ALGEBRA II PRO INFORMATIKY

6. Komutativní okruhy

Uvažujme obor integrity $R(+,\cdot,-,0,1)$, a definujme algebru $F(+,\cdot,-,\mathbf{0},\mathbf{1})$, kde $F = R\times(R\setminus\{0\})$ s operacemi: $(a,b)\cdot(c,d) = (a\cdot c, b\cdot d)$, $(a,b)+(c,d) = (a\cdot d + b\cdot c, b\cdot d)$, $-(a,b) = (-a,b)$, $\mathbf{0} = (0,1)$ a $\mathbf{1} = (1,1)$. Na algebře $F(+,\cdot,-,\mathbf{0},\mathbf{1})$ konečně definujme relaci $\sim$ předpisem $(a,b)\sim(c,d) \Leftrightarrow a\cdot d = b\cdot c$.

Věta 6.1. *Pro algebru $F(+,\cdot,-,\mathbf{0},\mathbf{1})$ platí:*

1. *$F(+)$ a $F(\cdot)$ jsou komutativní monoidy,*
2. *$\sim$ je kongruence na $F(+,\cdot,-,\mathbf{0},\mathbf{1})$ a $(0,a)\sim\mathbf{0}$ a $(a,a)\sim\mathbf{1}$ pro každé $a\in R\setminus\{0\}$,*
3. *$F/\sim$ je komutativní těleso,*
4. *zobrazení $\sigma: R\to F/\sim$ dané předpisem $\sigma(r) = [(r,1)]_\sim$ je prostý okruhový homomorfismus.*

Důkaz. Vezměme $(a,b),(c,d),(e,f)\in F$.

(1) Postupujeme zcela přímočaře podle definice.

$$(a,b)+((c,d)+(e,f)) = (a,b)+((cf+de,df)) = ((adf+b(cf+de),bdf)) =$$

$$= ((adf+bcf+bde,bdf)) = (((ad+bc)f+bde,bdf)) = ((a,b)+(c,d))+(e,f),$$

$$(a,b)+(c,d) = (ad+bc,bd) = (cb+ad,dd) = (c,d)+(a,b).$$

Ověřili jsme, že je operace $+$ asociativní a komutativní. Uvážíme-li, že $(a,b)+(0,1) = (a,b)$, máme dokázáno, že $F(+)$ je komutativní monoid. Totéž provedeme pro násobení:

$$(a,b)\cdot((c,d)\cdot(e,f)) = (a,b)\cdot((ce,df)) = (ace,bdf)) = ((a,b)\cdot(c,d))\cdot(e,f),$$

dále $(a,b)\cdot(c,d) = (c,d)\cdot(a,b)$ a $(a,b)\cdot(1,1) = (a,b)$, proto i $F(\cdot)$ je komutativní monoid.

(2) Předně uvažme, že je relace $\sim$ zřejmě reflexivní a symetrická a předpokládejme, že $(a,b)\sim(c,d)$ a $(c,d)\sim(e,f)$, tedy $ad = bc$ a $cf = de$. Potom $adf = bcf = bde$, a proto $(af-be)d = 0$. Jelikož $d\neq 0$, dostáváme z definice oboru integrity, že $af-be = 0$, a tudíž $(a,b)\sim(e,f)$. Díky pozorování Příkladu 3.3 z minulého semestru zbývá ověřit slučitelnost $\sim$ s operacemi $+$, $\cdot$ a $-$. Předpokládejme, že $(a_i,b_i)\sim(c_i,d_i)$ tedy $a_id_i = c_ib_i$ pro $i = 1,2$. Proto $(a_1b_2+b_1a_2)d_1d_2 = a_1d_1\cdot b_2d_2 + a_2d_2\cdot b_1d_1 = c_1b_1\cdot b_2d_2 + c_2b_2\cdot b_1d_1 = (c_1d_2+d_1c_2)b_1b_2$, tedy $(a_1,b_1)+(a_2,b_2)\sim(c_1,d_1)+(c_2,d_2)$. Dále $a_1a_2d_1d_2 = c_1c_2b_1b_2$, tudíž $(a_1,b_1)\cdot(a_2,b_2)\sim(c_1,d_1)\cdot(c_2,d_2)$ a konečně $(-a_1,b_1)\sim(-c_1,d_1)$ podle 5.2(2). Vztahy $(0,a)\sim\mathbf{0}$ a $(a,a)\sim\mathbf{1}$ plynou okamžitě z definice $\sim$.

(3) Díky (1), (2) a 3.9 už víme, že $F/\sim(+)$ a $F/\sim(\cdot)$ jsou komutativní monoidy. Zbývá tedy dokázat existenci inverzů v monoidech $F/\sim(+)$ a $F/\sim\setminus\{[\mathbf{0}]\}(\cdot)$ a distributivitu operace $+$ vzhledem k $\cdot$ na množině $F/\sim$. Označme $\frac{a}{b}$ rozkladové

Date: 28.6.2010.

třídy $[(a,b)]_\sim$. Všimněme si, že $\frac{ad}{bd} = \frac{ac}{bc}$ pro každé nenulové $b,d \in R$, protože $(ad,bd) \sim (ac,bc)$.

Nyní snadno spočítáme, že

$$\frac{a}{b} + \frac{-a}{b} = \frac{a+(-a)}{bb} = \frac{0}{bb} = \mathbf{0},$$

$$\frac{a}{b}\cdot\frac{c}{d} + \frac{a}{b}\cdot\frac{e}{f} = \frac{acbf+bdae}{bdbf} = \frac{acf+ade}{bdf} = \frac{a}{b}\cdot\frac{cf+de}{df} = \frac{a}{b}\cdot(\frac{c}{d}+\frac{e}{f}).$$

Konečně, zvolíme-li $\frac{a}{b} \neq \mathbf{0}$, pak $(a,b) \not\sim (0,1)$, tedy $a \neq 0$, a proto $\frac{b}{a} \in F$ a $\frac{a}{b}\cdot\frac{b}{a} = \mathbf{1}$. Tím jsme dokázali, že každý nenulový prvek F je invertibilní, a proto je $F/\sim$ komutativní těleso.

(4) Okamžitě vidíme, že je $\frac{a}{1}\cdot\frac{b}{1} = \frac{a\cdot b}{1}$, $\frac{a}{1}+\frac{b}{1} = \frac{a+b}{1}$ a $\sigma(1) = \mathbf{1}$, proto je σ homomorfismus. Konečně, je-li $\sigma(a) = \sigma(b)$, pak $a = b$, tedy jde o prostý homomorfismus. □

Definice. Komutativní těleso $F/\sim$ budeme nazývat *podílovým tělesem* okruhu R a jeho prvky budeme značit $\frac{a}{b} = [(a,b)]_\sim$.

Příklad 6.2. Těleso racionálních čísel $\mathbf{Q}(+,\cdot,-,0,1)$ je podílovým tělesem okruhu celých čísel $\mathbf{Z}(+,\cdot,-,0,1)$.

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 6.3. Algebra $\mathcal{P}(X)(\div,\cap,\mathrm{Id}_{\mathcal{P}(X)},\emptyset,X)$, 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 $\mathcal{P}(X)(\div,\cap,\mathrm{Id}_{\mathcal{P}(X)},\emptyset,X)$. Je-li naopak I ideál, všimněme si, že je uzavřen na konečná 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 $\mathcal{P}(X)(\div,\cap,\mathrm{Id}_{\mathcal{P}(X)},\emptyset,X)$ jsou všechny ideály hlavní.

Poznámka 6.4. *Nechť $S(\vee,\wedge,\mathbf{0},\mathbf{1},\ ')$ je Booleova algebra. Definujeme-li na S binární operaci $+$ předpisem $a+b = (a\wedge b')\vee(a'\wedge b)$, pak $S(+,\wedge,\mathrm{Id}_S,\mathbf{0},\mathbf{1})$ je Booleův okruh. Každá podalgebra resp. kongruence Booleovy algebry $S(\vee,\wedge,\mathbf{0},\mathbf{1},\ ')$ je podokruhem resp. kongruencí Booleova okruhu $S(+,\wedge,\mathrm{Id}_S,\mathbf{0},\mathbf{1})$.*

Důkaz. Přímo z definice vidíme, že jsou operace $+$ resp. $\wedge$ komutativní s neutrálními prvky $\mathbf{0}$ resp. $\mathbf{1}$. Dále $\wedge$ je asociativní 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 a 4.17

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

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

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

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

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

Konečně

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

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

Vezměme nyní podalgebru 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 $a', b', a+b = (a \wedge b') \vee (a' \wedge b) \in S$ 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. □

Poznámka 6.5. *Nechť $S(+, \cdot, -, 0, 1)$ 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 $S(\vee, \cdot, 0, 1, \ ')$ je Booleova algebra. Každý podokruh resp. kongruence Booleova okruhu $S(+, \cdot, -, 0, 1)$ je podalgebrou resp. kongruencí příslušné Booleovy algebry $S(\vee, \cdot, 0, 1, \ ')$.*

Důkaz. Nejprve dokážeme, že je $S(\cdot, \vee)$ distributivní svaz, k čemuž použijeme Poznámku 4.4. 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 předpkladu 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 $a \vee a' = a \cdot (1 + a) = a + a = 0$, 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 definováni výlučně pomocí operací původních, stejně přímočarou argumentací jako v 6.4 dokazuje, že se jedná o podalgebru a kongruenci přslušné Booleovy algebry $S(\vee, \cdot, 0, 1, \ ')$. □

