7. Dělitelnost

Definice. Řekneme, že $S(\cdot, 1)$ je *komutativní monoid s krácením*, pokud je $S(\cdot, 1)$ monoid s komutativní operací $\cdot$ splňující pro každé $a, b, c \in S$ podmínku $a \cdot c = b \cdot c \;\Rightarrow\; a = b$.

Buď $S(\cdot, 1)$ komutativní monoid s krácením 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. 1) $\mathbf{N}(\cdot, 1)$ a $\mathbf{Z} \setminus \{0\}(\cdot, 1)$ jsou komutativní monoidy s krácením.

2) Je-li $R(+, \cdot, -, 0, 1)$obor integrity, pak je $R \setminus \{0\}(\cdot, 1)$ komutativní monoid s krácením.

Poznámka 7.1. *Buď $R\setminus\{0\}(\cdot, 1)$ multiplikativní monoid (tedy komutativní monoid s krácením) nějakého oboru integrity $R(+, \cdot, -, 0, 1)$ (například okruhu celých čísel nebo reálných polynomů). Pak a/b právě když $bR \subseteq aR$ a $a\|b$ právě když $bR = aR$.*

Důkaz. Přímý důsledek definice. □

Poznámka 7.2. *Nechť $S(\cdot, 1)$ 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) *$S/\|(\cdot, [1]_{\|})$ je komutativní monoid s krácením a relace "dělí" na něm tvoří uspořádání.*

Důkaz. (1) viz [D, 5.10], (2) viz [D, 5.2], (3) viz [D, 5.5]. □

Příklad. Komutativní monoidy $\mathbf{N}(\cdot, 1)$ a $\mathbf{Z} \setminus \{0\}/\|(\cdot, 1)$ jsou izomorfní.

Definice. Buď $S(\cdot, 1)$ komutativní monoid s krácením 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, pokud c není invertibilní a $c = a \cdot b \;\Rightarrow\; c\|a$ nebo $c\|b$. Prvek c nazveme *prvočinitelem*, pokud c není invertibilní a $c/a \cdot b \;\Rightarrow\; c/a$ nebo c/b.

Poznámka 7.3. *Nechť $S(\cdot, 1)$ 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) viz [D, 5.12] a (2) viz [D, 5.13]. □

Poznámka 7.4. *Mějme $S(\cdot, 1)$ 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. Viz [D, 5.14]. □

Věta 7.5. *Nechť je každý ireducibilní prvek komutativního monoidu s krácením $S(\cdot, 1)$ 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 bijekce σ tak, že $p_i \| q_{\sigma(i)}$ pro všechna $i = 1, \dots, r$.*

Důkaz. Viz [D, 5.16]. □

Příklad. Uvažujme podokruh $\mathbf{Z}[\sqrt{5}] = \{a + \sqrt{5}b|\ a, b \in \mathbf{Z}\}$ 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 $\sqrt{5}-1$).

Zároveň dostáváme dva neasocivané ireducibilní rozklady prvku $4 = 2 \cdot 2 = (\sqrt{5}+1)\cdot(\sqrt{5}-1)$.

Definice. Buď $R(+, \cdot, -, 0, 1)$ obor integrity. *největší společný dělitel*, *ireducibilní prvek* respektive *prvočinitel* oboru integrity R bude největší společný dělitel, ireducibilní prvek, respektive prvočinitel komutativního monoidu s krácením $R \setminus \{0\}(\cdot, 1)$ Řekneme, že je R *obor integrity hlavních ideálů*, jestliže je jeho každý ideál hlavní.

