht' e je $\text{GCD}(a \cdot c, b \cdot c)$, pak je $(1 \cdot c) \parallel e$ podle (1), tedy c je $\text{GCD}(a \cdot c, b \cdot c)$. Protože je a společný dělitel $b \cdot c$, $a \cdot c$, dostáváme, že a/c . \square

Věta 2.6. Mějme $S(\cdot)$ komutativní monoid s krácením. Potom je každý prvočinitel ireducibilní. Pokud navíc pro každé $a, b \in S$ existuje $NSD(a, b)$ pak je každý ireducibilní prvek prvočinitelem.

Důkaz. Je-li p prvočinitel a $p = a \cdot b$, pak $p/a \cdot b$, a/p , b/p a platí, že p/a (tedy $p \parallel a$) nebo p/b (tedy $p \parallel b$).

Předpokládejme, že je p ireducibilní, p dělí součin $a \cdot b$ a nedělí prvek a . Protože existuje $\text{GCD}(p, a)$, který není asociován s prvkem p , plyne z ireducibility p , že 1 je $\text{GCD}(p, a)$. Navíc $p/a \cdot b$ a existuje $\text{GCD}(p \cdot b, a \cdot b)$, proto podle 2.5(2) p/b . \square

Příklad 2.7. Uvažujme podokruh $\mathbb{Z}[\sqrt{5}] = \{a + \sqrt{5}b \mid a, b \in \mathbb{Z}\}$ okruhu reálných čísel. Zřejmě se jedná o obor, tedy $\mathbb{Z}[\sqrt{5}] \setminus \{0\}(\cdot)$ je komutativního monoidu s krácením. Lze ukázat, že prvky 2 , $\sqrt{5} + 1$ a $\sqrt{5} - 1$ jsou ireducibilní, ale nejde o prvočinitele, protože $2/4 = (\sqrt{5} + 1) \cdot (\sqrt{5} - 1)$, ale 2 nedělí $\sqrt{5} + 1$, ani $\sqrt{5} - 1$ (podobně pro $\sqrt{5} + 1$ a $\sqrt{5} - 1$).

Cvičení:

- (1) Dokažte, že jsou dva největší společní dělitelé týchž prvků asociovány.
- (2) Popište prvočinitele okruhu reálných polynomů a okruhu komplexních polynomů.

- (3) Dokažte, že v UFD existují největší společní dělitele každé dvojice prvků.

3. OBORY HLAVNÍCH IDEÁLŮ

V Příkladu 2.1 jsme si všimli, že důležitým příkladem komutativního monoidu s krácením je monoid nenulových prvků oboru. Nyní omezíme svou pozornost na obory hlavních ideálů, pro něž díky Větě 2.6 nahlédneme, že jejich prvočinitele a ireducibilní prvky splývají. Pro obory hlavních ideálů se nám proto podaří zobecnit Základní větu aritmetiky. Na závěr kapitoly se soustředíme na obory umožňující algoritmické získání největšího společného dělitele prvků.

Definice. Řekneme, že je R *obor hlavních ideálů*, jestliže je každý jeho ideál hlavní.

Řekneme, že obor R je *UFD* (nebo Gaussův), splňuje-li dvě podmínky:

- (1) pro každý nenulový neinvertibilní prvek $a \in R$ existují ireducibilní prvky $p_1, \dots, p_n \in R \setminus \{0\}$, pro něž $a = p_1 \cdots p_n$
- (2) je-li navíc $a = q_1 \cdots q_k$ pro ireducibilní prvky q_1, \dots, q_k , pak $n = k$ a existuje bijekce σ tak, že $p_i \parallel q_{\sigma(i)}$ pro všechna $i = 1, \dots, n$.

Poznámka 3.1. *Bud' $R(+, \cdot, -, 0, 1)$ obor hlavních ideálů a $a_1, \dots, a_n \in R$. Pak existují prvky u_1, \dots, u_n tak, že $\sum_{i=1}^n a_i \cdot u_i$ je NSD(a_1, \dots, a_n).*

Důkaz. Snadno nahlédneme, že množina $I = \{\sum_{i=1}^n a_i u_i \mid u_i \in R\}$ je ideál oboru hlavních ideálů R , tedy existuje prvek $c \in I$, pro něžž $cR = I$. Protože $a_i R \subseteq cR$, je c společný dělitel a_1, \dots, a_n a zvolíme-li jiného společného dělitele d těchto prvků, dostáváme, že $cR = I \subseteq dR$, tedy $d \mid c$. \square

Následující tvrzení vyslovíme ještě v obecném kontextu komutativních monoidů s krácením.

Poznámka 3.2. *Nechť je každý ireducibilní prvek komutativního monoidu s krácením $S(\cdot)$ prvočinitelem a nechť $p_1, \dots, p_r, q_1, \dots, q_s \in S$ jsou ireducibilní prvky takové, že $p_1 \cdot p_2 \cdots p_r \parallel q_1 \cdot q_2 \cdots q_s$. Potom $r = s$ a existuje taková bijekce σ , že $p_i \parallel q_{\sigma(i)}$ pro všechna $i = 1, \dots, r$.*

Důkaz. Tvrzení dokážeme indukcí podle r . Jestliže $r = 1$ máme $p_1 = u \cdot q_1 \cdot q_2 \cdots q_s$ pro nějaký invertibilní prvek u podle 2.3(2) a protože je p_1 ireducibilní máme podle stejného tvrzení $s = 1$ (ostatní q_i by musely být invertibilní, což je v rozporu s definicí ireducibilního prvku).

Nechť tvrzení platí pro $r - 1$. Protože $p_r \mid q_1 \cdot q_2 \cdots q_s$, najdeme indukčním rozšířením definice prvočinitele takové $i \leq s$, pro které $p_r \mid q_i$, bez újmy na obecnosti můžeme předpokládat, že $i = s$. Z ireducibility prvků p_r i q_s plyne, že jsou nutné asociovány, proto můžeme krátit a dostaneme $p_1 \cdot p_2 \cdots p_{r-1} \parallel q_1 \cdot q_2 \cdots q_{s-1}$. Nyní podle indukčního předpokladu $r - 1 = s - 1$ a dostáváme hledanou permutaci σ na množině $\{1, \dots, r - 1\}$, kterou dodefinujeme $\sigma(r) = r$. \square

Věta 3.3. *Bud' $R(+, \cdot, -, 0, 1)$ obor hlavních ideálů. Pak platí:*

- (1) *Každý ireducibilní prvek $R(+, \cdot, -, 0, 1)$ je prvočinitelem.*
- (2) *$R(+, \cdot, -, 0, 1)$ je UFD.*

Důkaz. (1) Podle 3.1 jsou splněny předpoklady 2.6, které implikují závěr.

(2) Díky (1) a 3.2 platí jednoznačnost, zbývá tedy dokázat existenci ireducibilního rozkladu.

Předpokládejme ke sporu, že nějaký neinvertibilní prvek $a \in R$ nemá ireducibilní rozklad (tj. neexistuje posloupnost ireducibilních prvků c_1, \dots, c_k , pro které $a = c_1 \cdot \dots \cdot c_k$), a budeme induktivně vytvářet takovou posloupnost prvků a_i a b_i , že a_i nemá ireducibilní rozklad b_i není invertibilní a $a_i = a_{i+1}b_{i+1}$. Nejprve položíme $a_0 = a$.

Jestliže a_i nemá ireducibilní rozklad a není invertibilní, musí existovat dva neinvertibilní prvky x a y , z nichž aspoň jeden, například x , nemá ireducibilní rozklad a $a_i = x \cdot y$ (kdyby ho měly oba, tvořil by jejich součin ireducibilní rozklad a_i). Stačí tedy položit $a_{i+1} = x$ a $b_{i+1} = y$.

Nyní z 2.2 a 2.3 plyne, že $a_i R \subset a_{i+1} R$ a $a_i R \neq a_{i+1} R$. Snadno nahlédneme, že je $I = \bigcup_i a_i R$ ideál, který je podle předpokladu hlavní, tj. existuje takové $c \in I$, že $cR = I$. Protože $c \in a_i R$ pro dostatečně velké i , dostáváme, že $cR \subseteq a_i R \subset a_{i+1} R \subseteq cR$, tedy $cR = a_{i+1} R$, což je spor. \square

Poznamenejme, že Základní věta aritmetiky dokázaná minulý semestr je jednoduchým důsledkem předchozí věty použité na obor celých čísel. Konkrétně, protože je okruh $\mathbb{Z}(+, \cdot, -, 0, 1)$ obor hlavních ideálů, existují v monoidech $\mathbb{N} \setminus \{0\}(\cdot)$ a $\mathbb{Z} \setminus \{0\}(\cdot)$ největší společní dělitelé a zřejmě existují rozklady na ireducibilní prvky, tedy jsou v \mathbb{N} ireducibilní rozklady určeny až na pořadí jednoznačně, v \mathbb{Z} jsou jednoznačné až na pořadí a znaménko.

Definice. Bud' $R(+, \cdot, -, 0, 1)$ obor. Řekneme, že R je *eukleidovský obor*, existuje-li zobrazení $\nu : R \rightarrow \mathbb{N}_0 \cup \{-1\}$ (tzv. *eukleidovská funkce*) splňující pro každé $a, b \in R$, $b \neq 0$ podmínky:

- (1) jestliže a/b , pak $\nu(a) \leq \nu(b)$,
- (2) existuje $q, r \in R$ takové, že $a = b \cdot q + r$ a $\nu(r) < \nu(b)$.

Příklad 3.4. (1) Okruh celých čísel je eukleidovským oborem s eukleidovskou funkcí absolutní hodnotou $|\cdot|$. První podmínka definice platí zřejmě, druhá plyne z toho, že i v celých čísel umíme dělit se zbytkem.

(2) Pripomeňme

Algoritmus dělení se zbytkem

VSTUP: $a, b \in R[x]$, vedoucí koeficient b je invertibilní

VÝSTUP: $q, r \in R[x]$, pro které $a = q \cdot b + r$, $\deg r < \deg b$

0. $m := \deg b$; $n := \deg a - m$;
1. if $n < 0$ then return $0, a$ else $r := a$;
2. for $i := n$ downto 0 do $\{q_i := r_{i+m} b_m^{-1}; r := r - q_i x^i b\}$
3. return $\sum_i q_i x^i, r$.

Nyní snadno si rozmyslíme, že funkce, která každému polynomu s koeficienty v tělese přiřadí jeho stupeň splňuje podmínky eukleidovské funkce, proto je obor polynomů nad tělesem eukleidovským oborem.

(3) Podokruh $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (tzv. Gaussova celá čísla) okruhu komplexních čísel je eukleidovským oborem s eukleidovskou funkcí $\nu(a + bi) = a^2 + b^2$. Pripomeňme, že $|c_1 \cdot c_2| = |c_1| \cdot |c_2|$ pro každou dvojici komplexních čísel c_1 a c_2 , proto $\nu(\alpha \cdot \beta) = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 = \nu(\alpha) \cdot \nu(\beta)$ pro všechna $\alpha, \beta \in \mathbb{Z}[i]$. Jestliže α/β a $\beta \neq 0$, existuje $\gamma \in \mathbb{Z}[i]$, pro které $\alpha \cdot \gamma = \beta$, proto $\nu(\beta) = \nu(\alpha \cdot \gamma) = \nu(\alpha) \cdot \nu(\gamma) \geq \nu(\alpha)$, neboť $\nu(\gamma) \geq 0$.

Chceme-li vydělit se zbytkem Gaussovo celé číslo α nenulovým číslem β , najdeme nejprve komplexní $x + iy = \frac{\alpha}{\beta}$ a poté vezmeme taková $x_0, y_0 \in \mathbb{Z}$, pro která $|x -$

$x_0| \leq \frac{1}{2}$ a $|y - y_0| \leq \frac{1}{2}$. Položíme-li $\gamma = x_0 + iy_0$ a $\delta = \alpha - \beta \cdot \gamma$, pak vidíme, že $\frac{\delta}{\beta} = \frac{\alpha}{\beta} - \gamma = x - x_0 + i(y - y_0)$, tudíž $\frac{|\delta|^2}{|\beta|^2} = (x - x_0)^2 + (y - y_0)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$, proto $\nu(\delta) \leq \frac{\nu(\beta)}{2} < \nu(\beta)$.

(4) Podokruh $\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\}$ okruhu reálných čísel je eukleidovským oborem s eukleidovskou funkcí $\nu(a + b\sqrt{2}) = |a^2 - 2b^2|$. Důkaz toho, že je ν eukleidovská norma plyne podobně jako v (2) z faktu, že $\nu(\alpha \cdot \beta) = \nu(\alpha) \cdot \nu(\beta)$.

Následující důkaz je analogický důkazu, že každá podgrupa cyklické grupy je cyklická.

Věta 3.5. Každý eukleidovský obor je oborem hlavních ideálů.

Důkaz. Mějme $R(+, \cdot, -, 0, 1)$ eukleidovský obor s eukleidovskou funkcí $\nu : R \rightarrow \mathbb{N}_0 \cup \{-1\}$ a vezměme libovolný nenulový ideál I . V ideálu I zvolíme nenulový prvek a s minimální hodnotou $\nu(a)$. Zřejmě $aR \subseteq I$. Necht' $i \in I$. Pak podle definice existuje $q, r \in R$ takové, že $i = a \cdot q + r$ a $\nu(r) < \nu(a)$. Protože $r = i - a \cdot q \in I$ a $\nu(a)$ bylo minimální, je nutně $r = 0$ a $aR = I$. Protože nulový ideál $\{0\} = 0R$ je vždy hlavním ideálem, ukázali jsme, že všechny ideály eukleidovského oboru jsou hlavní. \square

Speciálně nyní víme, že pro komutativní těleso $T(+, \cdot, -, 0, 1)$ je $T[x]$ dle 3.4(2) eukleidovský obor s eukleidovskou funkcí danou stupněm polynomů, tedy jde podle právě dokázané věty o obor hlavních ideálů.

Příklad 3.6. (1) Okruh $\mathbb{Z}[x]$ polynomů s celočíselnými koeficienty není oborem hlavních ideálů, protože ideál $x\mathbb{Z}[x] + 2\mathbb{Z}[x] = \{\sum_i p_i x^i \mid 2/p_0\}$ není hlavní. Podle 3.5 tedy nejde o eukleidovský okruh.

(2) Protože v $\mathbb{Z}[\sqrt{5}] = \{a + \sqrt{5}b \mid a, b \in \mathbb{Z}\}$ nesplývají podle 2.7 ireducibilní prvky a prvočinitele, nejde podle 3.3 obor hlavních ideálů, tedy ani o eukleidovský okruh.

Poznamenejme, že je možné dokázat (i elementárními prostředky), že je okruh $\mathbb{Z}[\frac{1+\sqrt{19}i}{2}] = \{a + \frac{1+\sqrt{19}i}{2}b \mid a, b \in \mathbb{Z}\}$ obor hlavních ideálů, který není eukleidovský.

Věta 3.7. Máme-li $R(+, \cdot, -, 0, 1)$ eukleidovským obor s eukleidovskou funkcí ν a $a_0, a_1 \in R \setminus \{0\}$, pak funguje správně obecný

Eukleidův algoritmus

VSTUP: $a_0, a_1 \in R \setminus \{0\}$

VÝSTUP: $\text{GCD}(a_0, a_1)$, x, y , pro které $x_n \cdot a_0 + y_n \cdot a_1 = \text{GCD}(a_0, a_1)$.

0. $(u_0, u_1) := (1, 0)$; $(v_0, v_1) := (0, 1)$; $i := 1$

1. while $a_i \neq 0$ do {zvol $a_{i+1}, q_i \in R$ taková, že $a_{i-1} = a_i \cdot q_i + a_{i+1}$ a $\nu(a_{i+1}) < \nu(a_i)$; $x_{i+1} := x_{i-1} - x_i \cdot q_i$; $y_{i+1} := y_{i-1} - y_i \cdot q_i$; $i := i + 1$ }

2. return $a_{i-1}, x_{i-1}, y_{i-1}$.

Důkaz. Tvrzení 3.5 a 3.1 říkají, že největší společní dělitel všech dvojic prvků eukleidovského oboru existují. Protože a_n je $\text{GCD}(a_{n-1}, a_n)$, stačí dokázat, že prvky c a d jsou asociované pro každé $0 < i < n$, kde c je $\text{GCD}(a_{i-1}, a_i)$ a d je $\text{GCD}(a_i, a_{i+1})$. Protože c/a_i a $c/a_{i+1} = a_{i-1} - a_i \cdot q_i$ dostáváme z definice největšího společného dělitele že c/d . Podobně d/a_i a $d/a_{i-1} = a_i \cdot q_i + a_{i+1}$, tedy d/c .

Platnost formule $a_i = x_i \cdot a_0 + y_i \cdot a_1$ dokážeme indukcí podle i , Triviálně tvrzení platí pro $i = 0, 1$. Nyní stačí dosadit do výrazu $a_{i+1} = a_i \cdot q_i - a_{i-1}$ hodnoty $a_i = x_i \cdot a_0 + y_i \cdot a_1$ a $a_{i-1} = x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1$, abychom dostali

$$a_{i+1} = (x_i \cdot a_0 + y_i \cdot a_1) \cdot q_i - x_{i-1} \cdot a_0 + y_{i-1} \cdot a_1 =$$

$$= (x_{i-1} - x_i \cdot q_i) \cdot a_0 + (y_{i-1} - y_i \cdot q_i) \cdot a_1 = x_{i+1} \cdot a_0 + y_{i+1} \cdot a_1.$$

□

Příklad 3.8. Najdeme v $\mathbb{Z}[i](+, \cdot, -, 0, 1)$ Eukleidovým algoritmem největší společný dělitel prvků $a_0 = 6 - 7i$ a $a_1 = 7 + i$.

Nejprve spočítáme $\frac{6-7i}{7+i} = \frac{(6-7i)(7-i)}{(7+i)(7-i)} = \frac{35}{50} - \frac{55}{50}i$, tedy $q_1 = 1 - i$ a $a_2 = a_0 - q_1 \cdot a_1 = 6 - 7i - (1 - i)(7 + i) = -2 - i$. V dalším kroku počítáme $\frac{7+i}{-2-i} = \frac{(7+i)(-2+i)}{(-2-i)(-2+i)} = -\frac{15}{5} + \frac{5}{5}i = -3 + i$, tedy vidíme, že $q_2 = -3 + i$ a že a_2/a_1 . Zjistili jsme, že $-2 - i$ je největší společný dělitel prvků $6 - 7i$ a $7 + i$ a $-2 - i = (6 - 7i) + (-1 + i)(7 + i)$.