Důsledek 6.6. *Je-li $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ Booleova algebra, pak je P její podalgebra resp. ρ její kongruence právě tehdy, když je P podalgebra resp. ρ kongruence na Booleově okruhu $S(+, \wedge, \mathrm{Id}_S, \mathbf{0}, \mathbf{1})$ zavedeném v 6.4.*

Věta 6.7. *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 4.18 je Booleova algebra $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ izomorfní Booleově algebře $\mathcal{P}(A)(\cup, \cap, \emptyset, A,')$ a díky Větě 5.4 a Důsledku 6.6 stačí popsat svaz ideálů příslušného Booleova okruhu $\mathcal{P}(A)(\div, \cap, \mathrm{Id}_{\mathcal{P}(A)}, \emptyset, A)$. V příkladu 6.3 jsme zjistili, že ideály jsou právě tvaru $\mathcal{P}(Y)$ pro $Y \in \mathcal{P}(A)$. Konečně snadno nahlédneme, že $\mathcal{P}(Y) \vee \mathcal{P}(Y) = \mathcal{P}(Y \cup Z)$ a $\mathcal{P}(Y) \wedge \mathcal{P}(Y) = \mathcal{P}(Y \cap Z)$, tedy svaz ideálů (a tedy i svaz kongruencí původní Booleovy algebry) je izomorfní svazu $\mathcal{P}(A)(\cap, \cup)$. □

Příklad 6.8. Buď $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ konečná Booleova algebra. Víme, že je S izomorfní potenční Boolově algebře nad množinou všech atomů A. To mimo jiné znamená, že $|S| = |\mathcal{P}(A)| = 2^{|A|}$. Podle 6.7 existuje na $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ právě $2^{|A|} = |S|$ kongruencí.

Příklad 6.9. Buď 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 6.4 kongruencí na okruhu $\mathcal{P}(X)(\div, \cap, \mathrm{Id}_{\mathcal{P}(X)}, \emptyset, X)$. 0značme $Y = \bigcup[\emptyset]_\rho$. Využijeme-li popis kongruencí na okruzích pomocí ideálů a připomeneme, že podle 6.3 je ideál $[\emptyset]_\rho = \mathcal{P}(Y)$, vidíme, že $(A, B) \in \rho$, právě když $A \div B \subseteq Y$.

7. Dělitelnost

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 $a \cdot c = b \cdot c \ \Rightarrow \ a = b$.

Buď $S(\cdot)$ komutativní monoid s krácením (nebo $S(+, \cdot, -, 0, 1)$ obor integrity) a nechť $a, b \in S$. 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.

Příklad 7.1. (1) $\mathbf{N}(\cdot)$ a $\mathbf{Z} \setminus \{0\}(\cdot)$ jsou zřejmě komutativní monoidy s krácením.

(2) Je-li $R(+, \cdot, -, 0, 1)$ obor integrity, 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 $a - b = 0$.

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

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

Poznámka 7.2. *Buď $R(+, \cdot, -, 0, 1)$ oboru integrity 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. □

Poznámka 7.3. *Nechť $S(\cdot)$ 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. *Nechť $a, b \in S$. Pak $a\|b$ právě tehdy, když existuje invertibilní prvek $u \in S$ tak, že $a = b \cdot u$.*
3. *$\|$ je kongruence na $S(\cdot, 1)$.*
4. *$S/\|(\cdot)$ je komutativní monoid s krácením a relace "dělí" na něm tvoří uspořádání.*

Důkaz. (1) Jestliže $(a =) b \cdot c_0 = b \cdot c_1$, pak stačí vykrátit 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 vzahu za b, máme $a = a \cdot v \cdot u$, a vykrítíme-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 tranzitivní 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 zjevné, 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 vykrátit, 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 $[a]_\| \cdot [x]_\| = [b]_\|$ a $[b]_\| \cdot [y]_\| = [c]_\|$. Potom existují takové invertibilní prvky u a u, 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 $[a]_\| \cdot [x \cdot y]_\| = [c]_\|$. Konečně jestliže $[a]_\| \cdot [x]_\| = [b]_\|$ a $[b]_\| \cdot [y]_\| = [a]_\|$, 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 $[a]_\| = [b]_\|$.

□

Příklad 7.4. Komutativní monoidy $\mathbf{N}(\cdot)$ a $\mathbf{Z} \setminus \{0\}/\|(\cdot)$ jsou izomorfní.

Definice. Buď $S(\cdot)$ komutativní monoid s krácením (nebo $S(+, \cdot, -, 0, 1)$ obor integrity) a nechť $a, b, c, a_1, \dots, a_n \in S$. 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 integrity) a $c = a \cdot b \;\Rightarrow\; c\|a$ nebo $c\|b$. Prvek c nazveme *prvočinitelem*, jestliže c není invertibilní (ani nulový) a $c/a \cdot b \;\Rightarrow\; c/a$ nebo c/b.

Poznámka 7.5. *Nechť $S(\cdot)$ je komutativní monoid s krácením a $a, b, c \in S$.*

(1) *Nechť d je $NSD(a, b)$ a e je $NSD(a \cdot c, b \cdot c)$. Potom $(d \cdot c)\|e$*
(2) *Nechť 1 je $NSD(a, b)$ a $a/b \cdot c$. Existuje-li $NSD(a \cdot c, b \cdot c)$, pak a/c.*

Důkaz. (1) Protože dc/ac, dc/bc a e je $NSD(a \cdot c, b \cdot c)$, dc/e, tj. existuje u, pro něž $e = dcu$. To znamená, že dcu/ac a dcu/bc a vykrátíme-li du/a a du/b, a proto du/d, tudíž $u\|1$ a $(d \cdot c)\|e$ podle 7.3.

(2) Nechť e je $NSD(a \cdot c, b \cdot c)$, pak je $(1 \cdot c)\|e$ podle (1), tedy c je $NSD(a \cdot c, b \cdot c)$. Protože je a společný dělitel $b \cdot c$, $a \cdot c$, dostáváme, že a/c. □

Věta 7.6. *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 $p\|a$) nebo p/b (tedy $p\|b$).

Předpokládejme, že je p ireducibilní, p dělí součin $a \cdot b$ a nedělí prvek a. Protože existuje $NSD(p, a)$, který není asociován s p, plyne z ireducibility p, že 1 je $NSD(p, a)$. Navíc $p/a \cdot b$ a existuje $NSD(p \cdot b, a \cdot b)$, proto podle 7.5(2) p/b. □

Příklad 7.7. Uvažujme podokruh $\mathbf{Z}[\sqrt{5}] = \{a + \sqrt{5}b \mid a, b \in \mathbf{Z}\}$ okruhu reálných čísel. Zřejmě se jedná o obor integrity, tedy $\mathbf{Z}[\sqrt{5}] \setminus \{0\}(\cdot, 1)$ 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 $\sqrt{5} - 1$).

Věta 7.8. *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* $p_1 \cdot p_2 \cdot \dots \cdot p_r \| q_1 \cdot q_2 \cdot \dots \cdot q_s$. *Potom* $r = s$ *a existuje taková bijekce* σ*, že* $p_i \| q_{\sigma(i)}$ *pro všechna* $i = 1, \dots, r$.

Důkaz. Tvrzení dokážeme indukcí podle r. Jesliže $r = 1$ máme $p_1 = u \cdot q_1 \cdot q_2 \cdot \dots \cdot q_s$ pro nějaký invertibilní prvek u podle 7.3(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 $p_r / q_1 \cdot q_2 \cdot \dots \cdot q_s$, najdeme indukčním rozšířením definice prvočinitele takové $i \leq s$, pro které p_r / q_i, bez újmy na obecnosti můžeme předpokládat, že $i = s$. Z ireducibility prvků p_r i q_s plyne, že jsou nutně asociovány, proto můžeme vykrátit a dostaneme $p_1 \cdot p_2 \cdot \dots \cdot p_{r-1} \| q_1 \cdot q_2 \cdot \dots \cdot q_{s-1}$. Nyní podle indukčního předpokladu $r - 1 = s - 1$ a dostáváme hledanou permutaci σ na množině $\{1, \dots, r-1\}$, kterou dodefinujeme $\sigma(r) = r$. $\square$

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

Poznámka 7.9. *Buď* $R(+, \cdot, -, 0, 1)$ *obor integrity 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 $I = \{\sum_{i=1}^n a_i u_i | \; u_i \in R\}$ je ideál oboru integrity hlavních ideálů R, tedy existuje prvek $c \in I$, pro nějž $cR = I$. 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/c. $\square$

Věta 7.10. *Buď* $R(+, \cdot, -, 0, 1)$ *obor integrity hlavních ideálů. Pak platí:*

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

Důkaz. (1) Podle 7.9 jsou splněny předpoklady 7.6, které implikují závěr.

(2) Díky (1) a 7.8 platí jednoznačnost, zbývá tedy dokázat existenci ireducibilního rozkladu.