Poznámka 7.6. *Buď $R(+, \cdot, -, 0, 1)$ obor integrity hlavních ideálů a $a_1, \dots, a_n \in R \setminus \{0\}$. 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. Viz [D, 10.9]. □

Věta 7.7. *Buď $R(+, \cdot, -, 0, 1)$ je 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 takové ireducibilní prvky $p_1, \dots, p_n \in R \setminus \{0\}$, že $a = p_1 \cdot \dots \cdot p_n$. Jsou-li navíc prvky $q_1, \dots, q_k$ ireducibilní takové, že $a = q_1 \cdot \dots \cdot q_k$, pak $n = k$ a existuje bijekce σ tak, že $p_i \| q_{\sigma(i)}$ pro všechna $i = 1, \dots, n$*

Důkaz. (1) Podle 7.6 jsou splněny předpoklady 7.4, které implikují závěr.
(2) viz [D, 10.11]. □

Příklad. V momoidech $\mathbf{N} \setminus \{0\}(\cdot, 1)$ a $\mathbf{Z} \setminus \{0\}(\cdot, 1)$ existují největší společní dělitelé a zřejmě existuje rozklad na ireducibilní prvky, tedy jsou v $\mathbf{N}$ jsou ireducibilní rozklady určeny jednoznačně, v $\mathbf{Z}$ jsou určeny jednoznačné až na znaménko.

8. Okruhy polynomů

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 $\sum_{m \in M} p(m).m$. Na $R[M]$ definujme binární operace + a $\cdot$, unární operaci $-$ a nulární operace $\mathbf{0}$ a $\mathbf{1}$: $p+q = \sum_{m \in M}(p(m)+q(m)).m$, $p \cdot q = \sum_{m \in M}(\sum_{r \cdot s = m} p(r) \cdot q(s)).m$, $-p = \sum_{m \in M}(-p(m)).m$, $\mathbf{0} = \sum_{m \in M} 0.m$, $\mathbf{1} = 1.e + \sum_{m \in M \setminus \{e\}} 0.m$.

Poznámka 8.1. *Nechť $R(+, \cdot, -, 0, 1)$ je okruh a $M(\cdot, e)$ je monoid.*

(1) *$R[M](+, \cdot, -, \mathbf{0}, \mathbf{1})$ je okruh,*
(2) *zobrazení $i : R \to R[M]$ dané předpisem $i(r) = r.e$ (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 $\nu(m) = 1.m$ je prostý homomorfismus monoidu $M(\cdot, e)$ do monoidu $R[M](\cdot, \mathbf{1})$.*

Důkaz. (1) Přímočaré ověření definice okruhu,
(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 $p = \sum_{n\in\mathbf{N}_0} p(n).x^n$.

Příklad. 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 $R[{\mathbf{N}_0}^n] = (R[x_1,\dots,x_{n-1}])[x_n]$ se součinovým monoidem ${\mathbf{N}_0}^n(+,(0,\dots,0)$.

Poznámka 8.2. *Nechť $S(+,\cdot,-,0,1)$ je okruh, R jeho podokruh a nechť $\alpha\in S$. Potom 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. Viz [D, 10.17]. □

Homomorfismu j_α říkáme dosazovací homomorfismus.

Definice. Buď $R(+,\cdot,-,0,1)$ je okruh a $p = \sum_{n\in\mathbf{N}_0} a_n.x^n \in R[x]$. 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 $st\ p$.

Poznámka 8.3. *Nechť $R(+,\cdot,-,0,1)$ je okruh a $p,q\in R[x]$. Pak platí:*

(1) *$st\ -p = st\ p$,*
(2) *$st\ p+q \le max(st\ p,\ st\ q)$,*
(3) *je-li $p\neq 0\neq q$, pak $st\ p\cdot q \le st\ p + st\ q)$, je-li navíc R oborem integrity, potom $st\ p\cdot q = st\ p + st\ q)$,*
(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 $st\ p = 0$ a $p(0)$ je invertibilní prvek okruhu R.*

Důkaz. (1) - (3) viz [D, 10.3], (4) Viz [D, 10.17] a (5) viz 10.5. □

Příklad. Je-li p prvočíslo, pak $\mathbf{Z}_p(+,\cdot,-,0,1)$ je komutativní těleso charakteristiky p, tedy obor integrity. Podle Poznámky 7.3 je $Z_p[x]$ rovněž obor integrity (zřejmě nekonečný). Poznámka 7.1 (2) zaručuje existenci prostého okruhového homomorfismu Z_p do $Z_p[x]$, tedy charakteristika okruhu $Z_p[x]$ je rovna p. Pro obor integrity $Z_p[x]$ existuje jeho podílové těleso $Q(Z_p[x])$. Tím jsme zkonstruovali nekonečné těleso charakteristiky p.