Cvičení:

- (1) Dokažte, že jsou dva největší společní dělitelé těchto prvků asociovány.
- (2) Popište prvočinitele okruhu reálných polynomů a okruhu komplexních polynomů.
- (3) Dokažte, že v UFD existují největší společní dělitelé každé dvojice prvků.

4. OKRUHY POLYNOMŮ

Nejprve si uvědomíme, že známou definici polynomů nad okruhem můžeme nahlédnout velmi obecným (a velmi algebraickým) pohledem:

Vezměme okruh $R(+, \cdot, -, 0, 1)$ a monoid $M(\cdot)$ s neutrálním prvkem e a položme $R[M] = \{p : M \rightarrow R \mid \{m \mid p(m) \neq 0\} \text{ je konečné}\}$. Prvek $p \in R[M]$ budeme zapisovat také ve tvaru $\sum_{m \in M} p(m) \cdot m$. Na $R[M]$ definujme binární operace $+$ a \cdot , unární operaci $-$ a nulární operace $\mathbf{0}$ a $\mathbf{1}$:

$$p + q = \sum_{m \in M} (p(m) + q(m)) \cdot m, \quad p \cdot q = \sum_{m \in M} \left(\sum_{r \cdot s = m} p(r) \cdot q(s) \right) \cdot m,$$

$$-p = \sum_{m \in M} (-p(m)) \cdot m, \quad \mathbf{0} = \sum_{m \in M} 0 \cdot m, \quad \mathbf{1} = 1 \cdot e + \sum_{m \in M \setminus \{e\}} 0 \cdot m.$$

Poznámka 4.1. Necht' $R(+, \cdot, -, 0, 1)$ je okruh a $M(\cdot)$ je monoid s neutrálním prvkem e .

- (1) $R[M](+, \cdot, -, \mathbf{0}, \mathbf{1})$ je okruh,
- (2) zobrazení $i : R \rightarrow R[M]$ dané předpisem $i(r) = r \cdot e$ (tj. $[i(r)](m) = 0$ pro všechna $m \neq e$ a $[i(r)](e) = r$) je prostý okruhový homomorfismus.
- (3) zobrazení $\nu : M \rightarrow R[M]$ dané předpisem $\nu(m) = 1 \cdot m$ je prostý homomorfismus monoidu $M(\cdot)$ do monoidu $R[M](\cdot)$.

Důkaz. (1) Vezměme $p, q, r \in R$, kde $p = \sum_{m \in M} p(m) \cdot m, q = \sum_{m \in M} q(m) \cdot m, r = \sum_{m \in M} r(m) \cdot m$. Nejprve si uvědomíme, že jsou binární operace dobře definované (pro nulární a unární je korektnost definice zřejmá). K tomu stačí uvážit, že

$$\{m \mid (p + q)(m) \neq 0\} \subseteq \{m \mid p(m) \neq 0\} \cup \{m \mid q(m) \neq 0\}$$

a že

$$\{m \mid (p \cdot q)(m) \neq 0\} \subseteq \{a \cdot b \mid p(a) \neq 0, q(b) \neq 0\}.$$

Dále platí, že

$$p + q = \sum_{m \in M} (p(m) + q(m)) \cdot m = \sum_{m \in M} (q(m) + p(m)) \cdot m = q + p,$$

$$(p+q)+r = \sum_{m \in M} [(p(m)+q(m))+r(m)] \cdot m = \sum_{m \in M} (p(m)+q(m)+r(m)) \cdot m = p+(q+r).$$

Proto $\mathbf{0}$ je zjevně neutrální prvek operace $+$ a platí, že $p+(-p) = \mathbf{0}$, je $R(+, -, 0)$ komutativní grupa.

Podobně

$$\begin{aligned} (p+q) \cdot r &= \sum_{m \in M} \sum_{a \cdot b = m} [p(a) + q(a)] \cdot r(b) \cdot m = \\ &= \sum_{m \in M} \sum_{a \cdot b = m} (p(a) \cdot r(b) + q(a) \cdot r(b)) \cdot m = p \cdot r + q \cdot r, \end{aligned}$$

důkaz druhé distributivity je symetrický. Konečně zbývá ověřit, že je $R(\cdot, 1)$ monoid:

$$(p \cdot q) \cdot r = \left(\sum_{m \in M} \sum_{a \cdot b = m} (p(a) \cdot q(b)) \cdot m \right) \cdot r = \sum_{m \in M} \sum_{a \cdot b \cdot c = m} (p(a) \cdot q(b) \cdot r(c)) \cdot m = p \cdot (q \cdot r).$$

a

$$p \cdot \mathbf{1} = \sum_{m \in M} \sum_{a \cdot b = m} (p(a) \cdot \mathbf{1}(b)) \cdot m = \sum_{m \in M} (p(m) \cdot \mathbf{1}(e)) \cdot m = p = \mathbf{1} \cdot p.$$

(2) a (3) dostáváme okamžitě z konstrukce okruhu $R[M]$. \square

Poznamenejme, že předvedená obecná konstrukce se obvykle nazývá *monoidový okruh*.

Příklad 4.2. (1) Buď $R(+, \cdot, -, 0, 1)$ okruh a buď $\mathbb{N}_0(+, 0)$ monoid nezáporných celých čísel se sčítáním. Budeme-li prvky $p = \sum_{n \in \mathbb{N}_0} p(n) \cdot n \in R[\mathbb{N}_0]$ zapisovat ve tvaru $p = \sum_{n \in \mathbb{N}_0} p(n) \cdot x^n$ nebo $p = \sum_{n \in \mathbb{N}_0} p_n \cdot x^n$, pak vidíme, že je monoidový okruh $R[\mathbb{N}_0]$ právě okruhem polynomů jedné neurčité $R[x](+, \cdot, -, 0, 1)$. Místo $R[\mathbb{N}_0]$ budeme nadále psát $R[x]$ a operace budeme standardně zapisovat ve tvaru

$$p \pm q = \sum_{i \in \mathbb{N}_0} (p_i \pm q_i) \cdot x^i, p \cdot q = \sum_{n \in \mathbb{N}_0} \left(\sum_{i+j=n} p_i \cdot q_j \right) \cdot x^n.$$

(2) Polynomy více neurčitých můžeme zavést dvěma ekvivalentními způsoby: jednak indukcí $R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n]$ nebo jako monoidový okruh $R[\mathbb{N}_0^n] = (R[x_1, \dots, x_{n-1}])[x_n]$ se součinným monoidem $\mathbb{N}_0^n(+, (0, \dots, 0))$.

(3) Konstrukce okruhu $R[M]$ funguje i pro grupu, máme-li například konečnou grupu G řádu n , pak je $\mathbb{Z}_p[G]$ pro prvočíslo p rovněž vektorovým prostorem dimenze n nad tělesem \mathbb{Z}_p .

Na tomto místě opět zdůrazněme, že pro nás není vhodné chápání polynomů na okruhu s nosnou množinou R jako (vybrané) funkce $R \rightarrow R$. Například pro těleso \mathbb{Z}_2 existují pouze 4 funkce $\mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, zatímco polynomů nad \mathbb{Z}_2 je nekonečně mnoho.

Připomeňme, že pro okruh $R(+, \cdot, -, 0, 1)$ a $p = \sum_{n \in \mathbb{N}_0} a_n \cdot x^n \in R[x]$, kde $p \neq \mathbf{0}$, se největší takové $n \in \mathbb{N}_0$, že $a_n \neq 0$, nazývá stupněm polynomu p . Stupeň polynomu $\mathbf{0}$ je roven -1 . Stupeň polynomu p značíme $\deg p$.

Zopakujme pozorování o stupních, které jsme učinili minulý semestr:

Poznámka 4.3. *Nechť $R(+, \cdot, -, 0, 1)$ je okruh a $p, q \in R[x]$.*

- (1) $\deg p + q \leq \max(\deg p, \deg q)$,
- (2) *je-li $p, q \neq \mathbf{0}$, pak $\deg p \cdot q \leq \deg p + \deg q$, je-li navíc R oborem, potom $\deg p \cdot q = \deg p + \deg q$,*
- (3) *$R[x]$ je obor právě tehdy, když je R obor,*

Další pozorování si všimá velmi přirozená a zároveň užitečné algebraické vlastnosti dosazení do

Poznámka 4.4. Je-li $S(+, \cdot, -, 0, 1)$ komutativní okruh, R jeho podokruh a $\alpha \in S$, pak zobrazení $j_\alpha : R[x] \rightarrow S$ dané předpisem $j_\alpha(\sum_{n \in \mathbb{N}_0} a_n x^n) = \sum_{n \in \mathbb{N}_0} a_n \cdot \alpha^n$ je okruhový homomorfismus.

Důkaz. Nejprve snadno spočítáme, že $j_\alpha(0) = 0x^0$, $j_\alpha(1x^0) = 1$ a pro libovolné $a, b \in R[x]$, kde $a = \sum_n a_n \cdot x^n$ a $b = \sum_n b_n \cdot x^n$

$$j_\alpha(a + b) = j_\alpha\left(\sum_n (a_n + b_n) \cdot x^n\right) = \sum_n (a_n + b_n) \cdot \alpha^n = j_\alpha(a) + j_\alpha(b),$$

proto je j_α homomorfismus grup $R(+, -, 0)$ a $S(+, -, 0)$. Zbývá nahlédnout, že

$$j_\alpha(a \cdot b) = j_\alpha\left(\sum_n \sum_{k=0}^n (a_k \cdot b_{n-k}) \cdot x^n\right) = \sum_n \sum_{k=0}^n (a_k \cdot b_{n-k}) \cdot \alpha^n = j_\alpha(a) \cdot j_\alpha(b).$$

□

Definice. Nechť $S(+, \cdot, -, 0, 1)$ je komutativní okruh, R jeho podokruh, $\alpha \in S$ a $p \in R[x]$. Homomorfismu j_α z 4.4 říkáme *dosazovací homomorfismus*, α nazveme *kořenem* polynomu p , jestliže $j_\alpha(p) = 0$, a α je *vícenásobný kořen* polynomu p , pokud $(x - \alpha)^2/p$. *Kořenovým činitelem* (kořenu α) rozumíme polynom tvaru $x - \alpha$. Řekneme, že se polynom p rozkládá na *kořenové činitele* v $S[x]$, existují-li takové prvky $a \in R$ a $\alpha_1, \dots, \alpha_n \in S$, že $p = a \cdot (x - \alpha_1) \cdot \dots \cdot (x - \alpha_n)$.

V následujícím budeme často používat pro dosazení obvyklý zápis $p(\alpha)$ místo právě zavedeného zápisu $j_\alpha(p)$.

Poznámka 4.5. Nechť je $R(+, \cdot, -, 0, 1)$ obor, $\alpha \in R$ a $p \in R[x] \setminus \{0\}$.

- (1) α je kořenem p právě tehdy, když $(x - \alpha)/p$ v $R[x]$,
- (2) $x - \alpha$ je prvočinitel oboru $R[x]$,
- (3) je-li $p \neq 0$, pak p má nejvýše $\deg p$ kořenů.

Důkaz. (1) Předpokládejme, že je α kořenem p . Protože je 1 invertibilní prvek oboru R můžeme podle 3.4 vydělit polynom p polynomem $x - \alpha$ se zbytkem, tedy existují $q, r \in R[x]$, pro něž $p = (x - \alpha)q + r$ a $\deg r < \deg(x - \alpha) = 1$. Dosadíme-li nyní α do polynomu $r = p - (x - \alpha)q$ a využijeme-li 4.4, dostaneme $r(\alpha) = j_\alpha(r) = j_\alpha(p) - j_\alpha((x - \alpha)j_\alpha(q)) = 0 - 0q(\alpha) = 0$. Protože $\deg r < 1$, vidíme, že $r = 0$, a proto $(x - \alpha)/p$.

Jestliže $(x - \alpha)/p$, máme $p = (x - \alpha)q$ pro vhodné $q \in R[x]$ a tedy $p(\alpha) = (\alpha - \alpha)q(\alpha) = 0$ díky 4.4.

(2) Jestliže $(x - \alpha)/a \cdot b$ pro $a, b \in R[x]$, plyne z (1), že je α kořenem $a \cdot b$. Nyní $a(\alpha) \cdot b(\alpha) = 0$ podle 4.4, proto $a(\alpha) = 0$ nebo $b(\alpha) = 0$, neboť je R obor. Tedy $x - \alpha/a$ nebo $x - \alpha/b$ podle (1).

(3) Nechť $\alpha_1, \dots, \alpha_k \in R$ jsou různé kořeny p . Indukcí podle počtu r různých kořenů nahlédneme, že $p = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_k) \cdot q$ pro vhodný nenulový polynom q . Krok $r = 1$ nám dává (1). Jestliže $p = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_r) \cdot q$ a $(x - \alpha_{r+1})/p$ podle (1), pak $x - \alpha_{r+1}$ je prvočinitel podle (2) nedělí žádný z polynomů $x - \alpha_i$, kde $i \leq r$, proto $(x - \alpha_{r+1})/q$. Konečně z 4.3(3) plyne, že $\deg p = \deg((x - \alpha_1) \cdot \dots \cdot (x - \alpha_k) \cdot q) = k + \deg q \geq k$. □

Všimněme si, že 4.5(1) říká, že vícenásobný kořen je kořenem, a 4.5(2) nám poskytne příklady prvočinitelů (a tedy ireducibilních prvků) v okruhu polynomů nad obecným oborem.

Definice. Bud' $R(+, \cdot, -, 0, 1)$ komutativní okruh a $p = \sum_{i \geq 0} a_i x^i \in R[x]$. Derivací polynomu p budeme rozumět polynom $(\sum_{i \geq 0} a_i x^i)' = \sum_{i \geq 0} (i+1)a_{i+1}x^i$.

Poznámka 4.6. Nechť $R(+, \cdot, -, 0, 1)$ je komutativní okruh, $\alpha \in R$, $p, q \in R[x]$ a $n \in \mathbb{N}$. Pak platí:

- (1) $(p+q)' = p' + q'$, $(\alpha x^0 \cdot p)' = \alpha x^0 \cdot p'$,
- (2) $(p \cdot q)' = p' \cdot q + p \cdot q'$.
- (3) $(p^n)' = np^{n-1} \cdot p'$, kde $n = 1 + \dots + 1 \in R$.

Důkaz. (1), (2) Vlastnosti dostáváme přímočarým použitím definice.

(3) Dokážeme indukcí indukci podle n . Pro $n = 1$ je $(p^1)' = p' = 1p^0 \cdot p'$. Platí-li tvrzení pro $n - 1$ a použijeme-li (3) dostáváme

$$(p^n)' = (p \cdot p^{n-1})' = p' \cdot p^{n-1} + p \cdot (p^{n-1})' = p' \cdot p^{n-1} + p \cdot (n-1)p^{n-2} \cdot p' = np^{n-1} \cdot p'.$$

□

Poznámka 4.7. Nechť $S(+, \cdot, -, 0, 1)$ je obor, R jeho podokruh, $\alpha \in S$ a $p \in R[x]$.

- (1) α je vícenásobný kořen p , právě když je α kořenem p i p' ,
- (2) jestliže $\deg p \geq 1$ a 1 je GCD(p, p'), pak p nemá žádný vícenásobný kořen,
- (3) nedělí-li charakteristika R přirozené číslo n , pak $x^n - 1$ ani $x^{n+1} - x$ nemají v S žádný vícenásobný kořen.

Důkaz. Poznamenejme, že polynom s koeficienty v R můžeme přirozeným způsobem chápat jako polynom okruhu $S[x]$.

(1) Předpokládáme, že α je kořen p , tedy $p = (x - \alpha) \cdot q$ pro vhodný polynom $q \in S[x]$ podle 4.5(1). Pomocí 4.6(2) spočítáme $p' = q + (x - \alpha) \cdot q'$. Díky 4.4 vidíme, že je α kořenem p' právě tehdy, když je kořenem q a to je podle 4.5(1) ekvivalentní tomu, že $(x - \alpha)/q$ tj. $(x - \alpha)^2/p$.

(2) Tvrzení dokážeme nepřímo. Je-li α vícenásobný kořen p , potom podle (1) a 4.5(1) $(x - \alpha)/p'$. Protože $(x - \alpha)/p$, polynomy p a p' nemohou být nesoudělné.

(3) Označme $n \in R$ je součet n kopií 1 tělesa, a poznamenejme, že podle předpokladu $n \neq 0$. Protože polynom $(x^n - 1)' = n \cdot x^{n-1}$ je nenulový, $j_\alpha(n \cdot x^{n-1}) = (n \times 1) \cdot \alpha^{n-1} \neq 0$ pro všechna $\alpha \neq 0$, a naopak 0 není kořenem polynomu $x^n - 1$, $x^n - 1$ nemá žádný vícenásobný kořen díky (1).

Předpokládejme, že $(x - \alpha)^2/x^{n+1} - x$, tedy existuje $p \in S[x]$, pro který $(x - \alpha)^2 \cdot p = x^{n+1} - x = x \cdot (x^n - 1)$. Jestliže $\alpha = 0$, pak výraz vykrátíme na $x \cdot p = x^n - 1$, což není možné, protože $x^n - 1$ nemá kořen 0. Kdyby $\alpha \neq 0$, pak $(-\alpha)^2 \cdot p(0) = 0$, a proto $p(0) = 0$. Tedy podle 4.5(1) existuje takové $q \in S[x]$, že $p = x \cdot q$. Dosadíme-li za p do původní rovnosti a opět vykrátíme x , dostáváme, že $(x - \alpha)^2 \cdot q = x^n - 1$, což jsme vyloučili v první části důkazu (3). □

Příklad 4.8. V tělese charakteristiky 3 (např. \mathbb{Z}_3) platí, že $(x - 1)^3 = x^3 - 3x^2 + 3x - 1 = x^3 - 1$, tedy polynom $x^3 - 1$ má nad takovým tělesem vícenásobný kořen 1. Vidíme, že předpoklad o charakteristice z 4.7(3) nemůžeme odstranit. Navíc si všimněme derivace $(x^3 - 1)' = 0$.

Cvičení:

- (1) Dokažte, že okruh $\mathbb{Z}[\sqrt{3}] = \{a + \sqrt{3}b \mid a, b \in \mathbb{Z}\}$ je eukleidovským oborem.