Předpokládejme ke sporu, že nějaký neinvertibilní prvek $a \in R$ nemá ireducibilní rozklad (tj. neexistje posloupnost ireducibilních prvků $c_1, \dots, c_k$, pro kteréa $= c_1 \cdot \dots \cdot c_k$), 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 7.2 a 7.3 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 $cR \neq cR$, což je spor. $\square$

Příklad 7.11. Protože je okruh $\mathbf{Z}(+, \cdot, -, 0, 1)$ obor integrity hlavních ideálů, existují v monoidech $\mathbf{N} \setminus \{0\}(\cdot)$ a $\mathbf{Z} \setminus \{0\}(\cdot)$ největší společní dělitelé a zřejmě existují rozklady na ireducibilní prvky, tedy jsou v $\mathbf{N}$ jsou ireducibilní rozklady určeny až na pořadí jednoznačně, v $\mathbf{Z}$ jsou jednoznačné až na pořadí a znaménko.

8. Eukleidovské obory integrity

Příklad 8.1. Uvědomme si na příkladu polynomů z celočíselnými koeficienty, jakým způsobem zobecnit jejich chápání jako okruhu. Uvažujme polynomy $p, q \in \mathbf{Z}[x]$, kde polynomem rozumíme sumu $p = \sum_{i\in\mathbf{N}_0} p_i x^i$, resp $q = \sum_{i\in\mathbf{N}_0} q_i x^i$, jejichž skoro všechny (tj. až na konečně mnoho „výjimek") nulové. Takové polynomy umíme sčítat, odčítat a násobit: $p + q = \sum_{i\in\mathbf{N}_0}(p_i + q_i)\cdot x^i$, $-p = \sum_{i\in\mathbf{N}_0}(-p_i)\cdot x^i$ a $p \cdot q = \sum_{n\in\mathbf{N}_0}(\sum_{i+j=n} p_i \cdot q_j)\cdot x^n$. Všimněme si, že kromě okruhu $\mathbf{Z}(+,\cdot,-,0,1)$ v zavedení klasického pojmu polynomu využíváme ještě vlastnosti monoidu nezáporných celých čísel $\mathbf{N}_0(+)$ (nebo, ekvivalentně řečeno, izomorfního monoidu $\{x^n|\ n \in \mathbf{N}_0\}(\cdot)$).

Pozorování Příkladu 8.1 využijeme v následující obecné konstrukci.

Nechť $R(+,\cdot,-,0,1)$ je okruh a $M(\cdot,e)$ je monoid. Položme $R[M] = \{p : M \to R|\ \{m|p(m) \neq 0\}$ 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 $\mathbf{1}$:

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

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

Poznámka 8.2. *Nechť $R(+,\cdot,-,0,1)$ je okruh a $M(\cdot)$ je monoid s neutrálním prvkem e.*

(1) *$R[M](+,\cdot,-,\mathbf{0},\mathbf{1})$ je okruh,*
(2) *zobrazení $i : R \to R[M]$ 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 $\nu : M \to R[M]$ 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

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

a že

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

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

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

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

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

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

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 $R[M]$. □

Definice. Buď $R(+,\cdot,-,0,1)$ okruh a buď $\mathbf{N}_0(+,0)$ monoid nezáporných celých čísel se sčítáním. Potom okruh $R[\mathbf{N}_0](+,\cdot,-,\mathbf{0},\mathbf{1})$ nazveme *okruhem polynomů jedné neurčité* a jeho prvkům budeme říkat *polynomy.* Místo $R[\mathbf{N}_0]$ budeme psát $R[x]$ a polynomy budeme místo $p = \sum_{n\in\mathbf{N}_0} p(n).n \in R[x]$ zapisovat ve tvaru $p = \sum_{n\in\mathbf{N}_0} p(n)\cdot x^n$ nebo $p = \sum_{n\in\mathbf{N}_0} p_n\cdot x^n$.

Příklad 8.3. 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 $R[{\mathbf{N}_0}^n]$ se součinovým monoidem ${\mathbf{N}_0}^n(+,(0,\dots,0))$.

Definice. Buď $R(+,\cdot,-,0,1)$ je okruh a $p = \sum_{n\in\mathbf{N}_0} a_n\cdot x^n \in R[x]$. Je-li $p\neq\mathbf{0}$, budeme největší takové $n\in\mathbf{N}_0$, že $a_n\neq 0$, nazývat stupněm polynomu p. Stupeň polynomu $\mathbf{0}$ položíme roven -1. Stupeň polynomu p budeme označovat $\deg p$.

Poznámka 8.4. *Nechť $R(+,\cdot,-,0,1)$ je okruh a $p,q\in R[x]$. Pak platí:*

(1) $\deg -p = \deg p$,
(2) $\deg p+q \le \max(\deg p,\ \deg q)$,
(3) *je-li $p\neq 0\neq q$, pak $\deg p\cdot q \le \deg p + \deg q$, je-li navíc R oborem integrity, potom $\deg p\cdot q = \deg p + \deg q$,*
(4) *$R[x]$ je obor integrity právě tehdy, když je R obor integrity,*
(5) *je-li R obor integrity, polynom p je invertibilní prvek okruhu $R[x]$, právě když $\deg p = 0$ a $p(0)$ je invertibilní prvek okruhu R.*

Důkaz. Mějme $p = \sum_n p_n\cdot x^n$ a $q = \sum_n q_n\cdot x^n$, všimněme si, že $p_0 = p(0) = j_0(p)$.

(1) Plyne okamžitě z pozorování $\{n|\ p_n\neq 0\} = \{n|\ -p_n\neq 0\}$.

(2) Plyne z inkluze $\{n|\ p_n+q_n\neq 0\}\subseteq\{n|\ p_n\neq 0\}\cup\{n|\ q_n\neq 0\}$.

(3) Označme $\nu = \deg p$ a $\mu = \deg q$ q uvědomme si pro každé $n > \nu+\mu$, že koeficient u x^n v polynomu $\deg p\cdot q$ je $\sum_{k=0}^{n}(p_k\cdot q_{n-k}) = \sum_{k=0}^{n-\mu}(p_k\cdot 0) + \sum_{k=n-\mu+1}^{n}(0\cdot q_{n-k}) = 0$, proto $\deg p\cdot q\le\nu+\mu$.

Je-li R obor integrity, máme koeficient polynomu $p\cdot q$ u $x^{\nu+\mu}$:

$$\sum_{k=0}^{\nu+\mu}(p_k\cdot q_{n-k}) = \sum_{k=0}^{n-\mu-1}(p_k\cdot 0) + p_\nu\cdot q_\mu + \sum_{k=n-\mu+1}^{n}(0\cdot q_{n-k}) = p_\nu\cdot q_\mu\neq 0.$$

(4) Je-li $R[x]$ obor integrity, je každý jeho podokruh oborem integrity, tedy i $i(R[x])$. Navíc $i(R) \cong R$ podle 8.2(2) a 1. věty o izomorfismu, proto je R obor integrity.

Je-li R obor integrity a $p \neq 0 \neq q$, máme podle (3) $\deg p \cdot q = \deg p + \deg q \geq 0$, proto $p \cdot q \neq 0$.

(5) Jestliže $p \cdot q = 1$, pak podle (3) je $0 = \deg 1 = \deg p + \deg q$, proto $\deg p = \deg q = 0$, $p = p_0 x^0$ a $p_0 q_0 = 1$, tedy p_0 je invertibilní.

Naopak, jestliže $\deg p = 0$ a p_0 je invertibilní, pak $p \cdot p_0^{-1} x^0 = 1x^0$. □

Věta 8.5 (Dělení se zbytkem). *Nechť $R(+,\cdot,-,0,1)$ je obor integrity, $a,\ b \in R[x]$, a $b = \sum b_n x^n$. Předpokládejme, že $m = \deg b \geq 0$ a b_m je invertibilní v R. Potom existují jednoznačně určené polynomy $q,\ r \in R[x]$ tak, že $a = b \cdot q + r$ a $\deg r < \deg b$.*

Důkaz. Dokážeme nejprve existenční část tvrzení a to indukcí podle $n = \deg a - \deg b$. Jestliže $\deg a < \deg b$, a tedy $n < 0$, stačí položit $q = 0$ a $r = a$. Platí-li existenční tvrzení pro všechna $i < n$, dokážeme ho pro n. Buď $a = \sum a_n x^n$ a položme $u = a_{n+m} b_m^{-1} x^n$ a $t = a - u \cdot b$. Podle 8.4(2) a (3) je $\deg t \leq \max(\deg a, \deg u + \deg b) = n+m$ a koeficient polynomu t u mocniny x^{n+m} je $a_{n+m} - a_{n+m} b_m^{-1} b_m = 0$, tedy $\deg t - \deg b < n$. Proto pro polynom t můžeme užít indukční předpoklad, podle nějž existují takové polynomy v a r, že $t = b \cdot v + r$ a $\deg r < \deg b$. Položíme-li nyní $q = u + v$, dostáváme

$$b \cdot q + r = b \cdot u + b \cdot v + r = b \cdot u + t = a.$$

Konečně předpokládejme, že $a = b \cdot q' + r'$ a $\deg r' < \deg b$. Potom $b \cdot (q - q') = r' - r$ a podle 8.4(3) a protože $\deg(r' - r) < \deg b$, dostáváme $r' - r = 0$, a proto $q - q' = 0$ □

Definice. Buď $R(+,\cdot,-,0,1)$ obor integrity. Řekneme, že R je *eukleidovský obor integrity*, existuje-li zobrazení $\nu : R \to \mathbf{N}_0 \cup \{-1\}$ (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 $\nu(r) < \nu(b)$.