Věta 8.4 (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 $m = st\ b \ge 0$ 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 $st\ r < st\ b$.*

Důkaz. Viz [D, 10.6]. □

Definice. Buď $R(+,\cdot,-,0,1)$ obor integrity. Řekneme, že R je *eukleidovský obor integrity*, pokud existuje zobrazení $\nu : R\to\mathbf{N}_0\cup\{-1\}$ (tzv. *eukleidovská funkce*) splňující pro každé $a,\ b\in R$ podmínky:

(1) pokud a/b a $b\neq 0$, pak $\nu(a)\le\nu(b)$,
(2) pokud $b\neq 0$, existuje $q,r\in R$ takové, že $a = b\cdot q + r$ a $\nu(r) < \nu(b)$.

Poznámka 8.5. *Každý euklidovský obor integrity je oborem integrity hlavních ideálů.*

Důkaz. Viz [D, 10.8]. □

Důsledek 8.6. *Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso. Pak je $T[x]$ eukleidovským okruhem s eukleidovskou funkcí danou stupněm polynomů, tudíž je $T[x]$ oborem integrity hlavních ideálů.*

Příklad. (1) Okruh celých čísel je eukleidovským oborem integrity s eukleidovskou funkcí $|-|$.

(2) Podokruh $\mathbf{Z}[i] = \{a+bi|\ a,b \in \mathbf{Z}\}$ okruhu komplexních čísel je eukleidovským oborem integrity s eukleidovskou funkcí $\nu(a+bi) = a^2+b^2$.

(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 $\nu(a+b\sqrt{2}) = |a^2-2b^2|$.

Věta 8.7 (Eukleidův algoritmus). *Buď $R(+,\cdot,-,0,1)$ eukleidovským okruhem 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. Viz [D, 10.13]. □

Definice. Nechť $S(+,\cdot,-,0,1)$ je okruh a R jeho podokruh. Řekneme, že $\alpha \in S$ je *kořenem* polynomu $p \in R[x]$, pokud $j_\alpha(p) = p(\alpha) = 0$. *Kořenovým činitelem* (kořenu α) nazveme polynom tvaru $x-\alpha$. Řekneme, že se polynom $p \in R[x]$ rozkládá na *kořenové činitele* v $R[x]$, existují-li takové prvky $a,\alpha_1,\dots,\alpha_n \in R$, že $p = a\cdot(x-\alpha_1)\cdot\dots\cdot(x-\alpha_n)$.

Poznámka 8.8. *Nechť $R(+,\cdot,-,0,1)$ je obor integrity, $\alpha \in R$ a $p \in R[x]\setminus\{0\}$. Pak α je kořenem p právě tehdy, když $(x-\alpha)/p$.*

Důkaz. Viz [D, 10.18]. □

Poznámka 8.9. *Nechť $R(+,\cdot,-,0,1)$ je obor integrity a $p \in R[x]$. Je-li st $p \geq 0$, potom p má nejvýše st p kořenů.*

Důkaz. Přímý důsledek Poznámky 8.3 (3). □

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 $(\sum_{i\geq 0} a_i x^i)' = \sum_{i\geq 0}(i+1)a_{i+1}x^i$. Řekneme, že $\alpha \in R$ je *vícenásobným kořenem* polynomu p, pokud $(x-\alpha)^2/p$.

Poznámka 8.10. *Nechť $R(+,\cdot,-,0,1)$ je komutativní okruh, $\alpha \in R$ a $p,q \in R[x]$. Pak platí:*

1. $(p+q)' = p'+q'$,
2. $(\alpha p)' = \alpha p'$,
3. $(p\cdot q)' = p'\cdot q + p\cdot q'$.