- (2) Popište prvočinitele oboru Gaussových celých čísel.

5. KOŘENOVÁ NADTĚLESA

V této kapitole se budeme věnovat zkoumání vlastností kořenů polynomů nad tělesy. Nejprve si všimneme, že prvky n -prvkové konečné podgrupy multiplika-
tivní grupy komutativního tělesa lze nahlížet jako na všechny kořeny polynomu $x^n - 1$, což je hlavní argument tvrzení, že je tato grupa nutně cyklická. Poté se začneme zabývat hledáním těles, nad nimiž by se předem daný polynom rozkládal na kořenové činitele.

Nyní dokážeme nedokázané tvrzení z minulého semestru o multiplika-
tivní grupě libovolného tělesa:

Věta 5.1. *Nechť $T(+, \cdot, -, 0, 1)$ je komutativní těleso a necht' G je konečná pod-
grupa multiplika-
tivní grupy $T \setminus \{0\}(\cdot)$. Potom je G cyklická grupa.*

Důkaz. Uvažujme nejprve libovolnou konečnou grupu $G(\cdot)$ a položme $n = |G|$. Po-
znamenejme, že řádem prvku grupy budeme rozumět řád cyklické podgrupy tímto
prvkem generované. Podle Lagrangeovy věty dělí řád každého prvku konečné grupy
její řád. Označíme-li t_k počet všech prvků G , které jsou právě řádu k , vidíme, že
 $|G| = \sum_{k|n} t_k$. Připomeňme, že v cyklické grupě řádu n máme pro každé $k|n$ právě
jednu (cyklickou) podgrupu řádu k a počet generátorů této podgrupy, tedy právě
všechny prvky řádu k , udává hodnota Eulerovy funkce $\varphi(k)$, dává nám předchozí
rovnost vztah $n = \sum_{k|n} \varphi(k)$.

Tvrzení dokážeme sporem. Předpokládejme, že G je (konečná) podgrupa mul-
tiplika-
tivní grupy $T \setminus \{0\}(\cdot)$, která není cyklická, tedy $t_n = 0 (< \varphi(n))$. Z úvodních
úvah víme, že $n = |G| = \sum_{k|n} t_k = \sum_{k|n} \varphi(k)$, proto musí existovat $k|n$, pro nějž
 $t_k > \varphi(k)$, zvolme nějaké takové k a vezměme $u \in G$ řádu k . Potom pro všechny
prvky a cyklické grupy $\langle u \rangle$ platí $a^k = 1$, tedy a je kořenem polynomu $x^k - 1$. Ovšem
 $\langle u \rangle$ obsahuje právě $\varphi(k)$ generátorů, tj. prvků řádu k , tedy musí existovat nějaký
další prvek $v \in G \setminus \langle u \rangle$ řádu k . I on je kořenem polynomu $x^k - 1$, tedy jsme našli
 $k + 1$ kořenů polynomu stupně k , což je ve sporu s 4.5(3). \square

Příklad 5.2. $\mathbb{Z}_{53} \setminus \{0\}(\cdot)$ je podle 5.1 cyklická grupa řádu 52. To znamená, že
obsahuje $\varphi(52) = 3 \cdot 12 = 36$ generátorů.

Uvědomíme si, že homomorfismus okruhů lze přirozeným způsobem rozšířit na
homomorfismus příslušných polynomiálních okruhů.

Jsou-li $R(+, \cdot, -, 0, 1)$ a $S(+, \cdot, -, 0, 1)$ okruhy a $f : R \rightarrow S$ jejich homomorfis-
mus, pak označme $f_x : R[x] \rightarrow S[x]$ zobrazení určené předpisem $f_x(\sum_{i \geq 0} a_i x^i) =$
 $\sum_{i \geq 0} f(a_i) x^i$.

Poznámka 5.3. *Bud' $R(+, \cdot, -, 0, 1)$, $S(+, \cdot, -, 0, 1)$ a $T(+, \cdot, -, 0, 1)$ komutativní
okruhy a $f : R \rightarrow S$ a $g : S \rightarrow T$ homomorfismy. Potom platí:*

- (1) f_x je okruhový homomorfismus,
- (2) $(gf)_x = g_x f_x$,
- (3) f_x je izomorfismus, právě když f je izomorfismus,
- (4) $f j_\alpha = j_{f(\alpha)} f_x$ pro každé $\alpha \in R$.

Důkaz. (1) Zřejmě $f_x(1x^0) = 1x^0$, proto stačí dokázat slučitelnost f_x s operacemi + a \cdot . Bud' $a, b \in R[x]$, $a = \sum_n a_n x^n$, $b = \sum_n b_n x^n$:

$$\begin{aligned} f_x(a+b) &= f_x\left(\sum_n (a_n + b_n)x^n\right) = \sum_n f(a_n + b_n)x^n = \sum_n (f(a_n) + f(b_n))x^n = \\ &= \sum_n f(a_n)x^n + \sum_n f(b_n)x^n = f_x(a) + f_x(b), \end{aligned}$$

$$\begin{aligned} f_x(a \cdot b) &= f_x\left(\sum_n \sum_{k=0}^n (a_k \cdot b_{n-k})x^n\right) = \sum_n f\left(\sum_{k=0}^n (a_k \cdot b_{n-k})\right)x^n = \\ &= \sum_n \left(\sum_{k=0}^n f(a_k) \cdot f(b_{n-k})\right)x^n = \sum_n f(a_n)x^n \cdot \sum_n f(b_n)x^n = f_x(a) \cdot f_x(b). \end{aligned}$$

$$(2) \quad g_x f_x\left(\sum_n a_n x^n\right) = \sum_n g f(a_n)x^n = (gf)_x\left(\sum_n a_n x^n\right).$$

(3) Necht' je f_x izomorfismus. Jestliže $f(u) = f(v)$, pak $f_x(ux^0) = f_x(vx^0)$, a proto $u = v$, pro každé $u, v \in R$. Tedy f je prostý. Vezmeme-li $b \in S$ pak existuje ax^0 , pro který $f_x(ax^0) = bx^0$, tedy $f(a) = b$ a f je na celé S .

Je-li f izomorfismus, pak $f_x(f^{-1})_x = \text{Id}_{S[x]}$ a $(f^{-1})_x f_x = \text{Id}_{R[x]}$ podle (2), tedy $(f_x)^{-1} = (f^{-1})_x$ a f_x je izomorfismus.

$$(4) \quad f j_\alpha\left(\sum a_n x^n\right) = \sum f(a_n)f(\alpha)^n = j_{f(\alpha)} f_x\left(\sum a_n x^n\right). \quad \square$$

Připomeňme tvrzení, které jsme dokázali minulý semestr.

Poznámka 5.4. *Necht' $R(+, \cdot, -, 0, 1)$ je komutativní okruh a I jeho ideál. Potom faktorový okruh R/I je těleso právě tehdy, když I je maximální ideál.*

Důkaz. Připomeňme, že je svaz ideálů izomorfní svazu kongruencí okruhu, označme ρ_I kongruenci, která v tomto izomorfismu odpovídá ideálu I . Dále si uvědomme, že díky tomuto izomorfismu je I maximální ideál, právě když je ρ_I koatom svazu kongruencí a to je ekvivalentní tomu, že faktorokruh $R/\rho_I = R/I$ obsahuje pouze triviální kongruence. Tato podmínka ovšem na okruh R/I nastává právě tehdy, když je R/I těleso. \square

Věta 5.5. *Necht' $T(+, \cdot, -, 0, 1)$ je komutativní těleso a $u = \sum_{i \geq 0} a_i x^i \in T[x]$.*

- (1) *Faktorový okruh $T[x]/uT[x]$ je komutativní těleso, právě když je u ireducibilní.*
- (2) *Jestliže u není invertibilní, zobrazení $\mu(t) = tx^0 + uT[x]$ je prostý homomorfismus tělesa T do okruhu $T[x]/uT[x]$.*
- (3) *Je-li u ireducibilní, pak $\mu_y(\sum_{i \geq 0} a_i y^i)$ má kořen v tělese $T[x]/uT[x]$.*

Důkaz. (1) Podle Poznámky 5.4 stačí ověřit, že u je ireducibilní, právě když je $uT[x]$ maximální ideál. Necht' je u je ireducibilní a J ideál obsahující $uT[x]$. Podle 3.5 existuje $j \in T[x]$ $J = jT[x]$, tedy díky 2.2 j/u . Protože je u ireducibilní, máme buď $j||u$ a tudíž $uT[x] = J$ nebo $1||j$ a tudíž $jT[x] = T[x]$. Je-li $uT[x]$ maximální ideál, dostáváme závěr přímým použitím 2.2 a definice ireducibility.

(2) Uvědomme si, že zobrazení μ dostaneme jako složení homomorfismu i z 4.1(2) a přirozené projekce $\pi : T[x] \rightarrow T[x]/uT[x]$, proto $\mu = \pi i$ je opět homomorfismus. Jestliže konečně $\mu(a) = \mu(b)$, pak $u/ax^0 - bx^0$, tedy podle 4.3(3) je $ax^0 - bx^0$ musí být nulový polynom (v opačném případě by $\deg u \leq \deg(ax^0 - bx^0)$), a tedy μ je prosté.

(3) Stačí ověřit, že je $X = x + uT[x]$ kořenem $\sum_{i \geq 0} a_i y^i$ nad okruhem $T[x]/uT[x]$. Dosadíme-li, dostáváme $j_X(\sum_{i \geq 0} a_i y^i) = \sum_{i \geq 0} (a_i x^i + uT[x]) = (\sum_{i \geq 0} a_i x^i) + uT[x] = u + uT[x] = 0 + uT[x]$. \square

Pro každý ireducibilní polynom u označme symbolem $(T[x])_u$ těleso $T[x]/uT[x]$. Podle předchozí poznámky a 1. věty o izomorfismu můžeme ztotožnit těleso T a jeho homomorfní obraz $\mu(T)$, tedy těleso T budeme chápat jako podokruh tělesa $(T[x])_u$.

Definice. Necht' $U(+, \cdot, -, 0, 1)$ je komutativní těleso a $T \subseteq U$. Řekneme, že T je *podtěleso* U (resp. U je *nadtěleso* T), je-li T podokruh okruhu $U(+, \cdot, -, 0, 1)$ a T je těleso (tj. navíc $T \setminus \{0\}$ je podgrupou multiplikativní grupy $U \setminus \{0\}(\cdot)$ tělesa U).

Všimněme si, že množina všech podtěles komutativního tělesa tvoří uzávěrový systém, tj. průnik libovolného systému podtěles nějakého tělesa je opět podtěleso. To nám umožňuje zavést pro libovolné komutativní těleso U , jeho podtěleso T a prvek $\alpha \in U$ a podmnožinu $S \subseteq U$ následující **značení**:

- $T[S]$ je nejmenší podokruh U obsahující množinu $T \cup S$ a $T[\alpha] = T[\{\alpha\}]$
- $T(S)$ je nejmenší podtěleso U obsahující množinu $T \cup S$ a $T(\alpha) = T(\{\alpha\})$.

V následujícím budeme uvažovat vždy komutativní těleso U a jeho podtěleso T .

Poznámka 5.6. Jsou-li $T \subseteq U$ komutativní tělesa, $\alpha \in U$ a $S \subseteq U$, pak $T[\alpha] = \{\sum_{i=0}^n a_i \cdot \alpha^i \mid a_i \in T\} = j_\alpha(T[x])$, $T[\alpha] \subseteq T(\alpha)$ a $T[S] \subseteq T(S)$.

Důkaz. Zřejmě $\{p(\alpha) \mid p \in T[x]\} \subseteq T[\alpha]$, neboť $\alpha \in T[\alpha]$ a $T \subseteq T[\alpha]$. Naopak $\{p(\alpha) \mid p \in T[x]\} = j_\alpha(T[x])$ je podokruh U obsahující $\alpha = j_\alpha(x)$ a $t = j_\alpha(tx^0)$ pro všechna $t \in T$, proto $T[\alpha] \subseteq \{p(\alpha) \mid p \in T[x]\}$. Zbytek plyne okamžitě z definice. \square

Definice. Necht' $T \subseteq U$ jsou komutativní tělesa a $p \in T[x]$. Řekneme, že U je *kořenové nadtěleso* polynomu p , jestliže $U = T(\alpha)$ pro nějaký kořen $\alpha \in U$ polynomu p a U nazveme *rozkladovým nadtělesem* polynomu p , je-li $p = a(x - \alpha_1) \dots (x - \alpha_n)$ pro $a \in T$ a $\alpha_1, \dots, \alpha_n \in U$ a $U = T(\{\alpha_1, \dots, \alpha_n\})$.

Věta 5.7. Necht' $T(+, \cdot, -, 0, 1)$ je komutativní těleso a $p \in T[x]$, $\deg p \geq 1$.

- (1) existuje kořenové nadtěleso polynomu p ,
- (2) existuje rozkladové nadtěleso polynomu p .

Důkaz. (1) Podle 3.3 a 3.5 existuje (jednoznačný) ireducibilní rozklad polynomu p , zvolíme-li nějaký ireducibilní polynom p_1 , který dělí p , dostaneme podle 5.5 nadtěleso $U = (T[x])_{p_1}$, v němž má polynom p kořen α . Hledaným kořenovým nadtělesem je potom těleso $T(\alpha)$.

(2) Indukcí podle $n = \deg p$ dokážeme, že existuje komutativní nadtěleso V tělesa T , nad nímž se p rozkládá na kořenové činitele. Podle (1) existuje nadtěleso U , v němž má p kořen $\alpha \in U$. Označíme-li μ inkluzi T do U , pak $p = \mu_x(p) \in U[x]$ je polynom stupně n a podle 4.5(1) existuje polynom $v \in U[x]$ stupně $n-1$, pro který $u = (x - \alpha) \cdot v$. Podle indukčního předpokladu existuje nadtěleso V tělesa U , nad nímž se v a tedy i p rozkládá na kořenové činitele.

Dokázali jsme, že existují prvky $a \in U$ a $\alpha_1, \dots, \alpha_n \in V$, pro něž $p = a(x - \alpha_1) \dots (x - \alpha_n)$. Protože je $p \in T[x]$, máme $a \in T$, tedy rozkladovým nadtělesem polynomu p je právě těleso $T(\{\alpha_1, \dots, \alpha_n\})$. \square

Příklad 5.8. Těleso komplexních čísel je kořenovým i rozkladovým nadtělesem polynomu $x^2 + 1$ nad \mathbb{R} , $[\mathbb{C} : \mathbb{R}] = 2$.

6. MINIMÁLNÍ POLYNOMY ALGEBRAICKÝCH PRVKŮ

Nyní se podíváme na existující (například zkonstruované) rozšíření těles $T \subseteq U$ a budeme zkoumat množinu kořenů polynomů s koeficienty v T , které leží v U . Především si všimneme, že stupeň minimálního polynomu algebraického prvku α je stupeň příslušného jednoduchého rozšíření splývá.

Definice. Necht' $T \subseteq U$ jsou komutativní tělesa a $\alpha \in U$. Řekneme, že α je *algebraický prvek* nad T , existuje-li nenulový polynom $p \in T[x]$, jehož je α kořenem, tj. $j_\alpha(p) = 0$. V opačném případě mluvíme o *transcendentním prvku*. Těleso U nazveme *algebraickým rozšířením* tělesa T , jsou-li všechny prvky $\alpha \in U$ algebraické nad T . Polynom $p = \sum a_i x^i$ je *monický*, je-li $a_{\deg p} = 1$.

Věta 6.1. *Bud' $T \subseteq U$ komutativní tělesa a $\alpha \in U$ je algebraický prvek nad T . Pak existuje právě jeden takový monický polynom $m \in T[x] \setminus \{0\}$, že pro každé $p \in T[x] \setminus \{0\}$ platí, že $j_\alpha(p) = 0$, právě když $m|p$. Navíc m je ireducibilní, $(T[x])_m \cong T(\alpha)$ a $T[\alpha] = T(\alpha)$.*

Důkaz. Vezměme množinu $I = \{p \in T[x] \mid j_\alpha(p) = 0\} = j_\alpha^{-1}(0)$ všech polynomů, které mají kořen α . Protože je j_α homomorfismus podle 4.4, vidíme, že je I jako úplný vzor nulové podgrupy podgrupou grupy $T[x](+, -, 0)$. Jestliže $p \in I$ a $q \in T[x]$, máme $j_\alpha(pq) = 0 \cdot j_\alpha(q) = 0$, tedy $p \cdot q \in I$. Nahlédli jsme, že je I ideál, tedy podle 3.5 existuje jeho generátor $a = \sum a_n x^n \in I$. Protože je prvek α algebraický nad T , obsahuje $I = aT[x]$ nenulový polynom a proto je nenulový i polynom $a \in I$. Je-li $n = \deg a$, položíme $m = a_n^{-1}a$. Nyní je m monický, platí $I = mT[x]$, tedy $p(\alpha) = 0 \Leftrightarrow p \in I \Leftrightarrow m|p$, a zřejmě je takový monický polynom určen jednoznačně.

Nyní předpokládejme, že $m = a \cdot b$, kde $a, b \in T[x]$. Potom podle 4.4 $a(\alpha) = 0$ a pak $m||a$ nebo $b(\alpha) = 0$ a pak $m||b$, tedy m je ireducibilní. Konečně si všimneme, že díky 1. větě o izomorfismu a 5.6(1) je

$$(T[x])_m = T[x]/mT[x] = T[x]/\ker j_\alpha \cong j_\alpha(T[x]) = T[\alpha].$$

Protože je $T[x]/mT[x]$ podle 5.5 těleso, je i $T[\alpha]$ těleso, proto $T[\alpha] = T(\alpha)$. \square

Definice. Bud' $T \subseteq U$ komutativní tělesa. Polynom z předchozí věty nazveme *minimálním polynomem* algebraického prvku $\alpha \in U$, budeme ho značit m_α . *Stupeň rozšíření U nad T* definujeme jako $[U : T] = \dim_T U$, kde U chápeme jako vektorový prostor nad tělesem T .

Nejprve učinme drobné lineární algebraické pozorování.