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

Věta 8.6. *Každý eukleidovský obor integrity je oborem integrity hlavních ideálů.*

Důkaz. Mějme $R(+,\cdot,-,0,1)$ eukleidovský obor integrity s eukleidovskou funkcí $\nu : R \to \mathbf{N}_0 \cup \{-1\}$ a vezměme libovolný nenulový ideál I. V ideálu I zvolíme nenulový prvek a s minimální hodnotou $\nu(a)$. Zřejmě $aR \subseteq I$. Nechť $i \in I$. 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 integrity jsou hlavní. □

Uvědomíme-li si, že každý nenulový prvek tělesa je invertibilní, říká nám 8.5, že stupeň polynomu je eukleidovská funkce na oboru integrity polynomů nad tělesem a proto podle 8.6 platí následující pozorování:

Důsledek 8.7. *Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso. Pak je $T[x]$ eukleidovským obor integrity s eukleidovskou funkcí danou stupněm polynomů, tudíž je $T[x]$ oborem integrity hlavních ideálů.*

Příklad 8.8. (1) Okruh celých čísel je eukleidovským oborem integrity s eukleidovskou funkcí absolutní hodnotou $|-|$. První podmínka definice platí zřejmě, druhá plyne z toho, že i v celých čísel umíme dělit se zbytkem.

(2) Podokruh $\mathbf{Z}[i] = \{a + bi |\ a, b \in \mathbf{Z}\}$ (tzv. Gaussova celá čísla) okruhu komplexních čísel je eukleidovským oborem integrity s eukleidovskou funkcí $\nu(a+bi) = a^2 + b^2$. Připomeňme, 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 $\alpha, \beta \in \mathbf{Z}[i]$. Jetliže α/β a $\beta \neq 0$, existuje $\gamma \in \mathbf{Z}[i]$, 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 $x_0, y_0 \in \mathbf{Z}$, 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 $\nu(\delta) \leq \frac{\nu(\beta)}{2} < \nu(\beta)$.

(3) Podokruh $\mathbf{Z}[\sqrt{2}] = \{a+\sqrt{2}b |\ a, b \in \mathbf{Z}\}$ okruhu reálných čísel je eukleidovským oborem integrity 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 $\nu(\alpha \cdot \beta) = \nu(\alpha) \cdot \nu(\beta)$.

Věta 8.9 (Eukleidův algoritmus). *Buď $R(+, \cdot, -, 0, 1)$ eukleidovským obor integrity s eukleidovskou funkcí ν a nechť a_0, $a_1 \in R \setminus \{0\}$. Sestrojme posloupnosti prvků a_i a q_i následujícím postupem:*

1. *je-li $i \geq 1$ a a_i nedělí a_{i-1}, vezměme takové $a_{i+1} \in R$, že $a_{i-1} = a_i \cdot q_i + a_{i+1}$ a $\nu(a_{i+1}) < \nu(a_i)$.*
2. *je-li $i \geq 1$ a a_i dělí a_{i-1}, položme $n = i$ a konstrukce končí.*

Posloupnost a_i je konečná a a_n je $NSD(a_0, a_1)$. Definujme dále posloupnosti x_i a y_i tak, že $x_0 = y_1 = 1$, $x_1 = y_0 = 0$, a pro $i \geq 1$ položme $x_{i+1} = x_{i-1} - x_i \cdot q_i$ a $y_{i+1} = y_{i-1} - y_i \cdot q_i$. Potom $a_i = x_i \cdot a_0 + y_i \cdot a_1$, speciálně $x_n \cdot a_0 + y_n \cdot a_1$ je $NSD(a_0, a_1)$.

Důkaz. Tvrzení 8.6 a 7.9 říkají, že největší společní dělitelé všech dvoji prvků eukleidovského oboru integrity existují. Protože a_n je $NSD(a_{n-1}, a_n)$, stačí dokázat, že prvky c a d jsou asociované pro každé $0 < i < n$, kde c je $NSD(a_{i-1}, a_i)$ a d je $NSD(a_i, a_{i+1})$. Protože c/a_i a $c/a_{i+1} = a_{i-1} - a_i \cdot q_i$ dostáváme z defince NSD, 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 8.10. Najdeme v $\mathbf{Z}[i](+, \cdot, -, 0, 1)$ 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 $-2 - i = (6 - 7i) + (-1 + i)(7 + i)$.

Poznámka 8.11. *Je-li $S(+,\cdot,-,0,1)$ komutativni okruh, R jeho podokruh a $\alpha \in S$, pak zobrazení $j_\alpha : R[x] \to S$ dané předpisem $j_\alpha(\sum_{n\in\mathbf{N}_0} a_n x^n) = \sum_{n\in\mathbf{N}_0} a_n \cdot \alpha^n$ je okruhový homomorfismus.*

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

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

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

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

□

Definice. Nechť $S(+,\cdot,-,0,1)$ je komutativni okruh, R jeho podokruh, $\alpha \in S$ a $p \in R[x]$. Homomorfismu j_α z 8.11 říkáme *dosazovací homomorfismus*, α nazveme *kořenem* polynomu p, jestliže $j_\alpha(p) = 0$, a α je *vícenásobný kořen* polynomu p, pokud $(x-\alpha)^2/p$ v okruhu $S[x]$. *Kořenovým činitelem* (kořenu α) rozumíme polynom tvaru $x - \alpha \in S[x]$. 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 8.12. *Nechť je $R(+,\cdot,-,0,1)$ obor integrity, $\alpha \in R$ a $p \in R[x] \setminus \{\mathbf{0}\}$.*
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 8.5 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 8.11, 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 8.11.

(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 8.11, proto $a(\alpha) = 0$ nebo $b(\alpha) = 0$, neboť je R obor integrity. 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 $i \le r$, proto $(x-\alpha_{r+1})/q$. Konečně z 8.4(3) plyne, že $\deg p = \deg((x-\alpha_1) \cdot \dots \cdot (x-\alpha_k) \cdot q) = k + \deg p \ge k$. □

Všimněme si, že 8.12(1) říká, že vícenásobný kořen je kořenem, a 8.12(2) nám poskytne příklady prvočinitelů (a tedy ireducibilních prvků) v okruhu polynomů nad obecným oborem integrity.

Definice. Buď $R(+,\cdot,-,0,1)$ 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 8.13. *Nechť $R(+,\cdot,-,0,1)$ je komutativní okruh, $\alpha \in R$, $p, q \in R[x]$ a $n \in \mathbf{N}$. Pak platí:*

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

Důkaz. (1)–(3) Vlastnosti dostáváme přimočarým použitím definice.

(4) Dokážeme indukcí indukcí 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 8.14. *Nechť $S(+,\cdot,-,0,1)$ je obor integrity, 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 $NSD(p,\ p')$, 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 8.12(1). Pomocí 8.13(3) spočítáme $p' = q + (x-\alpha)\cdot q'$. Díky 8.11 vidíme, že je α kořenem p' právě tehdy, když je kořenem q a to je podle 8.12(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 8.12(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 8.12(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 8.15. V tělese charakteristiky 3 (např $\mathbf{Z}_3$) platí, že $(x-1)^3 = x^3 - 3x^2 + 3x - 1 = x^3 - 1$, tedy polynom $x^3 - 1$ má nad takovým tělesem kořen. Vidíme, že předpoklad o charakteru z 8.14(3) nemůžeme odstranit. Navíc si všimněme derivace $(x^3-1)' = 0$.

Nyní už jsme s to dokázat nedokázané tvrzení 2.14 z 2. kapitoly:

Věta 8.16. *Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso a nechť G je konečná podgrupa multiplikativní grupy $T \setminus \{0\}(\cdot)$. Potom je G cyklická grupa.*

Důkaz. Uvažujme nejprve libovolnou konečnou grupu $G(\cdot)$ a položme $n = |G|$. Poznamenejme, 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 $|G| = \sum_{k/|G|} t_k$. Připomeňme, že v cyklické grupě řádu n máme pro každé k/n právě jednu (cyklickou) podgrupu řádu k (viz 2.7) a počet generátorů této podgrupy, tedy právě všechny prvky řádu k, udává hodnota Eulerovy funkce $\varphi(k)$ (viz 2.9), dává nám předchozí rovnost vztah $n = \sum_{k/n} \varphi(k)$.

Nyní předpokládejme, že G je (konečná) podgrupa multiplikativní 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 $\langle u \rangle$ obshuje 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 8.12(3). $\square$

Příklad 8.17. $\mathbf{Z}_{53} \setminus \{0\}(\cdot)$ je podle 8.16 cyklická grupa řádu 52. To znamená, že obsahuje $\varphi(52) = 3 \cdot 12 = 36$ generátorů.

9. Kořenová a rozkladová nadtělesa

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

Definice. Jsou-li $R(+,\cdot,-,0,1)$ a $S(+,\cdot,-,0,1)$ okruhy a $f : R \to S$ jejich homomorfismus, pak definujme zobrazení $f_x : R[x] \to S[x]$ předpisem $f_x(\sum_{i\geq 0} a_i x^i) = \sum_{i\geq 0} f(a_i)x^i$.