Důkaz. Vlastnosti dostáváme okamžitě z definice. □

Poznámka 8.11. *Buď $R(+,\cdot,-,0,1)$ obor integrity, $p \in R[x]$ a nechť $\alpha \in R$ je kořen p. Potom α je vícenásobným kořenem, právě když je α kořenem p'.*

Důkaz. Viz [D, 10.14]. □

Důsledek 8.12. *Nechť $R(+,\cdot,-,0,1)$ je obor integrity, st $p \geq 1$ a $p \in R[x]$. Pokud 1 je $NSD(p,\ p')$, pak p nemá žádný vícenásobný kořen.*

Důkaz. Viz [D, 10.15]. □

Důsledek 8.13. *Nechť $R(+,\cdot,-,0,1)$ je obor integrity a charakteristika R nedělí přirozené číslo n. Potom polynomy $x^n - 1$ a $x^{n+1} - x$ nemají vícenásobný kořen.*

Důkaz. Viz [D, 10.16]. □

Příklad. V tělese charakteristiky 3 (např $\mathbf{Z}_3$) platí, že $(x-1)^3 = x^3 - 1$, tedy předpoklad o charakteru z předchozího důsledku nemůžeme odstranit.

Nyní už jsme s to dokázat nedokázané tvrzení z 5. kapitoly:

Věta 8.14. *Nechť $T(+,\cdot)$ je komutativní těleso a nechť G je konečná podgrupa multiplikativní grupy $T \setminus \{0\}(\cdot,{}^{-1},1)$. Potom G je cyklická grupa.*

Důkaz. Viz [D, 10.19]. □

9. Kořenová a rozkladová nadtělesa

Definice. Nechť $R(+,\cdot,-,0,1)$ a $S(+,\cdot,-,0,1)$ jsou okruhy a $f : R \to S$ je homomorfismus okruhů. Potom 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 $T(+,\cdot,-,0,1)$ 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. *$f j_\alpha = j_{f(\alpha)} f_x$ pro každé $\alpha \in R$.*

Důkaz. (1) viz [D, 11.1], (2) viz [D, 11.2], (3) přímá implikace viz [D, 11.3] a zpětnou dostaneme aplikací 8.1(2), (4) viz [D, 11.4]. □

Poznámka 9.2. *Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso a $u \in T[x] \setminus \{0\}$. Pak $T[x]/uT[x]$ je komutativní těleso, právě když je u ireducibilní. Je-li u ireducibilní, je zobrazení $t \to t + uT[x]$ prostý homomorfismus tělesa T do tělesa $T[x]/uT[x]$.*

Důkaz. Viz [D, 11.6]. □

Poznámka 9.3. *Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso a $u \in T[x]$ a $st(u) > 0$. Potom zobrazení $\mu(t) = t + uT[x]$ je prostý homomorfismus tělesa T do tělesa $T[x]/uT[x]$.*

Důkaz. Viz [D, 11.6]. □

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

Věta 9.4. *Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso a $u = \sum_{i\geq 0} a_i y^i \in T[y]$ je ireducibilní polynom stupně aspoň 1. Pak $(T[y])_u$ je komutativní těleso a polynom $\sum_{i\geq 0} a_i x^i$ má v $(T[y])_u$ kořen.*

Důkaz. Viz [D, 11.7]. □

Definice. Nechť $U(+,\cdot,-,0,1)$ je komutativní těleso a $T \subseteq U$. Řekneme, že T je *podtěleso* U (resp. U je *nadtěleso* T, pokud T je podokruh okruhu $U(+,\cdot,-,0,1)$ a T je těleso (tj. navíc $T \setminus \{0\}$ je podgrupou multiplikativní grupy $U \setminus \{0\}(\cdot,^{-1},1)$ tělesa U).