Poznámka 6.2. *Necht' $T \subseteq U \subseteq V$ jsou do sebe zařazená komutativní tělesa. Potom $[V : T] = [V : U][U : T]$.*

Důkaz. Je-li (\mathbf{v}_i) báze prostoru V nad tělesem U a (\mathbf{u}_i) báze prostoru U nad tělesem T , ukážeme, že $(\mathbf{u}_i \mathbf{v}_j)$ je báze prostoru V nad tělesem T . Vezmeme-li libovolné $a \in V$, pak existuje lineární kombinace $a = \sum_i d_i \mathbf{v}_i$, kde $d_i \in U$. Proto pro každé i existují lineární kombinace $d_i = \sum_j c_{ij} \mathbf{u}_i$, kde $c_{ij} \in T$. Vidíme, že $a = \sum_{ij} c_{ij} \mathbf{u}_i \mathbf{v}_i$, tedy $(\mathbf{u}_i \mathbf{v}_j)$ generuje V nad T . Podobně jestliže $0 = \sum_{ij} c_{ij} \mathbf{u}_i \mathbf{v}_i = \sum_i (\sum_j c_{ij} \mathbf{u}_i) \mathbf{v}_i$ pro nějaká $c_{ij} \in T$, dostáváme z lineární nezávislosti (\mathbf{v}_i) nad U , že $\sum_j c_{ij} \mathbf{u}_i = 0$ a z lineární nezávislosti (\mathbf{u}_i) nad T plyne, že všechna c_{ij} jsou nulová. Tím jsme ověřili, že $(\mathbf{u}_i \mathbf{v}_j)$ je lineárně nezávislá generující množina, tedy báze. Proto $[V : T] = |(\mathbf{u}_i \mathbf{v}_j)| = |(\mathbf{u}_i)| |(\mathbf{v}_j)| = [V : U][U : T]$. \square

Věta 6.3. *Nechť $T \subseteq U$ jsou komutativní tělesa a $\alpha, \alpha_1, \dots, \alpha_k \in U$.*

- (1) *Je-li α algebraický, pak $[T(\alpha) : T] = \deg m_\alpha$,*
- (2) *je-li $[T(\alpha) : T]$ konečné, pak je α algebraický,*
- (3) *je-li $[U : T]$ konečné, pak je U algebraické rozšíření tělesa T ,*
- (4) *$T(\alpha_1, \dots, \alpha_n) = T[\alpha_1, \dots, \alpha_n]$ je rozšířením konečného stupně tedy algebraickým rozšířením tělesa T , jsou-li $\alpha_1, \dots, \alpha_k$ algebraické nad T .*

Důkaz. (1) Položme $n = \deg m_\alpha$ a připomeňme, že $T[\alpha] = T(\alpha)$ podle Věty 6.1. Dokážeme, že množina $\{\alpha^i \mid i = 0, 1, \dots, n-1\}$ je bází $T[\alpha]$ nad tělesem T . Vezměme prvek $t \in T[\alpha]$, o němž z 5.6 víme, že je tvaru $t = p(\alpha)$ pro vhodný polynom $p \in T[x]$. Vydělíme-li nyní se zbytkem polynom p polynomem m_α , dostaneme (3.4) $p = qm_\alpha + r$ pro $q, r \in T[x]$ a $\deg r < n$. Nyní vidíme, že $t = p(\alpha) = q(\alpha)m_\alpha(\alpha) + r(\alpha) = r(\alpha)$, protože je α kořenem m_α , tedy $t = r(\alpha) = \sum_{i < n} r_i \alpha^i$ je T -lineární kombinací prvků $\{\alpha^i \mid i = 0, 1, \dots, n-1\}$. Je-li nyní $\sum_{i < n} c_i \alpha^i = 0$, kde $c_i \in T$, je α kořenem polynomu $c = \sum_{i < n} c_i x^i = 0$ stupně menšího než n . Protože podle 6.1 m_α/c , dostáváme, že $c = 0$, tudíž $\{\alpha^i \mid i = 0, 1, \dots, n-1\}$ je lineárně nezávislá množina.

(2) Je-li $[T(\alpha) : T]$ konečné, je množina $\{\alpha^i \mid i \geq 0\}$ lineárně závislá, tudíž existuje netriviální lineární kombinace $\sum_{i \leq n} d_i \alpha^i = 0$, tedy α kořenem nenulového polynomu $\sum_{i \leq n} d_i x^i$.

(3) Vezměme libovolné $\alpha \in U$. Potom je $T(\alpha)$ podprostor konečně generovaného vektorového prostoru U nad tělesem T , tedy $[T(\alpha) : T]$ je konečné a proto je α algebraický prvek podle (2).

(4) Tvrzení dokážeme indukcí podle n , přičemž jsme tvrzení pro $n = 1$ dokázali v 6.1, navíc $[T(\alpha) : T]$ je konečné podle (1). Předpokládejme, že tvrzení platí pro $k-1$. Nyní $T[\alpha_1, \dots, \alpha_n] = T[\alpha_1, \dots, \alpha_{n-1}][\alpha_n] = T(\alpha_1, \dots, \alpha_{n-1})[\alpha_n]$ a $T(\alpha_1, \dots, \alpha_{n-1})$ je konečného stupně nad T podle indukčního předpokladu. Protože je prvek α_n algebraický nad tělesem $T(\alpha_1, \dots, \alpha_{n-1})$, vidíme díky 6.1, že

$$T(\alpha_1, \dots, \alpha_{n-1})[\alpha_n] = T(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) = T(\alpha_1, \dots, \alpha_n).$$

Konečně díky (1), indukčnímu předpokladu a 6.2 dostáváme

$$\begin{aligned} [T(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) : T] &= \\ &= [T(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) : T(\alpha_1, \dots, \alpha_{n-1})][T(\alpha_1, \dots, \alpha_{n-1}) : T]. \end{aligned}$$

Protože jsou oba součinitele vpravo konečné, je i $[T(\alpha_1, \dots, \alpha_{n-1}, \alpha_n) : T]$ konečný. \square

Důsledek 6.4. *Nechť T je komutativní těleso, $p \in T[x]$ a nechť je U rozkladové nadtěleso polynomu p . Jsou-li $\alpha_1, \dots, \alpha_n \in U$ všechny kořeny polynomu p v tělese U , pak $U = T[\alpha_1, \dots, \alpha_n]$.*

Příklad 6.5. (1) $\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[\sqrt[3]{2}] = \{x + y\sqrt[3]{2} + z\sqrt[3]{4} \mid x, y, z \in \mathbb{Q}\}$ je kořenové nadtěleso polynomu $x^3 - 2$ nad \mathbb{Q} a $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, tedy $x^3 - 2$ je monický polynom stupně 3, a proto jde podle 6.3(1) a 6.1 právě o minimální polynom algebraického prvku $\sqrt[3]{2}$ nad \mathbb{Q} . Všimněme si, že zatímco nad \mathbb{Q} je polynom $x^3 - 2$ ireducibilní, nad \mathbb{R} máme ireducibilní rozklad $x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ a nad \mathbb{C} se polynom rozkládá na kořenové činitele.

(2) Nechť $k \in \mathbb{Z}$ a $\sqrt{k} \in \mathbb{C} \setminus \mathbb{Q}$. Pak $\mathbb{Q}(\sqrt{k}) \neq \mathbb{Q}$ a \sqrt{k} je kořenem polynomu $x^2 - k$, proto je $m_{\sqrt{k}} = x^2 - k$ díky 5.6 nutně minimální polynom a $[\mathbb{Q}(\sqrt{k}) : \mathbb{Q}] = \deg m_{\sqrt{k}} = 2$ podle 6.3(1). $\mathbb{Q}(\sqrt{k})$ je tzv. kvadratické rozšíření tělesa \mathbb{Q} .

(3) Prvek $\sqrt[5]{3}$ je kořenem polynomu $x^5 - 3 \in \mathbb{Q}[x]$ a prvek $\sqrt[7]{11}$ kořenem polynomu $x^7 - 11 \in \mathbb{Q}[x]$, tedy oba jsou algebraické nad \mathbb{Q} . Podle Poznámky 6.3(4) je $\mathbb{Q}(\sqrt[5]{3}, \sqrt[7]{11}) = \mathbb{Q}[\sqrt[5]{3}, \sqrt[7]{11}]$ algebraické rozšíření. Z toho plyne, že například pro prvek $\alpha = 5\sqrt[5]{3} + 2\sqrt[7]{11} - \sqrt[5]{27}\sqrt[7]{11} - 3$ existuje polynom $p \in \mathbb{Q}[x]$, jehož je α kořenem.

7. ROZKLADOVÁ NADTĚLESA A ALGEBRAICKÝ UZÁVĚR

Cílem této sekce je jednak důkaz tvrzení o jednoznačnosti existence rozkladových nadtěles a poté konstrukce algebraického uzávěru, tedy algebraického rozšíření, nad nímž se všechny polynomy rozkládají na kořenové činitele.

Poznámka 7.1. *Bud' $T_1 \subseteq U_1$ a $T_2 \subseteq U_2$ komutativní tělesa, bud' $f : T_1 \rightarrow T_2$ izomorfismus a necht' $\alpha \in U_1$ je algebraický prvek nad T_1 a $\beta \in U_2$ je algebraický prvek nad T_2 . Pak existuje takový izomorfismus $g : T_1(\alpha) \rightarrow T_2(\beta)$, že $g(\alpha) = \beta$ a $g(t) = f(t)$ pro všechna $t \in T_1$, právě když $f_x(m_\alpha) = m_\beta$.*

Důkaz. (\Rightarrow) Poznamenejme, že f_x je podle Poznámky 5.3(3) izomorfismus okruhů $T_1[x]$ a $T_2[x]$, proto je $f_x(m_\alpha)$ ireducibilní. Dále $j_{g(\alpha)}f_x(m_\alpha) = j_{g(\alpha)}g_x(m_\alpha) = g(j_\alpha(m_\alpha)) = g(0) = 0$ podle Poznámky 5.3(4), tedy $\beta = g(\alpha)$ je kořenem polynomu $f_x(m_\alpha) \in T_2[x] \subset U_2[x]$. Podle Věty 6.1 $m_\beta/f_x(m_\alpha)$. Protože je $f_x(m_\alpha)$ ireducibilní a monický, dostáváme nutně $m_\beta = f_x(m_\alpha)$.

(\Leftarrow) Stačí si uvědomit, že Věta 6.1 zaručuje existenci izomorfismů

$$i_\alpha : T_1[x]/(m_\alpha T_1[x]) \rightarrow T_1(\alpha), \quad i_\beta : T_2[x]/(m_\beta T_2[x]) \rightarrow T_2(\beta)$$

a že izomorfismus f_x indukuje podle předpokladu izomorfismus faktorových okruhů $\overline{f_x} : T_1[x]/(m_\alpha T_1[x]) \rightarrow T_2[x]/(m_\beta T_2[x])$, kde $\overline{f_x}(p + m_\alpha T_1[x]) = f_x(p) + m_\beta T_2[x]$. Složíme-li izomorfismy dostáváme

$$T_1(\alpha) \cong (T_1[x])_{m_\alpha} \cong (T_2[x])_{m_\beta} \cong T_2(\beta),$$

tedy máme izomorfismus $g = i_\beta \overline{f_x} i_\alpha^{-1}$. Nyní zbývá spočítat

$$g(t) = i_\beta \overline{f_x} i_\alpha^{-1}(t) = i_\beta \overline{f_x}(tx^0 + m_\alpha T_1[x]) = i_\beta(f(t)x^0 + m_\beta T_2[x]) = f(t)$$

pro každé $t \in T_1$ a podobně

$$g(\alpha) = i_\beta \overline{f_x} i_\alpha^{-1}(\alpha) = i_\beta \overline{f_x}(x^1 + m_\alpha T_1[x]) = i_\beta(x^1 + m_\beta T_2[x]) = \beta.$$

□

Věta 7.2. *Necht' T_1 a T_2 jsou komutativní tělesa, $f : T_1 \rightarrow T_2$ je izomorfismus a necht' U_1 je rozkladové nadtěleso polynomu $p \in T_1[x]$ a U_2 je rozkladové nadtěleso polynomu $f_x(p) \in T_2[x]$. Označme $\alpha_1, \dots, \alpha_n$ všechny kořeny polynomu p v U_1 a β_1, \dots, β_m všechny kořeny polynomu $f_x(p)$ v U_2 . Potom $n = m$ a existuje permutace σ a izomorfismus $g : U_1 \rightarrow U_2$ tak, že $g(\alpha_i) = \beta_{\sigma(i)}$ pro $i = 1, \dots, n$ a $g(t) = f(t)$ pro všechna $t \in T_1$.*

Důkaz. Znovu si všimněme, že f_x je izomorfismus okruhů $T_1[x]$ a $T_2[x]$. Tvrzení dokážeme indukcí podle stupně $k = \deg p = \deg f_x(p)$. Protože je rozkladové nadtěleso polynomu stupně 1 nad tělesem T_1 (T_2) rovno T_1 (T_2) stačí pro $k = 1$ položit $g = f$.

Předpokládejme, že tvrzení platí pro každou dvojici těles T_1 a T_2 a každý polynom stupně $k - 1$ nad tělesem T_1 a mějme polynom $p \in T_1[x] \subseteq U_1[x]$ stupně k . Protože $\alpha_n \in U_1$ je kořenem p , minimální polynom m_{α_n} dělí p podle 6.1, a

proto $f_x(m_{\alpha_n})$ dělí $f_x(p)$. Poznamenejme, že $\deg m_{\alpha_n} = \deg f_x(m_{\alpha_n}) > 0$ a že rozklad na ireducibilní prvky je podle 3.5 a 3.3 v okruhu $U_2[x]$ jednoznačný až na asociovanost, proto existuje (ireducibilní polynom) $x - \beta_i$, který dělí $f_x(m_{\alpha_n})$, bez újmy na obecnosti můžeme předpokládat, že $i = m$. Použijeme-li opět Větu 6.1, vidíme, že je polynom $f_x(m_{\alpha_n})$ ireducibilní (nad T_2) a monický, β_m je jeho kořen (nad U_2), a proto $f_x(m_{\alpha_n}) = m_{\beta_m}$. Nyní podle 7.1 existuje izomorfismus těles $h : T_1(\alpha_n) \rightarrow T_2(\beta_m)$, pro nějž platí, že $h(\alpha_n) = \beta_m$ a $h(t) = f(t)$ pro všechna $t \in T_1$. Zároveň můžeme v okruhu $T_1(\alpha_n)[x]$ vydělit polynom p polynomem $x - \alpha_n$, tedy najdeme polynom $q \in T_1(\alpha_n)[x]$ stupně $k - 1$, pro který $p = (x - \alpha_n)q$, a tudíž $f_x(p) = f_x(x - \alpha_n)f_x(q) = (x - \beta_m)f_x(q)$. Využijeme-li nyní indukčního předpokladu pro tělesa $T_1(\alpha_n)$ a $T_2(\beta_m)$, jejich izomorfismus h a polynom q , dostáváme, že $n - 1 = m - 1$, existuje permutace σ' na S_{n-1} a takový izomorfismus $g : U_1 \rightarrow U_2$, že $g(\alpha_i) = \beta_{\sigma'(i)}$ pro $i = 1, \dots, n - 1$ a $g(s) = h(s)$ pro všechna $s \in T_1(\alpha_n)$. Zřejmě tedy $n = m$, $g(t) = h(t) = f(t)$ pro všechna $s \in T_1$ a $g(\alpha_n) = \beta_m$. \square

Použijeme-li 7.2 pro $f = \text{Id}$ dostáváme

Důsledek 7.3. *Nechť T je komutativní těleso, $p \in T[x]$. Pak existuje až na izomorfismus právě jedno rozkladové nadtěleso polynomu p .*

Definice. Řekneme, že je komutativní těleso U *algebraicky uzavřené*, jestliže se každý nenulový polynom $p \in U[x]$ rozkládá nad U na kořenové činitele. Komutativní těleso U je *algebraickým uzávěrem tělesa T* , je-li U algebraicky uzavřené těleso, $T \subseteq U$, a žádné podtěleso V tělesa U , které obsahuje podtěleso T není algebraicky uzavřené.

Následující tvrzení dokážeme za použití množinově teoretického předpokladu principu transfinitní indukce, který je ekvivalentní tak zvanému axiomu výběru:

Věta 7.4. *Nechť T je komutativní těleso. Pak existuje jeho algebraický uzávěr U .*

Důkaz. Mějme κ nějaké ordinální číslo (nebo indexujeme přirozenými čísly). Nejprve si uvědomíme, že sjednocení řetězce těles $\bigcup_{\alpha < \kappa} U_\alpha$, kde U_α je podtěleso U_β pro každé $\alpha < \beta$, má přirozeně danou strukturu okruhu (operace jen stále rozšiřujeme) a je dokonce tělesem (inverzní prvek k prvku $t \in U_\alpha$ najdeme už v U_α). Zkonstruujeme posloupnost do sebe zařazených těles $T_i \subseteq T_{i+1}$, položíme $T_1 = T$.

Každé z těles T_i pro $i > 1$ přitom vytvoříme pomocí transfinitní indukce. Opatřeme nejprve indexy $\alpha < \kappa_i$ všechny polynomy nad T_i stupně nejvýše $i + 1$, t.j. $\{p_\alpha \mid \alpha < \kappa_i\} = \{p \in T_i[x] \mid \deg p \leq i + 1\}$. Položíme $T_{i0} = T_i$. Máme-li definováno těleso $T_{i\alpha}$ vezmeme jako těleso $T_{i\alpha+1}$ právě rozkladové nadtěleso polynomu $p_\alpha \in T_i[x] \subseteq T_{i\alpha}[x]$ nad tělesem $T_{i\alpha}$. Je-li β limitní ordinál položíme $T_{i\beta} = \bigcup_{\alpha < \beta} T_{i\alpha}$. Konečně definujeme $T_{i+1} = \bigcup_{\alpha < \kappa_i} T_{i\alpha}$.

Nyní stačí položit $U = \bigcup_{i \in \mathbb{N}} T_i$. Ukážeme, že U je algebraicky uzavřené. Je-li $p \in U[x]$, pak existuje takové i , že jsou všechny koeficienty p v T_i (p má jen konečně mnoho různých koeficientů) a navíc $\deg p \leq i + 1$. To ovšem znamená, že se p rozkládá nad $T_{i+1} \subseteq U$ na kořenové činitele.

Konečně poznamenejme, že algebraicky uzavřená podtělesa U tvoří uzávěrový systém, proto je průnik všech algebraicky uzavřených podtěles U obsahujících T hledaným algebraickým uzávěrem. \square

Podobnými prostředky jako u rozkladových nadtěles v Důsledku 7.3 se dá za použití axiomu výběru dokázat, že je algebraický uzávěr komutativního tělesa určen až na izomorfismus jednoznačně.