Poznámka 9.1. *Buď $R(+,\cdot,-,0,1)$, $S(+,\cdot,-,0,1)$ a $T(+,\cdot,-,0,1)$ komutativní okruhy a $f : R \to S$ a $g : S \to T$ 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. *$fj_\alpha = j_{f(\alpha)} f_x$ pro každé $\alpha \in R$.*

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

$$f_x(a+b) = f_x(\sum_n (a_n + b_n)x^n) = \sum_n f(a_n + b_n)x^n = \sum_n (f(a_n) + f(b_n))x^n =$$

$$= \sum_n f(a_n)x^n + \sum_n f(b_n)x^n = f_x(a) + f_x(b),$$

$$f_x(a \cdot b) = f_x(\sum_n \sum_{k=0}^{n} (a_k + b_{n-k})x^n) = \sum_n f(\sum_{k=0}^{n} (a_k + b_{n-k}))x^n =$$

$$= \sum_n (\sum_{k=0}^{n} f(a_k) + f(b_{n-k}))x^n = \sum_n f(a_n)x^n \cdot \sum_n f(b_n)x^n = f_x(a) \cdot f_x(b).$$

(2) $g_x f_x(\sum_n a_n x^n) = \sum_n gf(a_n)x^n = (gf)_x(\sum_n a_n x^n)$.

(3) Nechť je f_x izomorfismus. Jestliže $f(u) = f(v)$, pak $f_x(ux^0) = f(vx^0)$, 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 $f_x(f^{-1})_x = \mathrm{Id}_{S[x]}$ a $(f^{-1})_x f_x = \mathrm{Id}_{R[x]}$ podle (2), tedy $(f_x)^{-1} = (f^{-1})_x$ a f_x je izomorfismus.

(4) $fj_\alpha(\sum a_n x^n) = \sum f(a_n)f(\alpha)^n = j_{f(\alpha)} f_x(\sum a_n x^n)$. □

Věta 9.2. *Nechť $T(+, \cdot, -, 0, 1)$ je komutativní těleso a $u \in T[x]$. Pak faktorový $T[x]/uT[x]$ je komutativní těleso, právě když je u ireducibilní. Navíc zobrazení $\mu(t) = tx^0 + uT[x]$ je prostý homomorfismus tělesa T do okruhu $T[x]/uT[x]$ pro neinvertibilní u.*

Důkaz. Podle 5.7 stačí ověřit, že u je ireducibilní, právě když je $uT[x]$ maximální ideál. Nechť je u je ireducibilní a J ideál obsahující $uT[x]$. Podle 8.7 existuje $j \in T[x]$ $J = jT[x]$, tedy díky 7.2 j/u. Protože je u ireducibilní, máme buď $j\|u$ a tudíž $uT[x] = J$ nebo $j\|1$ a tudíž $J = T[x]$. Je-li $uT[x]$ maximální ideál, dostáváme závěr přímým použitím 7.2 a definice ireducibility.

Nyní si uvědomme, že zobrazení μ dostaneme jako složení homomorfismus i z 8.2(2) a přirozené projekce $\pi : T[x] \to T[x]/uT[x]$, proto $\mu = \pi i$ je opět homomorfismus. Jestliže konečně $\mu(a) = \mu(b)$, pak $u/ax^0 - bx^0$, tedy podle 8.4(3) je $ax^0 - bx^0$ musí být nulový polynom (v opačném případě by $\deg u \le \deg(ax^0 - bx^0)$), a tedy μ je prosté. □

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 $(T[x])_u$.

Věta 9.3. *Nechť $T(+, \cdot, -, 0, 1)$ je komutativní těleso a $u = \sum_{i \ge 0} a_i y^i \in T[y]$ je ireducibilní polynom. Pak $(T[y])_u$ je komutativní těleso a polynom $\sum_{i \ge 0} a_i x^i$ má v $(T[y])_u$ kořen.*

Důkaz. Díky 9.2 nám stačí ověřit, že je $Y = y + uT[y]$ kořenem $\sum_{i \ge 0} a_i x^i$ nad okruhem $(T[y])_u$. Dosadíme-li, dostáváme $j_Y(\sum_{i \ge 0} a_i x^i) = \sum_{i \ge 0}(a_i y^i + uT[y]) = (\sum_{i \ge 0} a_i y^i) + uT[y] = u + uT[y] = 0 + uT[y]$. □

Definice. Nechť $U(+, \cdot, -, 0, 1)$ 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).

Všimněmem si, že množina všech podtěles komutativního tělesa tvoří uzávěrový systém, tj. průnik libovolného systému podtěles nějakého tělese 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 9.4. *Jsou-li $T \subseteq U$ komutativní tělesa, $\alpha \in U$ a $S \subset U$, pak $T[\alpha] = \{\sum_{i=0}^n a_i \cdot \alpha^i |\ a_i \in T\} = j_\alpha(T[x])$, $T[\alpha] \subseteq T(\alpha)$ a $T[S] \subseteq T(S)$.*

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

Definice. Nechť $T \subseteq U$ 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 9.5. *Nechť $T(+,\cdot,-,0,1)$ 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 7.10 a 8.7 existuje (jednoznačný) ireducibilní rozklad polynomu p, zvolíme-li nějaký ireducibilní polynom p_1, který dělí p, dostaneme podle 9.3 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 8.12(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 rozkladový nadtělesem polynomu p je právě těleso $T(\{\alpha_1,\dots,\alpha_n\})$. $\square$

Definice. Nechť $T \subseteq U$ 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 9.6. *Buď $T \subseteq U$ 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 $I = \{p \in T[x]|\ j_\alpha(p) = 0\} = j_\alpha^{-1}(0)$ všech polynomů, které mají kořen α. Protože je j_α homomorfimus podle 8.11, 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 8.7 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 $n = \deg a$, položme $m = a_n^{-1}a$. 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 8.11 $a(\alpha) = 0$ a pak $m\|a$ nebo $b(\alpha) = 0$ a pak $m\|b$, tedy m je ireducibilní. Konečně si všimněme, že díky 1. větě o izomorfismu a 9.4(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 9.2 těleso, je i $T[\alpha]$ těleso, proto $T[\alpha] = T(\alpha)$. $\square$

Definice. Buď $T \subseteq U$ 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.

Příklad 9.7. Těleso komplexních čísel je kořenovým i rozkladovým nadtělesem polynomu $x^2 + 1$ nad $\mathbf{R}$, $[\mathbf{C} : \mathbf{R}] = 2$.

Důkaz. □

Poznámka 9.8. *Nechť $T \subseteq U$ jsou komutativní tělesa a $\alpha, \alpha_1, \dots, \alpha_n \in U$.*

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 $\alpha_1, \dots, \alpha_n$ algebraické nad T.*

Důkaz. (1) Položme $n = \deg m_\alpha$ a připomeňme, že $T[\alpha] = T(\alpha)$ podle 9.6. Dokážeme, že množina $\{\alpha^i |\ i = 0, 1, \dots, n-1\}$ je bází $T[\alpha]$ nad tělesem T. Vezměme prvek $t \in T[\alpha]$, o němž z 9.4 víme, že je tvaru $t = p(\alpha)$ pro vhodný polynom $p \in T[x]$. Vydělíme-li nyní se zbytkem polynom p poynomem m_α, dostaneme (8.5) $p = qm_\alpha + r$ 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 $\{\alpha^i |\ i = 0, 1, \dots, n-1\}$. 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 9.6 m_α / c, dostáváme, že $c = 0$, tudíž $\{\alpha^i |\ i = 0, 1, \dots, n-1\}$ je lineárně nezávislá množina.

(2) Je-li $[T(\alpha) : T]$ konečné, je množina $\{\alpha^i |\ i \geq 0\}$ 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) Nejprve ukážeme, že $[V : T] = [V : U][U : T]$ pro $T \subseteq U \subseteq V$ jsou do sebe zařazená komutativní tělesa. 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 $0 = \sum_{ij} c_{ij}\mathbf{u}_i\mathbf{v}_i = \sum_i(\sum_j c_{ij}\mathbf{u}_i)v_i$ 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 $[V : T] = |(\mathbf{u}_i\mathbf{v}_j)| = |(\mathbf{u}_i)||(\mathbf{v}_j)| = [V : U][U : T]$.

Nyní dokážeme indukcí podle n, přičemž jsme tvrzení pro $n = 1$ dokázali v 9.6, navíc $[T(\alpha) : T]$ je konečné podle (1). Předpokládejme, že tvrzení platí pro $n - 1$. 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 9.6, 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 dokázanému pozorování o stupni rozšíření dostáváme

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

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

Důsledek 9.9. *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 9.10. (1) $\mathbf{Q}(\sqrt[3]{2})=\mathbf{Q}[\sqrt[3]{2}]=\{x+y\sqrt[3]{2}+z\sqrt[3]{4}|\ x,y,z\in\mathbf{Q}\}$ je kořenové nadtěleso polynomu x^3-2 nad $\mathbf{Q}$ a $[\mathbf{Q}(\sqrt[3]{2}):\mathbf{Q}]=3$, tedy x^3-2 je monický polynom stupně 3, a proto jde podle 9.8(1) a 9.6 právě o minimální polynom algebraického prvku $\sqrt[3]{2}$ nad $\mathbf{Q}$. Všimněme si, že zatímco nad $\mathbf{Q}$ je polynom x^3-2 ireducibilní, nad $\mathbf{R}$ máme ireducibilní rozklad $x^3-2=(x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$ a nad $\mathbf{C}$ se polynom rozkládá na kořenové činitele.