Důsledek 9.5. *Je-li $T(+,\cdot,-,0,1)$ komutativní těleso a $u \in T[x]$ je polynom stupně aspoň 1, pak platí:*

(1) *existuje komutativní těleso U tak že T je podtěleso U a u má v U aspoň jeden kořen,*
(2) *existuje komutativní těleso V tak že T je podtěleso V a u se ve V rozkládá na kořenové činitele.*

Důkaz. (1) viz [D, 11.8] a (2) viz [D, 11.9]. □

Poznámka 9.6. *Množina všech podtěles komutativního tělesa tvoří uzávěrový systém.*

Důkaz. Plyne okamžitě z toho, že podokruhy T tvoří uzávěrový systém, podgrupy $T \setminus \{0\}$ tvoří rovněž uzávěrový systém a průnik dvou uzávěrových systémů je opět uzávěrový systém. □

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

Značení. Mějme komutativní tělesa $T \subseteq U$ a $\alpha \in U$ (resp. $S \subseteq U$). Označme
$T[\alpha]$ (resp. $T[S]$) nejmenší podokruh U obsahující množinu $T\cup\{\alpha\}$ (resp. $T\cup S$),
$T(\alpha)$ (resp. $T(S)$) nejmenší podtěleso U obsahující množinu $T\cup\{\alpha\}$ (resp. $T\cup S$).

Poznámka 9.7. *Nechť $T \subseteq U$ jsou komutativní tělesa, $\alpha \in U$, $S \subset U$.*

(1) $T[\alpha] = \{p(\alpha) |\ p \in T[x]\}$,
(2) $T[\alpha] \subseteq T(\alpha)$,
(3) $T[S] \subseteq T(S)$.

Důkaz. (1) viz [D, 12.2], (2) a (3) zřejmé. □

Definice. Nechť $T \subseteq U$ jsou komutativní tělesa a $p \in T[x]$. Řekneme, že U je *kořenové nadtěleso* polynomu p, pokud $U = T(\alpha)$ pro nějaký kořen $\alpha \in U$ polynomu p. 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 9.8. *Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso a $p \in T[x]$, st $p \geq 1$.*

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

Důkaz. Podle 9.5 existuje těleso U (V), které obsahuje kořen (nad nímž se p rozkládá na kořenové činitele) a podle 9.6 můžeme vzít nejmenší podtěleso U (V) s takovou vlastností. □

Definice. Nechť $T \subseteq U$ jsou komutativní tělesa a $\alpha \in U$. Řekneme, že α je *algebraický prvek* nad T, existuje-li nenulový polynom $p \in T[x]$ tak, že $j_\alpha(p) = p(\alpha) = 0$. 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 $a_{stp} = 1$.

Věta 9.9. *Buď $T \subseteq U$ komutativní tělesa a $\alpha \in U$ je algebraický prvek nad T. Pak existuje právě jeden monický polynom $m \in T[x]$ takový, že pro každé $p \in T[x] \setminus \{0\}$ platí, že $p(\alpha) = 0$, právě když m/p. Navíc m_α je ireducibilní, $(T[x])_{m_\alpha} \cong T(\alpha)$ a $T[\alpha] = T(\alpha)$.*

Důkaz. Viz [D, 12.3]. □

Definice. Polynom z předchozí věty nazveme *minimálním polynomem* algebraického prvku α, budeme ho značit m_α.

Definice. Buď $T \subseteq U$ komutativní tělesa. *Stupeň rozšíření* U nad T definujeme jako $[U : T] = dim_T U$, kde U chápeme jako vektorový prostor nad tělesem T.