Příklad 7.5. Je známým faktem, že těleso komplexních čísel je algebraickým uzávěrem tělesa reálných čísel.

Všimněme si také, že \mathbb{R} není algebraickým rozšířením tělesa \mathbb{Q} , protože polynomů $\mathbb{Q}[x]$ je pouze spočetně mnoho a každý má pouze konečně mnoho kořenů, tedy všech reálných kořenů $\mathbb{Q}[x]$ je opět pouze spočetně. Ovšem množina \mathbb{R} spočetná není.

Algebraický uzávěr tělesa racionálních čísel najdeme jako maximální algebraické rozšíření \mathbb{Q} v algebraicky uzavřeném tělese \mathbb{C} , což je podle předchozí úvahy nutně spočetná množina.

8. ÚVOD DO GALOISOVY TEORIE

Cílem této kapitoly je úvod do klasické Galoisovy teorie, která popisuje vlastnosti rozšíření pomocí takzvaných Galoisových grup. V následující kapitole posléze pomocí překladu vlastností rozkladových nadtěles polynomů do příslušné Galoisovy grupy dokážeme, že pro polynomy stupně většího než čtyři nemusí existovat žádný způsob jak pomocí obvyklých operací v tělese a odmocňování vyjádřit kořeny polynomu.

Nejprve definujeme centrální pojem této kapitoly.

Definice. Necht' $T \subseteq U$ je rozšíření komutativních těles. Zobrazení $\sigma : U \rightarrow U$ je T -izomorfismus, je-li to takový izomorfismus těles, že $\sigma(t) = t$ pro každé $t \in T$. Grupu $\text{Gal}(U/T)$ všech T -izomorfismů $U \rightarrow U$ budeme nazývat *Galoisovou grupou*.

Poznámka 8.1. Necht' $T \subseteq U$ je rozšíření komutativních těles, $f \in T[x]$, $\sigma \in \text{Gal}(U/T)$ a $A = \{\alpha \in U \mid f(\alpha) = 0\}$.

- (1) $\sigma|_A$ je permutace na množině A ,
- (2) jestliže $S \subseteq U$ je rozkladové nadtěleso polynomu f nad tělesem T , pak $\sigma(S) = S$.

Důkaz. (1) Stačí si všimnout, že pro každé $\alpha \in A$ máme $0 = \sigma(0) = \sigma(f(\alpha)) = f(\sigma(\alpha))$, tedy $\sigma(\alpha) \in A$. Protože je σ prosté zobrazení a A je konečná množina, tvoří $\sigma|_A$ permutaci na množině A .

(2) Jsou-li $\alpha_1, \dots, \alpha_n$ právě všechny kořeny f v rozkladovém nadtělese V pak podle (1) platí, že

$$\sigma(S) = \sigma(T(\alpha_1, \dots, \alpha_n)) = T(\sigma(\alpha_1), \dots, \sigma(\alpha_n)) = T(\alpha_1, \dots, \alpha_n) = S.$$

□

Důsledek 8.2. Pro každé rozkladové nadtěleso polynomu $f \in T[X]$ nad tělesem T existuje prostý grupový homomorfismus grupy $\text{Gal}(U/T)$ do grupy permutací všech různých kořenů polynomu f , a tudíž i do grupy permutací $S_{\deg f}$.

Příklad 8.3. (1) Protože je těleso komplexních čísel \mathbb{C} rozkladovým nadtělesem polynomu $x^2 + 1$ nad \mathbb{R} a tento polynom má právě dva kořeny i a $-i$, existuje nejvíce tolik homomorfismů Galoisovy grupy $\text{Gal}(\mathbb{C}/\mathbb{R})$, kolik existuje permutací na množině $\{i, -i\}$. Přitom snadno ověříme, že zobrazení \overline{id} dané $\overline{id}(a + bi) = a - bi$ pro $a, b \in \mathbb{R}$, je \mathbb{R} -homomorfismus, proto $\text{Gal}(\mathbb{C}/\mathbb{R}) = \{\text{id}, \overline{id}\} \cong \mathbb{Z}_2$.

(2) Podobně je $\mathbb{Q}(\sqrt{2})$ rozkladovým nadtělesem polynomu $x^2 - 2$ nad \mathbb{Q} , a proto $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\text{id}, \varphi\} \cong \mathbb{Z}_2$, kde \mathbb{Q} -izomorfismus $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$ pro $a, b \in \mathbb{Q}$.

(3) $\text{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\text{id}\}$, neboť polynom $x^3 - 2$, jehož je $\sqrt[3]{2}$ kořenem, má v tělese $\mathbb{Q}(\sqrt[3]{2})$ pouze tento kořen, zbylé dva jdou komplexní.

Definice. Nechť $T \subseteq U$ je rozšíření komutativních těles charakteristiky 0. Řekněme, že se jedná o *Galoisovo rozšíření* je-li U rozkladové nadtěleso nějakého polynomu $z \in T[x]$, který v U nemá žádné vícenásobné kořeny.

Poznámka 8.4. *Rozkladové nadtěleso libovolného polynomu nad tělesem charakteristiky 0 je vždy Galoisovo.*

Důkaz. Bud' U rozkladové nadtěleso polynomu $f \in T[x]$ nad tělesem T . Potom existuje ireducibilní rozklad polynomu $f = a \prod_i m_i^{\epsilon_i}$ v eukleidovském oboru $T[x]$, kde $a \in T$, $\epsilon_i \in \mathbb{N}$, $m_i \in T[x]$ jsou monické polynomy a $m_i \neq m_j$ pro $i \neq j$. Z ireducibility plyne, že pro $i \neq j$ nemají polynomy m_i a m_j v U žádný společný kořen, neboť jde o minimální polynomy nad T každého jejich kořenu, a navíc žádný z polynomů m_i nemá vícenásobný kořen, protože $\deg m_i' = \deg m_i - 1 \geq 0$ a tudíž m_i' a m_i jsou nesoudělné. To znamená, že polynom $g = \prod_i m_i$, který má stejné kořeny jako f nemá žádný vícenásobný kořen. Protože je U zřejmě rozkladové nadtěleso polynomu g , jedná se o Galoisovo rozšíření tělesa T . \square

Nadále nás budou zajímat především Galoisovy grupy Galoisových rozšíření. Nejprve si všimněme, že pro hledání rozkladových nadtěles ireducibilních polynomů nám mohou posloužit rozkladová nadtělesa jiných polynomů.

Poznámka 8.5. *Nechť $T \subseteq U$ je Galoisovo rozšíření komutativních těles a $m \in T[x]$ ireducibilní polynom.*

- (1) *Pro každé dva kořeny $\alpha, \beta \in U$ polynomu m existuje takový homomorfismus $f \in \text{Gal}(U/T)$, že $f(\alpha) = \beta$.*
- (2) *Jestliže v U leží nějaký kořen m , pak se m rozkládá nad U na kořenové činitele.*

Důkaz. (1) Můžeme předpokládat, že je m monický a tudíž se jedná právě o minimální polynom obou svých kořenů α i β nad tělesem T . Tedy podle 6.1 existuje takový T -izomorfismus $\varphi : T(\alpha) \rightarrow T(\beta)$, že $\varphi(\alpha) = \beta$. Nyní zbývá, abychom použili Větu 7.2 pro $T_1 = T(\alpha)$, $T_2 = T(\beta)$ a $U_1 = U_2 = U$.

(2) Nechť je U rozkladové nadtěleso polynomu $f \in T[x]$ nad tělesem T a označme V rozkladové nadtěleso polynomu fm nad tělesem T . Zřejmě $T \subseteq U \subseteq V$. Nechť $\alpha, \beta \in V$ jsou dva kořeny polynomu m , z nichž první leží v U . Ukážeme, že $\beta \in U$. Stejně jako v (1) dostaneme T -izomorfismus $\varphi : T(\alpha) \rightarrow T(\beta)$, který lze díky Větě 7.2 rozšířit na T -izomorfismus $\tilde{\varphi} \in \text{Gal}(U/T)$, pro který $\tilde{\varphi}(\alpha) = \beta$. Ovšem podle 8.1(2) máme $\tilde{\varphi}(U) = U$ a tudíž $\beta = \tilde{\varphi}(\alpha) \in U$. \square

Poznamenejme, že předchozí tvrzení slouží jako užitečný nástroj při výpočtu Galoisových grup.

Nyní vyslovíme část tak zvané Hlavní věty Galoisovy teorie, její další části, které popisují jednoznačnou korespondenci mezi Galoisovými rozšířeními a normálními podgrupami Galoisovy grupy, nebudeme v následujícím potřebovat.

Věta 8.6. *Jsou-li $T \subseteq U$ a $U \subseteq V$ Galoisova rozšíření komutativních těles, pak $\text{Gal}(V/U)$ je normální podgrupa grupy $\text{Gal}(V/T)$ a platí, že $\text{Gal}(V/T)/\text{Gal}(V/U)$ je izomorfní $\text{Gal}(U/T)$.*

Důkaz. Definujme zobrazení $\Phi : \text{Gal}(V/T) \rightarrow \text{Gal}(U/T)$ předpisem $\Phi(\sigma) = \sigma|_U$. Potom podle 8.1(2) jde o korektně definované zobrazení, jež je podle Věty 7.2 na. Snadno nahlédneme, že se jedná o grupový homomorfismus jehož jádro je právě množina $\text{Gal}(V/U)$. Nyní už závěr přímočaře plyne z 1. věty o izomorfismu pro grupy. \square

Grupa $G(\cdot)$ se nazývá metabelovská, pokud obsahuje takovou normální podgrupu N , že obě grupy $G/N(\cdot)$ i $N(\cdot)$ jsou komutativní.

Poznámka 8.7. *Nechť T je těleso charakteristiky 0, $a \in T$ a U buď rozkladové nadtěleso polynomu $x^n - a$ nad T . Pak $\text{Gal}(U/T)$ je metabelovská a pro $a = 1$ dokonce komutativní.*

Důkaz. Nejprve uvažujme rozkladové nadtěleso U polynomu $x^n - 1$ nad tělesem T . Nad tělesem charakteristiky 0 tvoří množina všech kořenů polynomu $x^n - 1$ grupu řádu n , která je podle Věty 5.1 cyklická. Označme α nějaký její generátor. Potom je každý homomorfismus $\varphi \in \text{Gal}(U/T)$ jednoznačně určen hodnotou $\varphi(\alpha)$ a navíc $\varphi(\alpha) \in \langle \alpha \rangle$, tedy existuje takové $k \in \mathbb{Z}_n$, že $\varphi(\alpha) = \alpha^k$. Vezmeme-li nyní pro $\varphi, \psi \in \text{Gal}(U/T)$ čísla $k, l \in \mathbb{Z}_n$, pro něž $\varphi(\alpha) = \alpha^k$ a $\psi(\alpha) = \alpha^l$ a jejichž existenci jsme právě dokázali, pak

$$\varphi\psi(\alpha) = \varphi(\alpha^l) = \alpha^{kl} = \psi(\alpha^k) = \psi\varphi(\alpha),$$

a proto $\varphi\psi = \psi\varphi$, tedy $\text{Gal}(U/T)$ je komutativní grupa.

Nyní uvažujme rozkladové nadtěleso U polynomu $x^n - a$ nad tělesem T a označme β nějaký kořen polynomu $x^n - a$. Vidíme, že $\beta\alpha^k$, $k \in \mathbb{Z}_n$, jsou pro generátor α cyklické grupy $\langle \alpha \rangle$ všech kořenů polynomu $x^n - 1$ právě všechny kořeny polynomu $x^n - a$. Položme $U = T(\alpha)$ a $V = U(\beta) = T(\alpha, \beta)$. Pak $T \subseteq U$ a $U \subseteq V$ jsou Galoisova rozšíření a z Věty 8.6 dostáváme izomorfismus $\text{Gal}(V/T)/\text{Gal}(V/U) \cong \text{Gal}(U/T)$. Už jsme dokázali, že je $\text{Gal}(U/T)$ komutativní, zbývá dokázat, že je komutativní i grupa $\text{Gal}(V/U)$. Tentokrát vidíme, že je každý homomorfismus $\varphi \in \text{Gal}(V/U)$ jednoznačně určen hodnotou $\varphi(\beta)$ a navíc $\varphi(\beta)$ je opět kořen polynomu $x^n - a$, tedy existuje číslo $k \in \mathbb{Z}_n$, že $\varphi(\beta) = \beta\alpha^k$. Vezmeme-li si tedy $\varphi, \psi \in \text{Gal}(V/U)$ dostaneme čísla $k, l \in \mathbb{Z}_n$, pro něž $\varphi(\beta) = \beta\alpha^k$ a $\psi(\beta) = \beta\alpha^l$ a platí

$$\varphi\psi(\beta) = \varphi(\beta\alpha^l) = \beta\alpha^{k+l} = \psi(\beta\alpha^k) = \psi\varphi(\beta),$$

a proto $\varphi\psi = \psi\varphi$ a grupa $\text{Gal}(V/U)$ je obdobně jako grupa $\text{Gal}(U/T)$ komutativní. \square

Nahlédneme smysl předchozího tvrzení na dvou příkladech.

Příklad 8.8. (1) Nechť p je prvočíslo. Protože jsou všechny kořeny polynomu $x^p - 1$ mocniny kořenu $e^{\frac{2\pi}{p}}$, je $\mathbb{Q}(e^{\frac{2\pi}{p}})$ rozkladové nadtěleso polynomu $x^p - 1$ nad \mathbb{Q} . Každý \mathbb{Q} -izomorfismus z Galoisovy grupy $\text{Gal}(\mathbb{Q}(e^{\frac{2\pi}{p}})/\mathbb{Q})$ je tedy určen obrazem kořenu $e^{\frac{2\pi}{p}}$ na ostatní kořeny $e^{\frac{2\pi k}{p}}$, tedy z úvah předchozího důkazu vidíme, že je $\text{Gal}(\mathbb{Q}(e^{\frac{2\pi}{p}})/\mathbb{Q})$ izomorfní podgrupě grupy $\mathbb{Z}_p^*(\cdot)$, což je cyklická grupa řádu $p - 1$, tedy i $\text{Gal}(\mathbb{Q}(e^{\frac{2\pi}{p}})/\mathbb{Q})$ je cyklická. Kdybychom dokázali, že je polynom cyklotomický polynom $\frac{x^p - 1}{x - 1} = \sum_{i=0}^{p-1} x^i$ ireducibilní nad \mathbb{Q} (což opravdu platí, ale důkaz zde uvádět nebudeme), pak bychom díky 8.5(1) dostali dokonce grupový izomorfismus $\text{Gal}(\mathbb{Q}(e^{\frac{2\pi}{p}})/\mathbb{Q}) \cong \mathbb{Z}_{p-1}$.

(2) Označme $U = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi}{3}})$. Není těžké nahlédnout, že je U právě rozkladové nadtěleso polynomu $x^3 - 2$ nad \mathbb{Q} , které má právě tři různé komplexní kořeny. To znamená, že je $\text{Gal}(U/\mathbb{Q})$ izomorfní nějaké podgrupě grupy permutací S_3 . Zřejmě $\{\text{id}, \bar{\text{id}}\} \subseteq \text{Gal}(U/\mathbb{Q})$. Uvědomíme-li si, že $x^3 - 2$ je v $\mathbb{Q}[x]$ ireducibilní, a proto podle 8.5(1) existují homomorfismy $\varphi_1, \varphi_2 \in \text{Gal}(U/\mathbb{Q})$, pro něž $\varphi_j(\sqrt[3]{2}) = \sqrt[3]{2}e^{\frac{2\pi j}{3}}$, našli jsme čtyři různé prvky $\text{Gal}(U/\mathbb{Q})$ a tudíž je podle Lagrangeovy věty $\text{Gal}(U/\mathbb{Q}) \cong S_3$.

9. ABELOVA-RUFFINIHO VĚTA

Nyní nejprve formalizujeme vlastnost polynomu, že jeho kořeny nelze vyjádřit pomocí koeficientů a operací v tělese spolu s odmocninami a poté vyslovíme verzi Abelovy-Ruffiniho věty, která říká, že pro každé přirozené $n \geq 5$ existují polynomy stupně n s racionálními koeficienty pro něž neexistuje vzorec na výpočet kořenů.

O grupě $G(\cdot)$ řekneme, že je řešitelná, jestliže existuje taková posloupnost normálních podgrup $\{1\} = N_0 \subset N_1 \subset \dots \subset N_k = G$ grupy $G(\cdot)$, že je faktorová grupa $N_i/N_{i-1}(\cdot)$ komutativní pro všechna $i = 1, \dots, k$.

Příklad 9.1. (1) Každá komutativní i metabelovská grupa je řešitelná.

(2) Permutační grupy $S_3(\circ)$ a $S_4(\circ)$ jsou řešitelné. První je dokonce metabelovská, v druhé stačí uvážit posloupnost normálních podgrup

$$\{1\} \subset \{\text{id}, (12)(34), (13)(24), (14)(23)\} \subset A_4 \subset S_4.$$

(3) Grupa $S_5(\circ)$ (stejně jako všechny ostatní grupy $S_n(\circ)$ pro $n \geq 5$) obsahuje pouze tři normální podgrupy $\{1\}$, A_5 a S_5 , jak lze ukázat elementárními prostředky. A protože $A_5(\circ)$ zřejmě není komutativní grupa, nemůže být $S_5(\circ)$ řešitelná.

Důkaz následujícího základních faktů z pokročilejší teorie grup z časových důvodů vynecháme (Poznamenejme, že jejich důkaz není příliš těžký a jsou k nalezení v téměř každé učebnici teorie grup).

Poznámka 9.2. Je-li $G(\cdot)$ grupa a $\{1\} = N_0 \subset N_1 \subset \dots \subset N_k = G$ posloupnost jejích normálních podgrup, pak je $G(\cdot)$ řešitelná, právě když jsou grupy $N_i/N_{i-1}(\cdot)$ řešitelné pro všechna $i = 1, \dots, k$.

Poznámka 9.3 (Cauchy). Je-li $G(\cdot)$ konečná grupa, jejíž řád dělí prvočíslo p , pak existuje prvek $g \in G$ řádu p tj. $|\langle g \rangle| = p$.

Je-li p prvočíslo, pak jsou v permutační grupě S_p prvky řádu p právě p -cykly.