(2) Nechť $k\in\mathbf{Z}$ a $\sqrt{k}\in\mathbf{C}\setminus\mathbf{Q}$. Pak $\mathbf{Q}(\sqrt{k})\neq\mathbf{Q}$ a $\sqrt{k}$ je kořenem polynomu x^2-k, proto je $m_{\sqrt{k}}=x^2-k$ díky 9.4 nutně minimální polynom a $[\mathbf{Q}(\sqrt{k}):\mathbf{Q}]=\deg m_{\sqrt{k}}=2$ podle 9.8(1). $\mathbf{Q}(\sqrt{k})$ je tzv. kvadratické rozšíření tělesa $\mathbf{Q}$.

(3) $\mathbf{R}$ není algebraickým rozšířením tělesa $\mathbf{Q}$, protože polynomů $\mathbf{Q}[x]$ je pouze spočetně mnoho a každý má pouze konečně mnoho kořenů, tedy všech reálných kořenů $\mathbf{Q}[x]$ je opět pouze spočetně. Ovšem množina $\mathbf{R}$ spočetná není.

(4) Prvek $\sqrt[5]{3}$ je kořenem polynomu $x^5-3\in\mathbf{Q}[x]$ a prvek $\sqrt[7]{11}$ kořenem polynomu $x^7-11\in\mathbf{Q}[x]$, tedy oba jsou algebraické nad $\mathbf{Q}$. Podle Poznámky 9.8(4) je $\mathbf{Q}(\sqrt[5]{3},\sqrt[7]{11})=\mathbf{Q}[\sqrt[5]{3},\sqrt[7]{11}]$ 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 $p\in\mathbf{Q}[x]$, jehož je α kořenem.

Poznámka 9.11. *Buď $T_1\subseteq U_1$ a $T_2\subseteq U_2$ komutativní tělesa, buď $f:T_1\to T_2$ izomorfismus a nechť $\alpha\in U_1$ je algebraický prvek nad T_1 a $\beta\in U_2$ je algebraický prvek nad T_2. Pak existuje takový izomorfismus $g:T_1(\alpha)\to T_2(\beta)$, 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 9.1(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 9.1(4), tedy $\beta=g(\alpha)$ je kořenem polynomu $f_x(m_\alpha)\in T_2[x]\subset U_2[x]$. Podle Věty 9.6 $m_\beta/f_x(m_\alpha)$. Protože je $f_x(m_\alpha)$ ireducibilní a monický, dostáváme nutně $m_\beta=f_x(m_\alpha)$.

($\Leftarrow$) Stačí si uvědomit, že Věta 9.6 zaručuje existenci izomorfismů

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

a že izomorfismus f_x indukuje podle předpokladu izomorfismus faktorových okruhů $\overline{f_x}:T_1[x]/(m_\alpha T_1[x])\to T_2[x]/(m_\beta T_2[x])$, 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 9.12. *Nechť T je komutativní těleso, $p \in T[x]$. Pak existuje až na izomorfismus právě jedno rozkladové nadtěleso polynomu p.*

Důkaz. Dokážeme pro komutativní tělesa T_1, T_2 a izomorfismus $f : T_1 \to T_2$, indukcí podle stupně polynomu $p \in T_1[x]$, že je rozkladové nadtěleso U_1 polynomu $p \in T_1[x]$ izomorfní rozkladovému nadtěleso U_2 polynomu $f_x(p) \in T_2[x]$.

Označme $\alpha_1, \dots, \alpha_n$ všechny kořeny polynomu p v U_1 a $\beta_1, \dots, \beta_m$ všechny kořeny polynomu $f_x(p)$ v U_2 a všimněme si, že f_x je izomorfismus okruhů $T_1[x]$ a $T_2[x]$. Budeme konstruovat izomorfismus $g : U_1 \to U_2$

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 dovojici 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 9.6, 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 8.7 a 7.10 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 9.6, 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 9.11 existuje izomorfismus těles $h : T_1(\alpha_n) \to T_2(\beta_m)$, 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 izomorfismus $g : U_1 \to U_2$. □

10. Konečná tělesa

Poznámka 10.1. *Buď T komutativní těleso (prvočíselné) kladné charakteristiky p, buď n přirozené číslo a nechť $q = p^n$. Pak množina $Q = \{t \in T \mid t^q = t\}$ tvoří podtěleso T.*

Důkaz. Nejprve uvážíme, že $f_p : T \to T$, $f_p(a) = a^p$ je okruhový homomorfismus. Okamžitě vidíme, že $0^p = 0$, $1^p = 1$, $(a \cdot b)^p = a^p \cdot b^p$. Dále $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} \times (a^i \cdot b^{p-i}) = a^p + b^p$, protože $p / \binom{p}{i}$ pro každé $i = 1, \dots, p-1$, tedy $\sum_{i=1}^{p-1} \binom{p}{i} \times (a^i \cdot b^{p-i}) = 0$. Indukčním argumentem zjistíme, že $f_{p^i} = f_{p^{i-1}} f_p$ je homomorfismus okruhů pro každé kladné i. Proto $(a+b)^{p^n} = f_{p^n}(a+b) = f_{p^n}(a) + f_{p^n}(b) = a^{p^n} + b^{p^n}$ a podobně $(-a)^{p^n} = -a^{p^n}$, $(a \cdot b)^{p^n} = a^{p^n} \cdot b^{p^n}$. Konečně 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 T □

Symbolem $k \times 1$ budeme v libovolném tělese označovat součet k kopií prvku 1 v případě kladného k a $k \times 1 = -|k| \times 1$ pro k záporné. Konečně $0 \times 1 = 0$

Poznámka 10.2. *Nechť T je konečné komutativní těleso, pak $P = \{k \times 1 |\ k \in \mathbf{N}\} \cong \mathbf{Z}_p$, kde p je prvočíslo, je podtěleso T a existuje n tak, že $|T| = |P|^n = p^n$.*

Důkaz. Nejprve si všimněme, že zobrazení $g : \mathbf{Z} \to T$ dané předpisem $g(k) = k \times 1$ je okruhový homomorfismus (viz také 2.1) a proto je $P = g(\mathbf{Z}) \cong \mathbf{Z}/\ker g = \mathbf{Z}/p\mathbf{Z} \cong \mathbf{Z}_p$ pro vhodné přirozené p. Protože je P podokruh tělesa, musí jít o obor integrity, tedy p je prvočíslo a P je těleso. Konečně každé těleso má nad svým libovolným podtělesem strukturu vektorového prostoru, tedy T je konečný vektorový prostor nad P a $|T| = |P|^n = p^n$, jestliže $n = dim_P(T)$. □

Věta 10.3. *Nechť $q \in \mathbf{N}$. Pak existuje komutativní těleso o q prvcích, právě když $q = p^n$ pro nějaké prvočíslo p a přirozené číslo n. Těleso o p^n prvcích je izomorfní rozkladovému nadtělesu polynomu $x^{p^n} - x$ nad $\mathbf{Z}_p$.*

Důkaz. ($\Rightarrow$) plyne okamžitě z 10.2.

($\Leftarrow$) Ukážeme, že rozkladové nadtěleso T polynomu $x^{p^n} - x$ nad $\mathbf{Z}_p$ má právě p^n prvků. Protože p nedělí $p^n - 1$ nemá polynom $x^{p^n} - x$ podle 8.14(3) žádný vícenásobný kořen, obsahuje T aspoň p^n prvků. V důsledku 10.1 je množina $Q = \{t \in T |\ t^{p^n} = t\}$ podtělesem, navíc $t^{p^n} = t$ právě když je t kořen polynomu $x^{p^n} - x$, tedy $|Q| = p^n$ (opět podle 8.5) 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 10.2, dostaneme, že všechny prvky U jsou kořenem polynomu $x^{p^n} - x$ nad tělesem $P = \{k \times 1 |\ k \in \mathbf{N}\} \cong \mathbf{Z}_p$, tedy U je rozkladové nadtěleso polynomu $x^{p^n} - x$ nad tělesem P. Závěr potom plyne z 9.12 □

Jednoznačně (až na izomorfismus) určené těleso o p^n prvcích se zpravidla značí $GF(p^n)$ (GF = Galois field).

Poznámka 10.4. *Nechť p je prvočíslo a k, n přirozené číslo. Pak k/n právě tehdy, když $(p^k - 1)/(p^n - 1)$.*

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

($\Leftarrow$) Nechť $(p^k - 1)/(p^n - 1)$ a $n = kd + r$, kde $0 \le r < k$. 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 $r = 0$. □

Věta 10.5. *Nechť T je konečné komutativní těleso a n přirozené číslo.*

(1) *T obsahuje podtěleso o q prvcích právě tehdy, když $q/|T|$ a $q - 1/|T| - 1$. Takové podtěleso je právě jedno.*
(2) *V $T[x]$ existuje ireducibilní polynom stupně n.*
(3) *Každý ireducibilní polynom stupně n z okruhu $\mathbf{T}[x]$ dělí polynom $x^{|T|^n} - x$.*

Důkaz. (1) ($\Rightarrow$) plyne z Lagrangeovy věty (1.13) použité pro grupy $T(+)$ a $T\setminus\{0\}(\cdot)$.

($\Leftarrow$) Podle 10.3 existuje takové prvočíslo p a přirozené číslo n $|T| = p^n$, tedy $q = p^k$ pro vhodné přirozené číslo $k \le n$. Díky 8.16 víme, že $T \setminus \{0\}(\cdot)$ je cyklická grupa, a proto podle 2.7 existuje její (jednoznažně určená) podgrupa G řádu $q - 1$. Protože podle 2.6 $u^{q-1} = 1$ pro každé $u \in G$, obshuje množina $Q = G \cup \{0\}$ právě všechny kořeny polynomu $x^{p^n} - x$. Tedy $Q = \{u \in T|\ u^q = u\}$ je podtěleso o q prvcích díky 10.1. Jeho jednoznačnost plyne z 2.6 a 2.7.