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

Poznámka 9.10. *Nechť $T \subseteq U \subseteq V$ jsou do sebe zařazená komutativní tělesa. Potom $[V : T] = [V : U][U : T]$.*

Důkaz. Viz [D, 12.1]. □

Poznámka 9.11. *Nechť $T \subseteq U$ jsou komutativní tělesa a $\alpha \in U$.*

(1) *Je-li α algebraický, pak $[T(\alpha) : T] = st\ m_\alpha$,*
(2) *je-li $[T(\alpha) : T]$ konečné, pak je α algebraický,*
(3) *je-li $[U : T]$ konečné, pak je U algebraické rozšíření tělesa T.*

Důkaz. (1) a (2) viz [D, 12.4] a (3) viz 12.5. □

Příklad. (1) $\mathbf{Q}(\sqrt[3]{2}) = \mathbf{Q}[\sqrt[3]{2}] = \{x + y\sqrt[3]{2} + z\sqrt[3]{4} \mid x, y, z \in \mathbf{Q}\}$ je kořenové nadtěleso polynomu $x^3 - 2$ nad $\mathbf{Q}$ a $[\mathbf{Q}(\sqrt[3]{2}) : \mathbf{Q}] = 3$, tedy $x^3 - 2$ je minimální polynom algebraického prvku $\sqrt[3]{2}$.

(2) $\mathbf{R}$ není algebraickým rozšířením tělesa $\mathbf{Q}$.

Poznámka 9.12. *Nechť $T \subseteq U$ jsou komutativní tělesa a $\alpha_1, \dots, \alpha_n \in U$ jsou algebraické prvky nad T. Pak $T(\alpha_1, \dots, \alpha_n) = T[\alpha_1, \dots, \alpha_n]$ je algebraickým rozšířením tělesa T.*

Důkaz. Viz [D, 12.6]. □

Důsledek 9.13. *Nechť T je komutativní těleso, $p \in T[x]$ a nechť U je 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. 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 8.12 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 9.14. *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. Viz [D, 13.3]. □

Věta 9.15. *Nechť T_1 a T_2 jsou komutativní tělesa, $f : T_1 \to T_2$ je izomorfismus a nechť U_1 je rozkladové nadtěleso polynomu $p \in T_1[x]$ a U_2 je rozkladové nadtěleso polynomu $f_x(p) \in T_2[x]$. Označme $\alpha_1, \dots, \alpha_n$ všechny kořeny polynomu p v U_1 a $\beta_1, \dots, \beta_m$ všechny kořeny polynomu $f_x(p)$ v U_2. Potom $n = m$ a existuje permutace σ a izomorfismus $g : U_1 \to U_2$ tak, že $g(\alpha_i) = \beta_{\sigma(i)}$ pro $i = 1, \dots, n$ a $g(t) = f(t)$ pro všechna $t \in T_1$.*

Důkaz. Viz [D, 13.4]. □

Důsledek 9.16. *Nechť T je komutativní těleso, $p \in T[x]$. Pak existuje až na izomorfismus právě jedno rozkladové nadtěleso polynomu p.*

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

Věta 9.17. *Nechť T je komutativní těleso. Pak existuje jeho algebraický uzávěr U.*

10. Konečná tělesa

Poznámka 10.1. *Žádné konečné komutativní těleso není algebraicky uzavřené.*

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

Důsledek 10.2. *Algebraický uzávěr konečného tělesa má (nekonečně) spočetnou mohutnost.*

Poznámka 10.3. *Buď T komutativní těleso (prvočíselné) 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. Viz [D, 7.22]. □

Poznámka 10.4. *Nechť T je konečné komutativní těleso, pak $P = \{k \times 1 \mid k \in \mathbf{N}\} \cong \mathbf{Z}_p$, kde p je prvočíslo, je podtěleso T a existuje n tak, že $|T| = |P|^n = p^n$.*

Důkaz. Viz [D, 13.5]. □

Věta 10.5. *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. Viz [D, 13.5]. □

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

Důsledek 10.6. *Konečné komutativní těleso T obsahuje podtěleso o q prvcích právě tehdy, když $q/|T|$ a $q-1/|T|-1$. Takové podtěleso je určeno jednoznačně.*

Poznámka 10.7. *Nechť p je prvočíslo a k, n přirozené číslo. Pak k/n právě tehdy, když $(p^k-1)/(p^n-1)$.*