Řekneme, že polynom $f \in T[x]$ je řešitelný v radikálech nad tělesem T , jestliže existuje posloupnost rozšíření $T = U_0 \subseteq U_1 \subseteq \dots \subseteq U_n$, pro níž je U_{i+1} rozkladové nadtěleso nějakého polynomu $x^{n_i} - a_i$ pro $a_i \in U_i$ nad tělesem U_i pro všechna $i = 0, \dots, n-1$, a rozkladové nadtěleso polynomu f leží v U_n .

Poznamenejme, že je známým faktem, že všechny komplexní polynomy stupně nejvýše čtyři jsou řešitelné v radikálech nad podtělesem generovaným jeho koeficienty (a příslušné vzorce známe nebo můžeme najít v tabulkách).

Nejprve vyslovíme jedno technické pozorování:

Poznámka 9.4. Je-li T těleso charakteristiky 0, $T \subseteq U$ Galoisovo rozšíření a V rozkladové nadtěleso polynomu $x^n - a \in U[x]$ nad tělesem U . Pak existuje takové rozšíření $V \subseteq W$, že $T \subseteq W$ je Galoisovo rozšíření a $\text{Gal}(W/U)$ je řešitelná grupa.

Důkaz. Vezměme si nějaký polynom $f \in T[x]$, jehož rozkladové nadtěleso je právě U , označme $m_a \in T[x]$ minimální polynom prvku a nad T a položme $g := m_a(x^n)$. Nyní si označme W rozkladové nadtěleso polynomu fg nad T . Protože $(x-a)/m_a$ platí, že $(x^n - a)/g$ v oboru $U[x]$, tudíž se polynom $x^n - a$ rozkládá nad tělesem W na kořenové činitele.

Nyní pomocí 9.2 dokážeme, že je grupa $\text{Gal}(W/U)$ řešitelná. Dřív než sestrojíme posloupnost rozšíření jejichž Galoisovy grupy budou tvořit řešitelné normální podgrupy grupy $\text{Gal}(W/U)$, všimneme si, že je kořen ireducibilního polynomu $m_a \in T[x]$ obsažen v Galoisově rozšíření U , což podle 8.5 znamená, že se m_a nad U rozkládá na kořenové činitele. Označme tyto kořeny $\alpha_1, \dots, \alpha_k \in U$, tedy $m_a = \prod_i (x - \alpha_i)$ a tudíž $g = \prod_i (x^n - \alpha_i) \in U[x]$. Nyní indukcí definujme podtěleso W_i tělesa W podmínkou, že $W_0 = U$ a W_i je právě rozkladové nadtěleso polynomu $x^n - \alpha_i$ nad tělesem W_{i-1} pro $i = 1, \dots, k$. Nyní vidíme, že se polynom fg nad tělesem W_k rozkládá na kořenové činitele, dále že rozšíření W_i je rozkladové nadtěleso polynomu $g = \prod_{j < i} (x^n - \alpha_j)$ nad U , tedy $U \subseteq W_i$ je Galoisovo rozšíření a že podle 8.7 je $\text{Gal}(W_i/W_{i-1})$ řešitelná. Použijeme-li nyní opakovaně Větu 8.6, dostáváme, že všechny grupy v řetězci

$$\text{Gal}(W/W_k) \subseteq \text{Gal}(W/W_{k-1}) \subseteq \dots \subseteq \text{Gal}(W/W_1) \subseteq \text{Gal}(W/W_0) = \subseteq \text{Gal}(W/U)$$

jsou normální pogrupy grupy $\text{Gal}(W/U)$ a dále, že

$$\text{Gal}(W_i/W_{i-1}) \cong \text{Gal}(W/W_{i-1})/\text{Gal}(W_i/W_i).$$

To podle 9.2 už nutně znamená, že je grupa $\text{Gal}(W/U)$ řešitelná. \square

Věta 9.5. *Je-li T těleso charakteristiky 0 a V rozkladové nadtěleso polynomu $f \in T[x]$ nad T , pak $|\text{Gal}(V/T)| = [V : T]$ a je-li polynom f řešitelný v radikálech nad T , pak je grupa $\text{Gal}(V/T)$ řešitelná.*

Důkaz. Nejprve si všimněme, že $T \subseteq V$ je podle 6.3(4) rozšíření konečného stupně. Dále dokážeme, že existuje prvek $\gamma \in V$, pro který $T(\gamma) = V$.

Budeme ke sporu předpokládat, že existuje taková dvojice prvků $\alpha, \beta \in V$, že $T(\alpha, \beta) \not\subseteq T(\gamma)$ pro všechna $\gamma \in V$. Označme m_α a m_β minimální polynomy prvků α a β nad T . Podle 8.5(2) se oba polynomy m_α i m_β rozkládají nad V na kořenové činitele, označme $\alpha_1, \dots, \alpha_a \in V$ všechny kořeny m_α a $\beta_1, \dots, \beta_b \in V$ všechny kořeny m_β . Protože existuje pro každou čtveřici i, j, k, l , pro níž $(i, j) \neq (k, l)$ nejvýše jedno řešení lineární rovnice $\alpha_i + x\beta_j = \alpha_k + x\beta_l$ a protože je těleso charakteristiky 0 nekonečné, existuje takové $t \in T$, že $\alpha_i + t\beta_j \neq \alpha_k + t\beta_l$ pro $(i, j) \neq (k, l)$. Zvolme jedno takové t a položme $\gamma := \alpha + t\beta$ a $p := m_\alpha(\gamma - tx)$. Potom $p(\beta) = 0$ a $p(\beta_i) \neq 0$ pro $\beta_i \neq \beta$. Nyní vezměme monický největší společný dělitel polynomů p a m_β v oboru $T(\gamma)[x]$, označme ho q . Potom nutně $x - \beta = q \in T(\gamma)[x]$, proto $\beta \in T(\gamma)$, a tudíž i $\alpha \in T(\gamma)$. Tedy $T(\alpha, \beta) \subseteq T(\gamma)$, obdrželi jsme spor.

Vezměme tedy takové $\gamma \in V$, že $T(\gamma) = V$, a jeho minimální polynom m_γ nad T . Podle 8.5(2) se m_γ rozkládá ve T na kořenové činitele a podle 8.4 m_γ nemá žádné vícenásobné kořeny. Zřejmě je každý T -homomorfismus z $\text{Gal}(V/T)$ určen obrazem prvku γ , ten se přitom musí zobrazit opět na kořen polynomu m_γ . Konečně podle 8.5(2) obraz prvku γ na každý kořen m_γ lze rozšířit T -homomorfismus z $\text{Gal}(V/T)$, což znamená, že

$$|\text{Gal}(V/T)| = \deg m_\gamma = [T(\gamma) : T] = [V : T].$$

Nyní předpokládejme, že je f řešitelný v radikálech nad T , a vezměme příslušnou posloupnost rozšíření $T = U_0 \subseteq U_1 \subseteq \cdots \subseteq U_n$, pro níž je U_{i+1} rozkladové nadtěleso nějakého polynomu $x^{n_i} - a_i$ nad tělesem U_i pro $a_i \in U_i$, kde pro $i = 1, \dots, n$, pro níž máme $V \subseteq U_n$.

Zkonstruujeme nyní pomocí předchozí poznámky dvě posloupnosti rozšíření

$$T = V_0 \subseteq V_1 \subseteq \cdots \subseteq V_{n-1} \subseteq V_n,$$

$$T = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_{n-1} \subseteq V_n$$

tak, aby platilo, že $U_i \subseteq V_i \subseteq W_i$, $T \subseteq W_i$ bylo Galoisovo rozšíření a grupa $\text{Gal}(W_i/W_{i-1})$ byla řešitelná. K tomu ovšem stačí vzít $V_0 = W_0 := U_0 = T$, a dále V_i jako rozkladové nadtěleso polynomu $x^{n_i} - a_i$ nad tělesem W_{i-1} a konečně W_i jako těleso, jehož existenci (a potřebné vlastnosti) nám zaručuje Poznámka 9.4.

Nyní zbývá podobně jako v předchozí poznámce využít Větu 8.6 a Poznámku 9.2, podle nichž jsou všechny normální podgrupy $\text{Gal}(W_n/W_i)$ grupy $\text{Gal}(W_n/T)$ řešitelné, a proto je řešitelná i grupa $\text{Gal}(W_n/T)$.

Konečně $\text{Gal}(V/T) \cong \text{Gal}(W_n/T)/\text{Gal}(W_n/V)$ je podle 9.2 rovněž řešitelná, čímž jsme dokončili důkaz. \square

Pro úplnost poznamenejme, že lze dokázat i obrácenou implikaci z předchozí věty.

Platnost následujícího tvrzení jsme prověřili pro $n = 2$ a 3 v Příkladech 8.3 a 8.8:

Poznámka 9.6. *Bud' p prvočíslo a $f \in \mathbb{Q}[x]$ ireducibilní polynom stupně p , který má $p-2$ reálných a 2 imaginární kořeny. Je-li U rozkladové nadtěleso polynomu f nad \mathbb{Q} , pak $\text{Gal}(U/\mathbb{Q}) \cong S_p$.*

Důkaz. Nejprve si všimněme, že \mathbb{Q} -izomorfismus $\bar{id} \in \text{Gal}(U/\mathbb{Q})$ je právě transpozice dvou komplexních kořenů. Dále podle 9.5 a 6.2 platí pro každý prvek $\alpha \in U$

$$|\text{Gal}(U/\mathbb{Q})| = |U : \mathbb{Q}(\alpha)| \cdot |\mathbb{Q}(\alpha) : \mathbb{Q}|.$$

Vezmeme-li $\alpha \in U$ jako kořen polynomu f , pak podle 6.3(3) $|\mathbb{Q}(\alpha) : \mathbb{Q}| = \deg f = p$, a proto $p/|\text{Gal}(U/\mathbb{Q})|$. To ovšem podle 9.3 znamená, že existuje prvek Galoisovy grupy $\text{Gal}(U/\mathbb{Q})$ řádu p . Uvědomíme-li si, že díky 8.2 je $\text{Gal}(U/\mathbb{Q})$ je izomorfní podgrupě symetrické grupy S_p a že libovolná transpozice a libovolný prvek řádu p , tedy právě p -cyklus už celou grupu S_p generují, dostáváme závěr, že $\text{Gal}(U/\mathbb{Q}) \cong S_p$. \square

Příklad 9.7. Mějme polynom $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$. Snadno spočítáme, že jeho první derivace $f' = 5x^4 - 4$ má právě dva reálné kořeny $\pm \sqrt[4]{\frac{4}{5}}$, pro které máme $f(-\sqrt[4]{\frac{4}{5}}) > 0 > f(\sqrt[4]{\frac{4}{5}})$, tudíž f má právě tři reálné a dva komplexní kořeny. Dále si uvědomme, že reducibilita polynomu f by znamenala i reducibilitu téhož polynomu s koeficienty upravenými modulo 3 v oboru polynom $\mathbb{Z}_3[x]$. Ovšem okamžitě vidíme, že $f \equiv x^5 + 2x + 2 \in \mathbb{Z}_3[x]$ nemá žádné kořeny v \mathbb{Z}_3 a například hrubou silou bychom rychle zjistili, že ho nedělí žádný polynom stupně 2 nad $\mathbb{Z}_3[x]$, což znamená, že je v okruhu $\mathbb{Z}_3[x]$ a tudíž i v $\mathbb{Q}[x]$ ireducibilní. Nyní nám předchozí poznámka říká, že je Galoisova grupa polynomu f , právě celá permutační grupa S_p , a proto podle Poznámky 8.7 a Věty 9.5 polynom f není řešitelný v radikálech.

Předchozí příklad ukazuje platnost následující klasické věty:

Věta 9.8 (Abel-Ruffini). *Pro každé přirozené číslo $n \geq 5$ existují racionální polynomy stupně n které nejsou řešitelné v radikálech nad tělesem \mathbb{Q} .*

Důkaz. Pro každé $n \geq 5$ stačí uvážit polynom $f = x^n - 4x^{n-4} + 2x^{n-5} \in \mathbb{Q}[x]$, který podle Příkladu 9.7 není řešitelný v radikálech nad tělesem \mathbb{Q} . \square

10. KONEČNÁ TĚLESA PO DRUHÉ

Konečná tělesa se nám podařilo minulý semestr zkonstruovat za předpokladu, že existují jisté ireducibilní polynomy. V této kapitole předvedeme obecně fungující konstrukci opírající se o kořenová nadtělesa polynomů. Jejím důsledkem bude i důkaz existence ireducibilních polynomů potřebných ke standardnímu chápání konečných těles. Pozorování týkající se jejich vlastností využijeme poté v další kapitole k jejich algoritmickému nalezení.

Platnost následujícího pozorování jsme si zčásti uvědomili už minulý semestr.

Poznámka 10.1. *Bud' T komutativní těleso (prvočíselné) kladné charakteristiky p , a nechť n je přirozené číslo. Definujme zobrazení $f_{p^n} : T \rightarrow T$ předpisem $f_{p^n}(a) = a^{p^n}$ a množiny $P := \{k \times 1 \mid k \in \mathbb{N}\}$, kde $k \times 1$ je součet k kopií prvku 1 v tělese T , a $Q := \{t \in T \mid f_{p^n}(t) = t\}$. Pak $P \subseteq Q \subseteq U$ jsou podtělesa tělesa T , $P \cong \mathbb{Z}_p$ a f_{p^n} je P -homomorfismus.*

Důkaz. Nejprve uvážíme, že $f_p : T \rightarrow T$, $f_p(a) = a^p$ je okruhový homomorfismus. Okamžitě vidíme, že $0^p = 0$, $1^p = 1$, $(a \cdot b)^p = a^p \cdot b^p$. Dále $(a+b)^p = \sum_{i=0}^p \binom{p}{i} a^i b^{p-i} = a^p + b^p$, protože $p/\binom{p}{i}$ pro každé $i = 1, \dots, p-1$, tedy $\sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i} = 0$. Indukčním argumentem zjistíme, že $f_{p^i} = f_{p^{i-1}} \circ f_p$ je homomorfismus okruhů pro každé kladné i . Přitom se f_{p^i} chová identicky na P , neboť $f_{p^i}(1) = 1$. Proto $(a+b)^{p^n} = f_{p^n}(a+b) = f_{p^n}(a) + f_{p^n}(b) = a^{p^n} + b^{p^n}$, podobně $(-a)^{p^n} = -a^{p^n}$, $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n}$ a například přímým výpočtem zjistíme, že $(a^{-1})^{p^n} = (a^{p^n})^{-1}$ pro každé nenulové a .

Mějme nyní $a, b \in Q$, tj. $(a^{p^n} = a, b^{p^n} = b)$. Pak $(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b$ a podobně $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n} = a \cdot b$, $(-a)^{p^n} = -a^{p^n}$. Je-li navíc $a \neq 0$, potom $(a^{-1})^{p^n} = (a^{p^n})^{-1} = a^{-1}$. čímž jsme ověřili, že $a + b, a \cdot b, -a, a^{-1} \in Q$. Protože $0, 1 \in Q$ zřejmě, vidíme, že Q je podtěleso tělesa T .

Pomocí homomorfismu $\varphi : \mathbb{Z} \rightarrow T$, $\varphi(z) = z \times 1$ a První věty o izomorfismu nahlédneme, že $P \cong \mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$, proto je P těleso \square

Věta 10.2. *Nechť $q \in \mathbb{N}$. Pak existuje komutativní těleso o q prvcích, právě když $q = p^n$ pro nějaké prvočíslu p a přirozené číslo n . Těleso o p^n prvcích je izomorfní rozkladovému nadtělesu polynomu $x^{p^n} - x$ nad \mathbb{Z}_p .*

Důkaz. (\Rightarrow) Vezmeme-li těleso T řádu q a položíme $P = \{k \times 1 \mid k \in \mathbb{N}\}$ víme z 10.1, že T má strukturu konečného vektorového prostoru nad P . Je-li $n = \dim_P(T)$, dostáváme, že $|T| = |P|^n = p^n$.

(\Leftarrow) Ukážeme, že rozkladové nadtěleso T polynomu $x^{p^n} - x$ nad \mathbb{Z}_p má právě p^n prvků. Protože p nedělí $p^n - 1$, nemá polynom $x^{p^n} - x$ podle 4.7(3) žádný vícenásobný kořen. Těleso T tedy obsahuje aspoň p^n prvků. V důsledku 10.1 je

množina $Q = \{t \in T \mid t^{p^n} = t\}$ podtělesem, navíc $t^{p^n} = t$ právě když je t kořen polynomu $x^{p^n} - x$, tedy $|Q| = p^n$ (opět podle 4.7) a $Q = T$.

Vezmeme-li nyní libovolně těleso U o p^n prvcích, pak pro každé $u \in U \setminus \{0\}$ $u^{p^n-1} = 1$ podle 2.6, a proto $u^{p^n} = u$ pro všechna $u \in U$. Využijeme-li dále 10.1, dostaneme, že všechny prvky U jsou kořenem polynomu $x^{p^n} - x$ nad tělesem $P = \{k \times 1 \mid k \in \mathbb{N}\} \cong \mathbb{Z}_p$, tedy U je rozkladové nadtěleso polynomu $x^{p^n} - x$ nad tělesem P . Závěr potom plyne z 7.2 \square

Jednoznačně (až na izomorfismus) určené těleso o p^n prvcích se zpravidla značí $GF(p^n)$ (GF = Galois field) nebo \mathbb{F}_{p^n} .

Poznámka 10.3. *Konečné komutativní těleso T obsahuje podtěleso o q prvcích právě tehdy, když $q \mid |T|$ a $q - 1 \mid |T| - 1$. Takové podtěleso je právě jedno.*

Důkaz. (\Rightarrow) plyne z Lagrangeovy věty použité pro grupy $T(+)$ a $T \setminus \{0\}(\cdot)$.

(\Leftarrow) Podle 10.2 existuje takové prvočíslo p a přirozené číslo $n \mid |T| = p^n$, tedy $q = p^k$ pro vhodné přirozené číslo $k \leq n$. Díky 5.1 víme, že $T \setminus \{0\}(\cdot)$ je cyklická grupa, a proto existuje její jednoznačně určená podgrupa G řádu $q - 1$. Protože $u^{q-1} = 1$ pro každé $u \in G$, obsahuje množina $Q = G \cup \{0\}$ právě všechny kořeny polynomu $x^{p^n} - x$. Tedy $Q = \{u \in T \mid u^q = u\}$ je podtěleso o q prvcích díky 10.1. Jeho jednoznačnost plyne jednoznačností volby grupy G . \square

Poznámka 10.4. *Nechť p je prvočíslo a k, n přirozená čísla a \mathbf{T} těleso. Pak jsou následující tvrzení ekvivalentní:*

- (a) k/n v \mathbb{Z} ,
- (b) $(p^k - 1)/(p^n - 1) \in \mathbb{Z}$,
- (c) $(x^{q^k} - x)/(x^{q^n} - x) \in \mathbf{T}[x]$

Důkaz. (a) \Rightarrow (b) Jestliže $n = kd$, snadno spočítáme, že $p^n - 1 = (p^k - 1) \sum_{i=0}^{d-1} p^{ik}$.