(2) Z 10.3 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 (1) a 10.3 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 9.8(3) algebraický a $U \setminus \{0\} = \langle\alpha\rangle \subseteq T(\alpha)$, proto $T(\alpha) = U$ a $\deg(m_\alpha) = [U : T] = n$ podle 9.8(1), kde m_α je minimální polynom algebraického prvku α nad T. Konečně m_α je nad T ireducibilní podle 9.6.

(3) 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 (2) můžeme bez újmy na obecnosti ztotožnit těleso T s izomorfním podtělesem tělesa U, které existuje podle (1). Těleso U je podle 10.3 rozkladovým nadtělesem polynomu $x^{q^n} - x$ nejen nad tělesem $\mathbf{Z}_p$, nýbrž i nad každým větším podtělesem, tedy i nad tělesem T. Dále podle 9.3 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 9.12 vzít tak, aby byl na podtělesech T identický, má m kořen v U, označme ho α. Snadno s pomocí 9.6 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 $\mathbf{T}[x]$. □

Věta 10.6. *Nechť T je konečné komutativní těleso, d přirozené číslo a $u \in T[x]$ ireducibilní polynom stupně n. Položme $q = |T|$. Následující tvrzení jsou ekvivalentní:*

(a) $(x^{q^n} - x)/(x^{q^d} - x)$ *v* $T[x]$,
(b) $u/(x^{q^d} - x)$ *v* $T[x]$,
(c) $(q^n - 1)/(q^d - 1)$ *v* $\mathbf{Z}$,
(d) n/d *v* $\mathbf{Z}$.

Důkaz. (a)⇒(b) z 10.5(3) plyne, že $u/(x^{q^n} - x)$ a z tranzitivity relace / dostáváme závěr.

(b)⇒(c) Opět uvážíme, že rozkladové nadtěleso U polynomu $(x^{q^d} - x)$ nad $\mathbf{Z}_p$ má podle 10.3 právě q^d prvků a obsahuje jako podtěleso těleso izomorfní T (a ta můžeme ztotožnit) podle 10.5(1). 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 9.8(1). Tedy $|T(\alpha)| = q^n$ a $(q^n - 1)/(q^d - 1)$ podle 10.5.

(c)⇒(a) Použijem obdobný argument jako v důkazu 10.4: je-li $(q^d - 1) = s(q^n - 1)$,pak $(x^{q^d} - x) = x(x^{q^n - 1} - 1)\sum_{i=0}^{s-1} x^{i(q^n-1)}$.

(c)⇔(d) Protože $q = p^r$ pro vhodné přirozené r a prvočíslo p podle 10.3, máme $((p^r)^n - 1)/((p^r)^d - 1) \Leftrightarrow rn/rd$ díky 10.4, což zřejmě nastává $\Leftrightarrow n/d$. □

Uvážíme-li, že se pro každé prvočíslo p polynom $x^{(p^n)^d} - x \in \mathbf{Z}_p[x]$ nad svým rozkladovým nadtělesem U podle 8.14(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 10.7. *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 10.8. (1) Hledáme-li nerozložitelné polynomy ze $\mathbf{Z}_2[x]$ stupně 4, víme z 10.5(3), 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 $\mathbf{Z}_2$ 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 $\mathbf{Z}_2$ součinem právě všech ireducibilních polynomů stupně 1 (takové jsou právě 2) a stupně 7. Proto nad $\mathbf{Z}_2$ existuje právě $18 = \frac{128-2}{7}$ nerozložitelných polynomů stupně 7.

(3) Spočítáme pomocí 10.7 neasociované nerozložitelné polynomy stupně šest nad tělesem $\mathbf{Z}_3$. 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 $\mathbf{Z}_3$ existuje právě $116 = \frac{729-(3\cdot 1+3\cdot 2+8\cdot 3)}{6}$.

11. Volné algebry a variety

Definice. Je-li I množina, budeme říkat zobrazení $\Omega : I \to \mathbf{N}$ *typ*. Řekneme, že 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. Buď $\Omega : I \to \mathbf{N}$ nějaký typ, X množina a nechť indexovaná množina symbolů operací $\{\alpha_i|\ i \in I\}$ je disjunktní s X. Definujme indukcí posloupnost množin W_i:

$W_0 = \{\alpha_i|\ i \in I, \Omega(i) = 0\} \cup X$ 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 $W_\Omega(X) = \bigcup_{n\in\mathbf{N}} W_n$ 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 11.1. Buď $X = \{x\}$ 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 11.2. *Nechť $\Omega : I \to \mathbf{N}_0$ nějaký typ a X je množina. Potom X generuje algebru termů $W_\Omega(X)(\alpha_i|\ i \in I)$.*

Důkaz. Dokážme indukcí podle n, že $W_n \subseteq \langle X\rangle$. Zřejmě $W_0 \subseteq \langle X\rangle$. Nechť $W_n \subseteq \langle X\rangle$. 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 $(\alpha_i, w_1, \dots, w_{\Omega(i)}) = \alpha_i(w_i, \dots, w_{\Omega(i)}) \in \langle X\rangle$, proto $W_{n+1} \subseteq \langle X\rangle$. □

Poznámka 11.3. *Buď $\Omega : I \to \mathbf{N}_0$ typ, X množina a $A(\alpha_i|\ i \in I)$ algebra typu Ω. Pak pro každé zobrazení $\varphi : X \to A$ existuje právě jeden homomorfismus $\overline{\varphi} : W_\Omega(X) \to A$ tak, že $\overline{\varphi}|_X = \varphi$.*

Důkaz. Budeme induktivně rozšiřovat zobrazení φ na množiny W_n. Nejprve definujme $\varphi_0 : W_0 \to A$ 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 $\varphi_n : W_n \to A$ rozšíříme ho na $\varphi_{n+1} : W_{n+1} \to A$ $\varphi_{n+1}(\alpha_i, w_1, \dots, w_{\Omega(i)}) = \alpha_i(\varphi_n(w_1), \dots, \varphi_n(w_{\Omega(i)}))$, jestliže $i \in I$, $\Omega(i) \neq 0$ a $w_1, \dots, w_{\Omega(i)} \in W_n$. Konečně položme $\overline{\varphi} = \bigcup_n \varphi_n$, Z konstrukce je zjevné, že jde o jedinou možnou definici rozšiřujícího homomorfismu. □

Věta 11.4. *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 11.3 na příslušný homomorfismus. □

Poznámka 11.5. *Nechť 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 $\varphi : W_\Omega(X) \to W_\Omega(Y)$. 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 $b : X \to Y$ můžeme ji podle 11.3 rozšířit na homomorfismus $\varphi : W_\Omega(X) \to W_\Omega(Y)$ a její inverz $b^{-1} : Y \to X$ na homomorfismus $\psi : W_\Omega(Y) \to W_\Omega(X)$. Z jednoznačnosti rozšíření identity na X resp. X na endomorfismus na $W_\Omega(X)$, resp. $W_\Omega(Y)$ plyne, že $\varphi\psi = Id$ a $\psi\varphi = Id$, tedy φ je izomorfismsu. □

Připomeňme definici součinové algebry. Mějme $n \in \mathbf{N}$, 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

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

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

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

Definice. Nechť 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 $\varphi : W_\Omega(X) \to A$ je $\varphi(u) = \varphi(w)$. Třídu $\mathcal{V}$ algeber typu Ω nazveme *varietou*, existuje-li taková množina identit M, že $\mathcal{V}$ je tvořena právě všemi algebrami typu Ω splňujícími všechny identity z M.

Věta 11.6 (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. ($\Rightarrow$) Nechť $\mathcal{V}$ je varieta s množinou identit M. Zvolme $A \in \mathcal{V}$ a vezměme nějakou podalgebru B algebry A. Označme $i : B \to A$ inkluzi množin a všimněme si, že je i homomorfismus. Máme-li nyní $(u, w) \in M$ a libovolný homomorfismus $\varphi : W_\Omega(X) \to B$, 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 $\psi : A \to B$, kde opět $A \in \mathcal{V}$, $(u, w) \in M$ a homomorfismus $\varphi : W_\Omega(X) \to \psi(B)$. Pro každé $x \in X$ definujme zobrazení $\mu : X \to A$ podmínkou $\mu(x) \in \psi(\varphi(x))^{-1}$. Zobrazení μ můžeme podle 11.3 rozšířit na homomorfismus $\overline{\mu} : X \to \psi(B)$, pro nějž $\psi\overline{\mu} = \varphi$. Protože $\overline{\mu}(u) = \overline{\mu}(v)$, dostáváme i $\varphi(u) = \psi\overline{\mu}(u) = \overline{\mu}(w) = \varphi(w)$, tedy $\psi(B) \in \mathcal{V}$.

Konečně mějme systém algeber $A_j \in \mathcal{V}$, kde $j \in J$, a homomorfismus $\varphi : W_\Omega(X) \to \prod_{j \in J} A_j$ a $(u, w) \in M$. Označme $\pi_k : \prod_{j \in J} A_j \to A_k$ pro každé $\in J$ 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 $\in J$, je podle definice součinu algeber $\varphi(u) = \varphi(w)$.