Věta 10.8. *Pro každé konečné komutativní těleso T a přirozené číslo n existuje nad T ireducibilní polynom stupně n.*

Důkaz. Viz [D, 13.6]. □

Důsledek 10.9. *Pro každé prvočíslo p a přirozené číslo n existuje nad $\mathbf{Z}_p$ ireducibilní polynom stupně n.*

Poznámka 10.10. *Nechť T je konečné komutativní těleso. Každý ireducibilní polynom stupně n z okruhu $\mathbf{T}[x]$ dělí polynom $x^{|T|^n}-x$.*

Věta 10.11. *Nechť T je konečné komutativní těleso, d přirozené číslo a $u \in \mathbf{T}[x]$ ireducibilní polynom stupně k. Položme $q = |T|$. Následující tvrzení jsou ekvivalentní:*

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

Důsledek 10.12. *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. 1) Hledáme-li nerozložitelné polynomy ze $\mathbf{Z}_2[x]$ stupně 4, víme z Poznámky 10.8, že všechny musí dělit polynom $x^{16}-x$, resp. $x^{15}-1$. Dále nám Důsledek 10.10 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) Neboť 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 Důsledků 9.9 a 9.10 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 $116 = \frac{729-(3\cdot 1+3\cdot 2+8\cdot 3)}{6}$.

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 10.13. *Pro každý polynom nad komutativním tělesem existuje bezčtvercový rozklad.*

Důkaz. Bezprostřední důsledek 7.7 spolu s 8.6. □

Poznámka 10.14. *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 $f = g^2 h$, 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 (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 10.15 (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 $\varphi([g]_f) = ([(g) mod f_1], \dots [(g) mod f_n])$ okrohový izomorfismus.*

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

Věta 10.16. *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 $1 \leq st\ u \leq st\ f$, 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 f_1 a f_2 dva neasociované ireducibilní faktory f, potom existuje takové $i \leq k$ a $s \in T$, že f_1 dělí $(w_i - s)$ a f_2 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 Poznámce 10.3 využít toho, že zobrazení $p \to u^|T|$ tvoří endomorfismus na $T[x]$ a tedy i na $V = T[x]/fT[x]$. To ovšem plyne z Věty 10.5.

(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 Poznámky 10.15 je $\varphi([v]_f) = ([(v) mod f_1], \dots [(v) mod f_n])$ 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 (viz 10.3) 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 $t \neq s$ nesoudělné, dostáváme $f / \prod_{s\in T} nsd(u-s, f)$, 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 $u - 1$. 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 vlastnosti u a nesoudělnosti $u - s$ a $u - t$ pro $t \neq s$. □

Příklad (Berlekampův algoritmus)**.** Pomocí předchozí věty budeme umět rozložit bezčtvercový polynom, najdeme-li bázi vektorového prostoru W.

Položme $(x^{j-1}) mod\ f = \sum_{i=1}^n q_{ij}x^i$ pro každé $j = 1, \dots, n$ a setsvme matici $Q = (q_{ij})$. Všimneme-li si, že $Q\mathbf{v}^T = \mathbf{v}^T$, právě když $(\sum_{i<n} v_ix^i) \equiv (\sum_{i<n} v_ix^i)\ mod\ f$, 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].

11. Boleovy algebry

Připomeňme, že svaz můžeme chápat jako algebru $S(\wedge, \vee)$ nebo uspořádanou množinu $(S, \leq)$ (splňující jisté podmínky, viz 3. kapitola).