(b) \Rightarrow (a) Nechť $(p^k - 1)/(p^n - 1)$ a $n = kd + r$, kde $0 \leq r < k$. Víme, že $p^{kd} - 1 = (p^k - 1) \sum_{i=0}^{d-1} p^{ik}$, tedy $(p^k - 1)/((p^n - 1) - (p^{kd} - 1))$. Protože $(p^n - 1) - (p^{kd} - 1) = p^{kd}(p^r - 1)$ a čísla $p^k - 1$ a p^{kd} jsou nesoudělná, máme $(p^k - 1)/(p^r - 1)$. Ovšem $r < k$, proto $r = 0$.

(b) \Leftrightarrow (c) Použijeme obdobný argument jako v důkazu (a) \Leftrightarrow (b), je-li totiž $(q^n - 1) = s(q^k - 1)$, pak $(x^{q^n} - x) = x(x^{q^k-1} - 1) \sum_{i=0}^{s-1} x^{i(q^k-1)}$. \square

Spojením charakterizace konečných těles 10.2 a dvou předchozích technických pozorování ukážeme, že konstrukce konečných těles pomocí ireducibilních polynomů zavedená v minulém semestru bude vždy k dispozici.

Věta 10.5. *Pro každé konečné komutativní těleso T a přirozené číslo n existuje nad T ireducibilní polynom stupně n .*

Důkaz. Z 10.2 víme, že $|T| = p^k$ pro vhodné přirozené k a že existuje těleso U , které má p^{nk} prvků. Navíc $(p^k - 1)/(p^{nk} - 1)$ podle 10.4, proto díky 10.3 a 10.2 obsahuje U podtěleso izomorfní T , bez újmy na obecnosti můžeme toto podtěleso s tělesem T ztotožnit. Nyní si stačí uvědomit, že $U \setminus \{0\}(\cdot)$ je cyklická grupa, a zvolit nějaký generátor α grupy $U \setminus \{0\}$. Prvek α je podle 6.3(3) algebraický a $U \setminus \{0\} = \langle \alpha \rangle \subseteq T(\alpha)$, proto $T(\alpha) = U$ a $\deg(m_\alpha) = [U : T] = n$ podle 6.3(1), kde m_α je minimální polynom algebraického prvku α nad T . Konečně m_α je nad T ireducibilní podle 6.1. \square

Poznámka 10.6. *Nechť T je konečné komutativní těleso. Každý ireducibilní polynom stupně n z okruhu $\mathbf{T}[x]$ dělí polynom $x^{|T|^n} - x$.*

Důkaz. Nechť $m \in \mathbf{T}[x]$ ireducibilní polynom stupně n , bez újmy na obecnosti můžeme předpokládat, že je m monický. Položme $q = |T| = p^k$ pro vhodné prvočíslo p a vhodné přirozené k a buď U těleso o p^{kn} prvcích. Podobně jako v důkazu 10.5 můžeme bez újmy na obecnosti ztotožnit těleso T s izomorfním podtělesem tělesa U , které existuje podle 10.3. Těleso U je podle 10.2 rozkladovým nadtělesem polynomu $x^{q^n} - x$ nejen nad tělesem \mathbb{F}_p , nýbrž i nad každým větším podtělesem, tedy i nad tělesem T . Dále podle 5.5 je $(\mathbf{T}[x])_m$ komutativní těleso o p^{kn} prvcích, v němž má polynom m kořen. Protože $(\mathbf{T}[x])_m \cong U$ a izomorfismus lze díky 7.2 vzít tak, aby byl na podtělesech T identický, má m kořen v U , označme ho α . Snadno s pomocí 6.1 nahlédneme, že m je minimálním polynomem prvku α nad tělesem T , a protože je α kořenem polynomu $x^{q^n} - x$, máme $m/(x^{q^n} - x)$ v okruhu $\mathbf{T}[x]$. \square

Věta 10.7. *Nechť T je konečné komutativní těleso, d přirozené číslo a $u \in \mathbf{T}[x]$ ireducibilní polynom stupně n . Položme $q = |T|$. Následující tvrzení jsou ekvivalentní:*

- (a) $(x^{q^n} - x)/(x^{q^d} - x)$ v $\mathbf{T}[x]$,
- (b) $u/(x^{q^d} - x)$ v $\mathbf{T}[x]$,
- (c) n/d v \mathbb{Z} .

Důkaz. (a) \Rightarrow (b) z 10.6 plyne, že $u/(x^{q^n} - x)$ a z tranzitivity relace $/$ dostáváme závěr.

(b) \Rightarrow (c) Opět uvážíme, že rozkladové nadtěleso U polynomu $(x^{q^d} - x)$ nad \mathbb{F}_p má podle 10.2 právě q^d prvků a obsahuje jako podtěleso těleso izomorfní T (a to můžeme ztotožnit) podle 10.3. Protože $u/(x^{q^d} - x)$ existuje nad tělesem U kořen $\alpha \in U$ polynomu u . To znamená, že je minimální polynom m_α algebraického prvku α nad T asociován s polynomem u a tudíž $[T(\alpha) : T] = \deg m_\alpha = \deg u = n$ podle 6.3(1). Proto $|T(\alpha)| = q^n$, tedy $(q^n - 1)/(q^d - 1)$ podle 10.3 a n/d díky 10.4.

(c) \Leftrightarrow (a) Protože $q = p^r$ pro vhodné přirozené r a prvočíslo p podle 10.2, máme $((p^r)^n - 1)/((p^r)^d - 1) \Leftrightarrow rn/rd$ díky 10.4, což zřejmě nastává $\Leftrightarrow n/d$. \square

Uvážíme-li, že se pro každé prvočíslo p polynom $x^{(p^n)^d} - x \in \mathbb{F}_p[x]$ nad svým rozkladovým nadtělesem U podle 4.7(3) rozkládá na různé kořenové činitele, tedy na vzájemně neasociované polynomy, nemohou být vzájemně asociovány ani členy ireducibilního rozkladu $x^{(p^n)^d} - x$ v jakémkoli podtělese tělesa U . Díky předchozí větě dostaneme:

Důsledek 10.8. *Nechť p je prvočíslo, n přirozené číslo a $q = p^n$. Pak polynom $x^{q^d} - x$ je právě součinem všech monických ireducibilních polynomů nad tělesem $GF(q^d)$ všech stupňů k , které dělí d .*

Příklad 10.9. (1) Hledáme-li nerozložitelné polynomy ze $\mathbb{F}_2[x]$ stupně 4, víme z 10.6, že všechny musí dělit polynom $x^{16} - x$, resp. $x^{15} - 1$. Dále nám 10.7 říká, že nerozložitelný polynom stupně k (≤ 4) dělí polynom $x^{16} - x$ právě když $k/4$ (tj. právě když existuje podtěleso šestnáctiprvkového tělesa o 2^k prvcích). Tudíž polynom $x^{16} - x$ budou dělit právě všechny nerozložitelné polynomy stupně 1, 2 a 4. Jediným nerozložitelným polynomem stupně 2 nad tělesem \mathbb{F}_2 je polynom $x^2 + x + 1$. Snadno spočítáme, že $x^{16} - x = x(x - 1)(x^2 + x + 1)(x^{12} + x^9 + x^6 + x^3 + 1)$, tedy polynom $x^{12} + x^9 + x^6 + x^3 + 1$ už nutně musí být součinem všech nerozložitelných

polynomů stupně 4 (zřejmě existují právě 3). Dopočítáme, že $x^{12} + x^9 + x^6 + x^3 + 1 = (x^4 + x^3 + x^2 + x + 1)(x^4 + x^3 + 1)(x^4 + x + 1)$.

(2) Protože těleso o 2^7 prvcích obsahuje pouze vlastní podtěleso o 2 prvcích (7 je totiž prvočíslo), je polynom $x^{128} - x$ nad \mathbb{F}_2 součinem právě všech ireducibilních polynomů stupně 1 (takové jsou právě 2) a stupně 7. Proto nad \mathbb{F}_2 existuje právě $18 = \frac{128-2}{7}$ nerozložitelných polynomů stupně 7.

(3) Spočítáme pomocí 10.7 neasociované nerozložitelné polynomy stupně šest nad tělesem \mathbb{F}_3 . Víme, že polynom $x^{729} - x$ se rozkládá na součin všech vzájemně neasociovaných (mají totiž různé kořeny) ireducibilních polynomů stupně $k/6$, tedy rozklad $x^{729} - x$ na ireducibilní činitele obsahuje právě polynomy stupně 1, 2, 3 a 6. Zřejmě máme právě 3 neasociované ireducibilní polynomy stupně 1 a snadno spočteme (např. stejným postupem pro polynom $x^9 - x$), že existují rovněž 3 neasociované neireducibilní polynomy stupně 2. Konečně pomocí rozkladu polynomu $x^{27} - x$ na nerozložitelné polynomy (stejnou metodou) zjistíme, že existuje až na asociovanost $8 = \frac{27-(3 \cdot 1)}{3}$ neireducibilních polynomů stupně 3. Tedy snadno dopočítáme, že neasociovaných ireducibilních polynomů stupně 6 nad \mathbb{F}_3 existuje právě $116 = \frac{729-(3 \cdot 1+3 \cdot 2+8 \cdot 3)}{6}$.

11. IREDUCIBILNÍ ROZKLAD POLYNOMŮ

Nyní předvedeme algoritmus na ireducibilní rozklad polynomů nad konečnými tělesy, který nám díky Důsledku 10.8 umožní efektivně najít ireducibilní polynomy daného stupně n nad konečným tělesem řádu q jako ireducibilní faktory polynomu $x^q - x$.

Definice. Řekneme, že polynom f je *bez čtverců*, jestliže neexistuje žádný takový polynom g (nad tímž tělesem) kladného stupně, aby g^2/f . Je-li $f = \prod_{i=1}^n f_i^i$, kde všechny polynomy f_i jsou bez čtverců, mluvíme o *bezčtvercovém rozkladu* polynomu f .

Poznámka 11.1. Pro každý polynom nad komutativním tělesem existuje (až na asociovanost jednoznačný) bezčtvercový rozklad.

Důkaz. Bezprostřední důsledek 3.3 spolu s 3.5. □

Poznámka 11.2. Nechť T je komutativní těleso, $f \in T[x]$. Pak je f bez čtverců právě když 1 je $\text{GCD}(f, f')$.

Důkaz. Jestliže $f = g^2h$, pak podle 4.7(3) $f' = g \cdot (gh)' + g' \cdot gh = g \cdot ((gh)' + g'h)$, tedy g/f' .

Předpokládejme, že 1 není $\text{GCD}(f, f')$, tedy 4.7(2) existuje ireducibilní polynom g , který dělí f' i f , tj. $f = g \cdot a$, $f' = g \cdot b$. Protože $g \cdot b = f' = (g \cdot a)' = g \cdot a' + g' \cdot a$ a protože g a g' jsou nesoudělné, dostáváme, že g/a a tedy g^2/f . □

Bezčtvercový rozklad polynomu nad tělesem kladné charakteristiky

VSTUP: $f \in T[x] \setminus T$, pro $p = \text{charakteristika } T$

VÝSTUP: f_1, \dots, f_k , pro které $f = \prod_{i=1}^n f_i^i$ je bezčtvercový rozklad.

0. $c_1 := \text{GCD}(f, f')$; $g_1 := \frac{f}{c_1}$; $i := 1$;

1. while $\text{deg}(g_i > 0)$ do $\{g_{i+1} := \text{GCD}(c_i, g_i)$; $c_{i+1} := \frac{c_i}{g_i}$; $f_i := \frac{g_i}{g_{i+1}}$; $i++\}$

2. $c := c_{i-1} = \sum_i a_i x^i$;
3. if $\deg c > 0$ then $(f_p, f_{2p}, \dots) :=$ zavolej rekurzivně algoritmus pro vstup $\sqrt[p]{c} = \sum_i a_{ip} x^i$;
4. return f_1, f_2, \dots

Poznámka 11.3. Algoritmus bezčtvercového rozklad polynomu nad tělesem kladné charakteristiky funguje správně.

Důkaz. Necht' $f = \prod_{i=1}^n f_i^i$ je bezčtvercový rozklad. Potom

$$f' = \left[\sum_{i \notin p\mathbb{N}} i f_i' f_i^{i-1} \cdot \prod_{j \notin p\mathbb{N} \cup \{i\}} f_j^j \right] \cdot \left[\prod_{i \in p\mathbb{N}} f_i^i \right],$$

a proto

$$c_1 = \text{GCD}(f, f') = \left[\prod_{j \notin p\mathbb{N}} f_j^{j-1} \right] \cdot \left[\prod_{i \in p\mathbb{N}} f_i^i \right].$$

Odtud dostáváme, že $g_1 = \prod_{j \notin p\mathbb{N}} f_j$ a $g_2 = \prod_{j \geq 2, j \notin p\mathbb{N}} f_j$.

Podobně nahlédneme, že

$$c_k = \left[\prod_{j \geq k, j \notin p\mathbb{N}} f_j^{j-1} \right] \cdot \left[\prod_{i \in p\mathbb{N}} f_i^i \right]$$

a že $g_k = \prod_{j \geq k, j \notin p\mathbb{N}} f_j$. Odtud vidíme, že $\frac{g_k}{h_k} = f_k$ pokud p nedělí k a $\frac{g_k}{h_k} = 1$ v opačném případě. Tedy našli jsme členy bezčtvercového rozkladu pro všechna i , jež nejsou dělena číslem p . Navíc po konečných krocích dostaneme

$$c_n = \left[\prod_{i \in p\mathbb{N}} f_i^i \right] = \sum_i a_i x^{ip} = \left(\sum_i a_i x^i \right)^p.$$

Zbytek už plyne z rekurze algoritmus na polynom $\sum_i a_i x^i$, kdy najdeme členy f_i bezčtvercového rozklad pro p/i , jestliže p^2 nedělí i . \square

Poznámka 11.4 (Čínská věta o zbytcích). Mějme konečné komutativní těleso T , navzájem nesoudělné ireducibilní polynomy $f_1, \dots, f_n \in \mathbf{T}[x]$ a položme $f = \prod_{i=1}^n f_i$. Pak je zobrazení $\varphi : \mathbf{T}[x]/fT[x] \rightarrow \prod_{i=1}^n T[x]/f_iT[x]$ dané předpisem $\varphi([g]_f) = ([g]_{\text{mod}f_1}, \dots, [g]_{\text{mod}f_n})$ okruhový izomorfismus.

Důkaz. Obdobný jako u Čínské věty o zbytcích pro okruh celých čísel. \square

Věta 11.5. Bud' T konečné komutativní těleso a f monický bezčtvercový polynom. Označme $V = T[x]/fT[x]$ a $W = \{u \in V \mid u^{|T|} = u\}$.

- (1) V je vektorový prostor nad tělesem T a W jeho podprostor.
- (2) Je-li f součinem k ireducibilních polynomů, pak $\dim_T W = k$.
- (3) Je-li $[u]_f \in W$ a $1 \leq \deg u \leq \deg f$, potom $f = \prod_{s \in T} \text{GCD}(u - s, f)$.
- (4) Je-li $[u_1]_f \dots [u_k]_f$ báze vektorového prostoru W a g a h dva neasociované ireducibilní faktory f , potom existuje takové $i \leq k$ a $s \in T$, že g dělí $(w_i - s)$ a h nedělí $(w_i - s)$.

Důkaz. (1) V je komutativní grupou s přirozeně definovaným násobením skalářem, o němž snadno nahlédneme, že tvoří na V strukturu vektorového prostoru. Abychom dokázali, že je W jeho podprostor, stačí podobně jako v 10.1 využít toho, že zobrazení $u \rightarrow u^{|T|}$ tvoří endomorfismus na $T[x]$ a tedy i na $V = T[x]/fT[x]$. Ovšem z 10.2 plyne, že $t^{|T|} = t$ pro každé $t \in T$ a $(a+b)^p = a^p + b^p$, kde $a, b \in T[x]$ a $|T| = p^n$ pro prvočíslo p , protože je p charakteristika okruhu $T[x]$, tudíž i $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.

(2) Bud' $f = f_1 \cdots f_k$ rozklad f na monické ireducibilní polynomy a označme $V_i = T[x]/f_i T[x]$ a $W_i = \{u \in V_i \mid u^{|T|} = u\}$. Podle 11.4 je zobrazení $\varphi : V \rightarrow \prod_{i=1}^k V_i$ dané předpisem $\varphi([v]_f) = ([v]_{f_1}, \dots, [v]_{f_n})$ izomorfismus okruhů (a zřejmě i vektorových prostorů) V a $\prod_{i=1}^k V_i$. Vidíme, že $\varphi(W) \subseteq \prod_{i=1}^k W_i$ ($\subseteq \prod_{i=1}^k V_i$). Protože dále pro každé $(w_1, \dots, w_k) \in \prod_{i=1}^k W_i$, existuje vzor $w \in V$, tj. $\varphi(w) = (w_1, \dots, w_k)$, přičemž $\varphi(w^{|T|}) = (w_1^{|T|}, \dots, w_k^{|T|}) = (w_1, \dots, w_k) = \varphi(w)$, tedy $\varphi(W) = \prod_{i=1}^k W_i$. Konečně si všimněme, že každý okruh V_i je těleso a W_i jeho podtěleso o nejvýše $|T|$ prvcích díky 10.1 a zároveň je W_i nenulový vektorový $|T|$ -prostor, má tedy právě $|T|$ prvků. Tím jsme ověřili, že $|W| = |\prod_{i=1}^k W_i| = |T|^k$, proto je $\dim_T(W) = k$.