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

Zvolme libovolnou algebru $A \in \mathcal{U}$. Díky 11.4 existuje množina Y a homomorfismus $p : W_\Omega(Y) \to A$ 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 $\psi : W_\Omega(Y) \to \prod_{\rho \in R} W_\Omega(Y)/\rho$ 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 sučinové 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 ukážeme, že $\rho_Y \subseteq ker\ p$. Vezměme (a, b), aby platilo, že $p(a) \neq p(b)$ a nechť 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 $W_\Omega(X) \to A$, identita (a, b) na A není splněna, proto existuje algebra $B \in \mathcal{V}$ a takový homomorfismus $f : W_\Omega(X) \to B$, že $f(a) \neq f(b)$, který můžeme díky 11.3 rozšířit (na $Y \setminus X$ zobrazení dodefinujeme libovolně) na homomorfismus $f : W_\Omega(Y) \to B$. To znamená, že $(a, b) \notin \rho_Y$.

Konečně použitím 1. a 2.věty o izomorfismu dostáváme, že $A \cong W_\Omega(Y)/ker\ p$ je izomorfní faktorové algebře $W_\Omega(Y)/\rho_Y$, tedy díky uzavřenosti $\mathcal{V}$ na faktory dostáváme, že $A \in \mathcal{V}$. $\square$

Příklad 11.7. (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 přibyde ještě komutativita: $(x \cdot y, y \cdot x)$).

(3) Třída všech okruhů tvoří varietu.

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

12. Algebraický uzávěr

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.

Věta 12.1. *Nechť T je komutativní těleso. Pak existuje jeho algebraický uzávěr U.*

Důkaz. Mějme κ nějaké ordinální číslo (nebo indexujme 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 dánu 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 $T_i \subseteq T_{i+1}$, položme $T_1 = T$.

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. $\{p_\alpha |\ \alpha < \kappa_i\} = \{p \in T_i[x] |\ \deg p \leq i + 1\}$. 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 definujme $T_{i+1} = \bigcup_{\alpha<\kappa_i} T_{i\alpha}$.

Nyní stačí položit $U = \bigcup_{i\in\mathbf{N}} T_i$. 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. $\square$

Poznámka 12.2. *Žádné konečné komutativní těleso není algebraicky uzavřené.*

Důkaz. Je-li T je konečné těleso, polynom $1 + \prod_{t\in T}(x - t)$ (stupně $|T|$) nemá v T žádný kořen, tedy T není algebraicky uzavřené. $\square$

Důsledek 12.3. *Algebraický uzávěr konečného tělesa je nekonečný.*

Všimneme-li si, že polynomů omezeného stupně nad konečným tělesem je jen konečně mnoho a že rozkladové nadtěleso libovolného polynomu nad konečným tělesem je opět konečné podle 9.9, vidíme, že hodnoty κ_i i všechna tělesa $T_{i\alpha}$ a T_i jsou v důkazu 12.1 konečná. Algebraický uzávěr konečného tělesa tedy leží ve spočetném sjednocení konečných těles, proto musí být spočetný.

Příklad 12.4. Algebraický uzávěr libovolného konečného tělesa charakteristiky p obsahuje těleso o p^n prvcích pro každé kladné celé n.

13. Ireducibilní rozklad polynomů

Definice. Řekneme, že polynom f je *bez čtverců*, jestliže neexistuje žádný takový polynom g (nad týmž 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 13.1. *Pro každý polynom nad komutativním tělesem existuje bezčtvercový rozklad.*

Důkaz. Bezprostřední důsledek 7.10 spolu s 8.7. □

Poznámka 13.2. *Nechť T je komutativní těleso, $f \in T[x]$. Pak je f bez čtverců právě když 1 je $NSD(f, f')$.*

Důkaz. Postupujeme podobně jako v Poznámce 8.11. Jestliže $f = g^2h$, pak podle 8.10(3) $f' = g \cdot (gh)' + g' \cdot gh = g \cdot ((gh)' + g'h)$, tedy g/f'.

Předpokládejme, že 1 není $NSD(f, f')$, tedy podle 7.7 (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. □

Příklad 13.3. [Bezčtvercový rozklad polynomu nad tělesem kladné charakteristiky] Mějme těleso T prvočíselné charakteristiky p a $f \in T[x]$. Označujme $nsd(a, b)$ jednoznačně určený monický polynom, který je $NSD(a, b)$.

Položme $c_1 = nsd(f, f')$, $\quad g_1 = \frac{f}{c_1}$, $\quad h_1 = nsd(c_1, g_1)$, a induktivně definujme posloupnosti $\{c_i\}$, $\{g_i\}$, $\{h_i\}$:

$$c_i = \frac{c_{i-1}}{h_{i-1}}, \quad g_i = h_{i-1}, \quad h_i = nsd(c_i, g_i).$$

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

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

a proto

$$c_1 = nsd(f, f') = [\prod_{j \notin p\mathbf{N}} f_j^{j-1}] \cdot [\prod_{i \in p\mathbf{N}} f_i^i].$$

Odtud dostáváme, že $g_1 = \prod_{j \notin p\mathbf{N}} f_j$ a $h_1 = \prod_{j \geq 2, j \notin p\mathbf{N}} f_j$.

Podobně nahlédneme, že $c_k = [\prod_{j \geq k, j \notin p\mathbf{N}} f_j^{j-1}] \cdot [\prod_{i \in p\mathbf{N}} f_i^i]$ a že $g_k = h_{k-1} = \prod_{j \geq k, j \notin p\mathbf{N}} f_j$. Odtud snadno spočítáme, že $\frac{g_k}{h_k} = f_k$ pokud p nedělí p a $\frac{g_k}{h_k} = 1$ v opačném případě. Máme tedy algoritmus k nalezení členů bezčtvercového rozkladu pro všechna i, jež nedělí p. Všimneme-li si, že po konečně krocích dostaneme

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

Použijeme-li nyní rekurzivně algoritmus na polynom $\sum_i a_i x^i$, najdeme členy f_i bezčtvercový rozklad pro p/i, jestliže p^2 nedělí i. Dále můžeme pokračovat rekurzí.

Podrobnosti viz [MS].

Poznámka 13.4 (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 $\varphi : \mathbf{T}[x]/fT[x] \to \prod_{i=1}^n T[x]/f_iT[x]$ dané předpisem $\varphi([g]_f) = ([(g)modf_1], \dots [(g)modf_n])$ okruhový izomorfismus.*

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

Věta 13.5. *Buď T konečné komutativní těleso a f monický bezčtvercový polynom. Označme $V = T[x]/fT[x]$ a $W = \{u \in V|\ u^{|T|} = u\}$.*

(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 $1 \le \deg u \le \deg f$, potom $f = \prod_{s\in T} nsd(u-s, f)$.*
(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 $i \le k$ 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 skalárem, 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 $u \to u^{|T|}$ tvoří endomorfismus na $T[x]$ a tedy i na $V = T[x]/fT[x]$. Ovšem z 10.3 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) Buď $f = f_1 \cdot \dots \cdot f_k$ rozklad f na monické ireducibilní polynomy a označme $V_i = T[x]/f_iT[x]$ a $W_i = \{u \in V_i|\ u^{|T|} = u\}$. Podle 13.4 je zobrazení $\varphi : V \to \prod_{i=1}^k V_i$ dané předpisem $\varphi([v]_f) = ([(v) mod\ f_1], \dots [(v) mod\ f_n])$ 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 $f / \prod_{s\in T} nsd(u-s, f)$. Jelikož jsou polynomy $u-s$ a $u-t$ pro $t \ne s$ nesoudělné, dostáváme $\prod_{s\in T} nsd(u-s, f)/f$, 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_1f_2 nedělí $u-s$ pro žádné $s \in T$. Předpokládejme nyní, že pro každé i existuje takové $s_i \in T$, že $f_1f_2/(u_i - s_i)$ a vezměme T-lineární kombinaci $u = \sum_{i=1}^k a_iu_i$. Potom $f_1f_2 / \sum_{i=1}^k a_i(u_i - s_i) = u - \sum_{i=1}^k a_is_i$, čímž dostáváme spor. Dokázali jsme, že existuje takové i, že f_1f_2 nedělí $(u_i - s)$ pro žádné $s \in T$. Nyní zbývá pomocí (3) zvolit $s \in T$, pro nějž $f_1/(u_i - s)$. □

Příklad 13.6. [Berlekampův algoritmus] Pomocí předchozí věty budeme umět rozložit bezčtvercový polynom nad konečným tělesem, najdeme-li bázi vektorového prostoru W. Položme $n = \deg f$, $r = |T|$ a $(x^{r(j-1)}) mod\ f = \sum_{i=1}^n q_{ij}x^{i-1}$ pro každé $j = 1, \dots, n$. Nyní sestavíme matici $Q = (q_{ij})$. Všimneme-li si, že $Q\mathbf{v}^T = \mathbf{v}^T$, právě když $(\sum_{i<n} v_ix^i)^r \equiv (\sum_{i<n} v_ix^i)\ mod\ f$, kde $\mathbf{v} = (v_0, \dots, v_{n-1})$, stačí nám najít bázi řešení homogenní soustavy rovnic s maticí $Q - I_n$. Podrobnosti viz [MS].

[MS] - odkazuje na bakalářskou práci Milana Straky (2006)
http://fox.ucw.cz/papers/factoring/