Definice. Řekneme, že svaz $S(\wedge, \vee)$ je *distributivní*, platí-li pro každé $a, b, c \in S$, že $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

Poznámka 11.1. *Svaz $S(\wedge, \vee)$ je distributivní, právě když pro každé $a, b, c \in S$ platí, že $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ (tj. svaz $S(\wedge, \vee)$ je distributivní, právě když je opačný svaz $S(\vee, \wedge)$ distributivní).*

Důkaz. Viz [D, 14.6]. □

Poznámka 11.2. *Každý distributivní svaz je modulární.*

Důkaz. Viz [D, 14.6]. □

Příklad. Nechť $M_5 = \{\mathbf{0}, \mathbf{1}, u, v, w\}$, buď $\mathbf{0}$ nejmenší prvek, $\mathbf{1}$ největší prvek a $u \vee v = u \vee w = v \vee w = \mathbf{1}$ a $u \wedge v = u \wedge w = v \wedge w = \mathbf{0}$. Pak $M_5(\wedge, \vee)$ je modulární svaz, který není distributivní.

Definice. Nechť má svaz $S(\wedge, \vee)$ nejmenší prvek $\mathbf{0}$ a největší prvek $\mathbf{1}$. *Komplementem* prvku $a \in S$ nazveme takový prvek $a' \in S$, že $a \vee a' = \mathbf{1}$ a $a \wedge a' = \mathbf{0}$.

Poznámka 11.3. *Každý prvek distributivního svazu má nejvýše jeden komplement.*

Důkaz. Viz [D, 14.8]. □

Definice. *Booleovou algebrou* nazveme takovou algebru $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$, že $S(\wedge, \vee)$ je distributivní svaz s největším prvkem $\mathbf{1}$ a nejmenším prvkem $\mathbf{0}$ a unární operace $'$ přiřadí každému prvku jeho komplement.

Poznámka 11.4. *Nechť $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ je Booleova algebra. Pak pro každé $a, b \in S$ platí:*

(1) $(a')' = a$,
(2) $(a \vee b)' = a' \wedge b'$,
(3) $(a \wedge b)' = a' \vee b'$,
(4) $(\mathbf{1})' = \mathbf{0}$ *a* $(\mathbf{0})' = \mathbf{1}$.

Důkaz. Viz [D, 14.9]. □

Příklad. Nechť $\mathcal{P}(X)$ je množina všech podmnožin množiny X a pro každou podmnožinu $Y \subseteq X$ definujme $Y' = X \setminus Y$. Pak $\mathcal{P}(X)(\cup, \cap, \emptyset, X, \ ')$ je Booleova algebra.

Vezmeme-li $M = \{m_1, \dots, m_n\}$ neprázdnou konečnou podmnožinu Booleovy algebry, pak značme $\bigwedge M = m_1 \wedge m_2 \wedge \dots \wedge m_n$ a $\bigvee M = m_1 \vee m_2 \vee \dots \vee m_n$. Dále $\bigwedge \emptyset = \mathbf{1}$ a $\bigvee \emptyset = \mathbf{0}$.

Věta 11.5. *Buď $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ konečná Booleova algebra a A buď množina všech atomů svazu S. Potom zobrazení $\varphi : \mathcal{P}(A) \to S$ dané předpisem $\varphi(B) = \bigvee B$ je izomorfismus Booleových algeber $S(\vee, \wedge, \mathbf{0}, \mathbf{1}, \ ')$ a $P(A)(\cup, \cap, \emptyset, X, \ ')$.*

Důkaz. Viz [D, 15.2]. □

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. Algebra $\mathcal{P}(X)(\div, \cap, Id, \emptyset, X)$, kde $\div$ značí symetrickou diferenci, je pro každou neprázdnou množinu X Booleův okruh.

Poznámka 11.6. *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 $S(+, \wedge, Id_S, \mathbf{0}, \mathbf{1})$ je Booleův okruh. Každá podalgebra resp. kongruence Booleovy algebry $S(\vee, \wedge, \mathbf{0}, \mathbf{1},\ ')$ je podokruhem resp. kongruencí Booleova okruhu $S(+, \wedge, Id_S, \mathbf{0}, \mathbf{1})$.*

Důkaz. Viz [D, 15.3]. □

Poznámka 11.7. *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. Viz [D, 15.3]. □

Příklad. 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.

[D] - odkazuje na skripta docenta Drápala na adrese
http://www.karlin.mff.cuni.cz/~drapal/skripta/

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