(3) Využijeme-li faktu, že okruhy W_i jsou $|T|$ -prvková tělesa a φ indukuje okruhový izomorfismus W a $\prod_{i=1}^k W_i$, pro každý prvek $w \in W$ dostáváme $w^{|T|} - w = \prod_{s \in T} (w - s) = 0$, kde ztotožníme prvky tělesa T a rozkladové třídy $[sx^0]_f$. Je-li tedy $[u]_f = w \in W$, platí, že $f / \prod_{s \in T} (u - s)$, proto $f / \prod_{s \in T} \text{GCD}(u - s, f)$. Jelikož jsou polynomy $u - s$ a $u - t$ pro $t \neq s$ nesoudělné, dostáváme $\prod_{s \in T} \text{GCD}(u - s, f) / f$, a protože jsou oba polynomy monické dostáváme dokonce rovnost.

(4) Bez újmy na obecnosti oddělíme například polynomy f_1 a f_2 . Protože $\omega = ([1], [0], \dots, [0]) \in \prod_{i=1}^k W_i$, existuje polynom w , pro nějž $[u] \in W$ a $\varphi([u]) = \omega$. To znamená, že $f_1/u - 1$ a f_2/u , proto f_2 nedělí $u - 1$. Podle (3) plyne, že f_1 nedělí $u - s$ pro žádné $s \in T \setminus \{1\}$, tedy a $f_1 f_2$ nedělí $u - s$ pro žádné $s \in T$. Předpokládejme nyní, že pro každé i existuje takové $s_i \in T$, že $f_1 f_2 / (u_i - s_i)$ a vezmeme T -lineární kombinaci $u = \sum_{i=1}^k a_i u_i$. Potom $f_1 f_2 / \sum_{i=1}^k a_i (u_i - s_i) = u - \sum_{i=1}^k a_i s_i$, čímž dostáváme spor. Dokázali jsme, že existuje takové i , že $f_1 f_2$ nedělí $(u_i - s)$ pro žádné $s \in T$. Nyní zbývá pomocí (3) zvolit $s \in T$, pro nějž $f_1 / (u_i - s)$. \square

Následující algoritmus využívá předchozí věty, konkrétně nalezení báze vektorového prostoru W , k rozkladu bezčtvercového polynomu nad konečným tělesem:

Berlekampův algoritmus

VSTUP: $f \in T[x] \setminus T$, bez čtverců, kde T je konečné těleso.

VÝSTUP: g_1, \dots, g_k , ireducibilní rozklad f .

0. $n := \deg f$; $q := |T|$; $\sum_{i=1}^n q_i x^{i-1} := (x^q)^{j-1} \pmod f =$
1. spočítej bázi (u_1, \dots, u_n) řešení soustavy rovnic $(Q - I_n)u = 0$, kde $u_1 = (1, 0, \dots, 0)^T$;
2. $i := 2$; $F := \{f\}$
3. while $|F| < n$ do {nahrad' každé $g \in F$ netriviálními faktory rozkladu $g = \prod_{s \in T} \text{GCD}(u_i - s, g)$; i^{++} }
4. return F

Poznámka 11.6. Berlekampův algoritmus funguje správně.

Důkaz. Plyne přímo z Věty 11.5. \square

Na závěr poznamenejme, že nám Důsledek 10.8 umožňuje snadno formulovat algoritmus ještě jednoho typu rozkladu polynomu, který je užitečný v jiných variantách ireducibilní faktorizace. Konkrétně pro rostoucí $i > 0$ budeme pro bezčtvercový polynom $f \in T[x]$, kde $q = |T|$, počítat polynomy $h_i := \text{GCD}(f, x^q - x)$; $f :=$

$\frac{f}{h_i}$, pak budou všechny ireducibilní faktory jednotlivých polynomů h_i vždy právě stupně i .

12. VOLNÉ ALGEBRY

Na závěr celého kurzu se vrátíme k obecnému konceptu obecných algeber daného typu a ukážeme, že každou algebru můžeme dostat faktorizací základního typu algeber, jimž se říká volné.

Připomeňme, že pro množinu I , se zobrazení $\Omega : I \rightarrow \mathbb{N}$ říká *typ*. Algebra $A(\alpha_i | i \in I)$ je typu Ω , pokud pro každé $i \in I$ je α_i právě $\Omega(i)$ -ární operací.

Definice. Bud' $\Omega : I \rightarrow \mathbb{N}$ nějaký typ, X množina a necht' indexovaná množina symbolů operací $\{\alpha_i | i \in I\}$ je disjunktní s X . Definujme indukci posloupnost množin W_i :

$$W_0 = \{\alpha_i | i \in I, \Omega(i) = 0\} \cup X \text{ a}$$

$$W_{n+1} = \{(\alpha_i, w_1, \dots, w_{\Omega(i)}) | i \in I, w_j \in W_n, \Omega(i) \neq 0\} \cup W_n.$$

Položme $W_\Omega(X) = \bigcup_{n \in \mathbb{N}} W_n$ a definujme pro každé $i \in I$ na množině $W_\Omega(X)$ $\Omega(i)$ -ární operaci α_i předpisem $\alpha_i(w_1, \dots, w_{\Omega(i)}) = (\alpha_i, w_1, \dots, w_{\Omega(i)})$. Potom algebru $W_\Omega(X)(\alpha_i | i \in I)$ (typu Ω) nazveme (absolutně volnou) *algebrou termů* nad X typu Ω .

Příklad 12.1. Bud' $X = \{x\}$ jednoprvková množina písmen, $I = \{*\}$ a $\Omega(*) = 1$, tedy uvažujeme jednu unární operaci. Potom $W_\Omega(X) = \{x, (\alpha_*, x), (\alpha_*, \alpha_*, x), \dots\}$, proto je $W_\Omega(X)$ nekonečná.

Poznámka 12.2. Necht' $\Omega : I \rightarrow \mathbb{N}_0$ nějaký typ a X je množina. Potom X generuje algebru termů $W_\Omega(X)(\alpha_i | i \in I)$.

Důkaz. Dokážeme indukci podle n , že $W_n \subseteq \langle X \rangle$. Zřejmě $W_0 \subseteq \langle X \rangle$. Necht' $W_n \subseteq \langle X \rangle$. Vezmeme-li $i \in I$, pro něž $\Omega(i) \neq 0$, a $w_1, \dots, w_{\Omega(i)} \in W_n \subseteq \langle X \rangle$, pak $(\alpha_i, w_1, \dots, w_{\Omega(i)}) = \alpha_i(w_1, \dots, w_{\Omega(i)}) \in \langle X \rangle$, proto $W_{n+1} \subseteq \langle X \rangle$. \square

Poznámka 12.3. Bud' $\Omega : I \rightarrow \mathbb{N}_0$ typ, X množina a $A(\alpha_i | i \in I)$ algebra typu Ω . Pak pro každé zobrazení $\varphi : X \rightarrow A$ existuje právě jeden homomorfismus $\bar{\varphi} : W_\Omega(X) \rightarrow A$ tak, že $\bar{\varphi}|_X = \varphi$.

Důkaz. Budeme induktivně rozšiřovat zobrazení φ na množiny W_n . Nejprve definujme $\varphi_0 : W_0 \rightarrow A$ předpisem $\varphi_0(x) = \varphi(x)$ pro všechna $x \in X$ a $\varphi_0(\alpha_i) = \alpha_i$ pro všechna taková i , pro něž $\Omega(i) = 0$. Máme-li definováno $\varphi_n : W_n \rightarrow A$ rozšíříme ho na $\varphi_{n+1} : W_{n+1} \rightarrow A$ $\varphi_{n+1}(\alpha_i, w_1, \dots, w_{\Omega(i)}) = \alpha_i(\varphi_n(w_1), \dots, \varphi_n(w_{\Omega(i)}))$, jestliže $i \in I$, $\Omega(i) \neq 0$ a $w_1, \dots, w_{\Omega(i)} \in W_n$. Konečně položme $\bar{\varphi} = \bigcup_n \varphi_n$. Z konstrukce je zřejmé, že jde o jedinou možnou definici rozšiřujícího homomorfismu. \square

Věta 12.4. Každá algebra daného typu Ω je homomorfním obrazem algebry $W_\Omega(X)$ pro nějakou množinu X .

Důkaz. Stačí vzít za X libovolnou množinu generátorů (například celou algebru) a identitu na X rozšířit podle 12.3 na příslušný homomorfismus. \square

Poznámka 12.5. Necht' Ω je typ a X a Y množiny. Pak je algebra termů $W_\Omega(X)$ nad X izomorfní algebře termů $W_\Omega(Y)$ nad Y právě tehdy, když existuje bijekce mezi X a Y (tj. $|X| = |Y|$).

Důkaz. (\Rightarrow) Vezměme nějaký izomorfismus $\varphi : W_\Omega(X) \rightarrow W_\Omega(Y)$. Nejprve dokážeme, že $\varphi(X) \subseteq Y$. Předpokládejme, že existuje $x \in X$, pro které $\varphi(x) = w \notin Y$, tj. buď existuje $i \in I$, pro něž $\Omega(i) = 0$ a $w = \alpha_i$ nebo existuje $n > 0$, pro něž $w \in W_n \setminus W_{n-1}$. První možnost je ovšem ve sporu s prostotou φ , protože $\varphi(x) = \varphi(\alpha_i)$, a protože $w = \alpha_j(w_1, \dots, w_{\Omega(j)})$ pro $j \in I$ a $w_k \in W_{n-1}$, dostáváme $x = \alpha_j(\varphi^{-1}(w_1), \dots, \varphi^{-1}(w_{\Omega(j)})) \notin W_0$, což rovněž není možné. Tedy $\varphi(X) \subseteq Y$ a stejným argumentem pro inverzní izomorfismus obdržíme $\varphi^{-1}(Y) \subseteq X$, tudíž φ indukuje bijekci mezi X a Y .

(\Leftarrow) Máme-li bijekci $b : X \rightarrow Y$ můžeme ji podle 12.3 rozšířit na homomorfismus $\varphi : W_\Omega(X) \rightarrow W_\Omega(Y)$ a její inverz $b^{-1} : Y \rightarrow X$ na homomorfismus $\psi : W_\Omega(Y) \rightarrow W_\Omega(X)$. Z jednoznačnosti rozšíření identity na X resp. Y na endomorfismus na $W_\Omega(X)$, resp. $W_\Omega(Y)$ plyne, že $\varphi\psi = Id$ a $\psi\varphi = Id$, tedy φ je izomorfismus. \square

13. VARIETY ALGEBER

V poslední kapitole ukážeme, že třídy algeber splňujících nějaký systém rovností lze charakterizovat právě jako třídy uzavřené na podalgebry, homomorfní obrazy a součiny.

Připomeňme definici součinnové algebry. Mějme $n \in \mathbb{N}$, neprázdný systém množin A_j , $j \in J$ a systém n -árních operací α_i na A_j . Definujme operaci $\prod_{j \in J} \alpha_i$ na $\prod_{j \in J} A_j$ vztahem

$$\left[\prod_{j \in J} \alpha_i(f_1, \dots, f_{\Omega(i)}) \right](j) = \alpha_i(f_1(j), \dots, f_{\Omega(i)}(j)),$$

kde $f_i \in \prod_{j \in J} A_j$.

Snadno nahlédneme, že $\prod_{j \in J} A_j (\prod_{j \in J} \alpha_i \mid i \in I)$ opět algebra typu Ω (mluvíme o *součinu algeber*), je-li $A_j (\alpha_i \mid i \in I)$ neprázdný systém algeber stejného typu Ω .

Definice. Necht' Ω je typ a X je nekonečná spočetná množina. *Identitou* nazveme libovolnou dvojici $(u, w) \in W_\Omega(X) \times W_\Omega(X)$. Řekneme, že algebra A typu Ω *splňuje identitu* (u, w) , pokud pro každý homomorfismus $\varphi : W_\Omega(X) \rightarrow A$ je $\varphi(u) = \varphi(w)$. Třídou \mathcal{V} algeber typu Ω nazveme *varietou*, existuje-li množina identit M tak, že \mathcal{V} je tvořena právě všemi algebry typu Ω splňujícími všechny identity z M .

Příklad 13.1. 1) Třída všech grup tvoří varietu (přitom tato varieta splňuje identity $(x \cdot (y \cdot z), (x \cdot y) \cdot z)$, $(x \cdot 1, x)$, $(1 \cdot x, x)$ a $(x \cdot x^{-1}, 1)$).

2) Třída všech komutativních grup tvoří varietu (k identitám grupy přibude ještě komutativita: $(x \cdot y, y \cdot x)$).

3) Třída všech okruhů tvoří varietu.

Věta 13.2 (Birkhoff). *Třída \mathcal{V} algeber typu Ω je varieta právě tehdy, když je \mathcal{V} uzavřená na všechny podalgebry, homomorfní obrazy a součiny algeber z \mathcal{V} .*

Důkaz. (\Rightarrow) Necht' \mathcal{V} je varieta s množinou identit M . Zvolme $A \in \mathcal{V}$ a vezměme nějakou podalgebru B algebry A . Označme $i : B \rightarrow A$ inkluzi množin a všimněme si, že je i homomorfismus. Máme-li nyní $(u, w) \in M$ a libovolný homomorfismus $\varphi : W_\Omega(X) \rightarrow B$, pak $i\varphi$ je homomorfismus $W_\Omega(X)$ do A , proto $i\varphi(u) = i\varphi(w)$. Ovšem i je prosté zobrazení, tedy $\varphi(u) = \varphi(w)$.

Nyní vezměme homomorfismus $\psi : A \rightarrow B$, kde opět $A \in \mathcal{V}$, $(u, w) \in M$ a homomorfismus $\varphi : W_\Omega(X) \rightarrow \psi(B)$. Pro každé $x \in X$ definujme zobrazení $\mu :$

$X \rightarrow A$ podmínkou $\mu(x) \in \psi(\varphi(x))^{-1}$. Zobrazení μ můžeme podle 12.3 rozšířit na homomorfismus $\bar{\mu} : X \rightarrow \psi(B)$, pro nějž $\psi\bar{\mu} = \varphi$. Protože $\bar{\mu}(u) = \bar{\mu}(w)$, dostáváme i $\varphi(u) = \psi\bar{\mu}(u) = \bar{\mu}(w) = \varphi(w)$, tedy $\psi(B) \in \mathcal{V}$.

Konečně mějme systém algeber $A_j \in \mathcal{V}$, kde $j \in J$, a homomorfismus $\varphi : W_\Omega(X) \rightarrow \prod_{j \in J} A_j$ a $(u, w) \in M$. Označme $\pi_k : \prod_{j \in J} A_j \rightarrow A_k$ pro každé $k \in J$ přirozenou projekci na k -tou složku a všimněme si, že se jedná o homomorfismus. Protože $\pi_k \varphi(u) = \pi_k \varphi(w)$ pro každé $k \in J$, je podle definice součinu algeber $\varphi(u) = \varphi(w)$.

(\Leftarrow) Vezměme množinu všech identit M , které splňuje každá algebra a dále označme \mathcal{U} varietu všech algeber splňujících M . Zřejmě $\mathcal{V} \subseteq \mathcal{U}$.

Nejprve zvolme libovolnou algebru $A \in \mathcal{U}$. Díky 12.4 existuje množina Y a homomorfismus $p : W_\Omega(Y) \rightarrow A$ na celou algebru A . Uvážíme množinu R všech kongruencí ρ na $W_\Omega(Y)$, pro něž $W_\Omega(Y)/\rho \in \mathcal{V}$. Vidíme, že $\prod_{\rho \in R} W_\Omega(Y)/\rho \in \mathcal{V}$ podle předpokladu a dále přirozeně definované zobrazení $\psi : W_\Omega(Y) \rightarrow \prod_{\rho \in R} W_\Omega(Y)/\rho$ je homomorfismus. Proto pro kongruenci $\rho_Y = \bigcap_{\rho \in R} \rho$ pomocí 1. věty o izomorfismu dostáváme vztah $W_\Omega(Y)/\rho_Y = W_\Omega(Y)/\ker \psi \cong \psi(W_\Omega(Y))$, tedy $W_\Omega(Y)/\rho_Y$ je podalgebra součinnové algebry z \mathcal{V} , tedy i $W_\Omega(Y)/\rho_Y \in \mathcal{V}$ a ρ_Y je nejmenší kongruence na $W_\Omega(Y)$, pro níž $W_\Omega(Y)/\rho_Y \in \mathcal{V}$.

Nyní obměnou ukážeme, že $\rho_Y \subseteq \ker p$. Vezměme (a, b) , aby platilo, že $p(a) \neq p(b)$ a necht' X je spočetná (stačí samozřejmě konečná) podmnožina Y , která obsahuje všechna písmena termů z a a b . Protože $W_\Omega(X) \subseteq W_\Omega(Y)$ a restrikce p na $W_\Omega(X)$ indukuje homomorfismus $W_\Omega(X) \rightarrow A$, identita (a, b) na A není splněna, proto existuje algebra $B \in \mathcal{V}$ a takový homomorfismus $f : W_\Omega(X) \rightarrow B$, že $f(a) \neq f(b)$, který můžeme díky 12.3 rozšířit (na $Y \setminus X$ zobrazení dodefinujeme libovolně) na homomorfismus $f : W_\Omega(Y) \rightarrow B$. To znamená, že $(a, b) \notin \rho_Y$ a inkluze $\rho_Y \subseteq \ker p$ tím máme ověřenu.

Konečně použitím 1. věty o izomorfismu dostáváme, že $A \cong W_\Omega(Y)/\ker p$. Ta je ovšem izomorfní faktorové algebře algebry $W_\Omega(Y)/\rho_Y$, konkrétně díky 2. větě o izomorfismu máme

$$A \cong W_\Omega(Y)/\ker p \cong (W_\Omega(Y)/\rho_Y)/(\ker p/\rho_Y)$$

Proto z uzavřenosti \mathcal{V} na faktory dostáváme, že $A \in \mathcal{V}$. \square

Uvědomíme-li si, že homomorfní obraz algebry je podle První věty o izomorfismu izomorfní faktorů původní algebry, dostáváme reformulaci Birkhoffovy věty:

Důsledek 13.3. *Třída \mathcal{V} algeber typu Ω je varieta právě tehdy, když je \mathcal{V} uzavřená na všechny podalgebry, součiny a faktorizaci.*

Příklad 13.4. (1) Třída všech těles není podle Birkhoffovy věty varietou, neboť součin dvou těles (např. $\mathbb{Z}_2 \times \mathbb{Z}_2$) není tělesem.

(2) Třídy všech grup chápaných jako algebry typu $(1, 1, 1)$, komutativních grup, či okruhů jsou variety, protože jsou uzavřené na součiny, podalgebry i homomorfní obrazy.