Algebra 2

Michal Vaner

24. února 2010

1 Dělitelnost

Řekneme, že $S(\cdot, 1)$ je ***komutativní monoid s krácením***, je-li $\cdot$ komutativní a asociativní a funguje tam krácení: $\forall a, b, c \in S; a \cdot b = a \cdot c \rightarrow b = c$.

V $S(\cdot, 1)$ řekneme, že a ***dělí*** b $(a \backslash b)$, $a, b \in S$, jestliže $\exists c \in S; b = a \cdot c$.

a je ***asociováno*** s b $(a||b)$, pokud $a \backslash b \wedge b \backslash a$.

Poznámka:
Je-li $R(+, \cdot, -, 0, 1)$ obor integrity a $a, b \in R - \{0\}$, pak $a \backslash b$ (v $R - \{0\}$ $(\cdot, 1)$) $\Leftrightarrow b \cdot R \subseteq a \cdot R$. $a||b \Leftrightarrow a \cdot R = b \cdot R$.

Důkaz:
$b = a \cdot c$, což znamená $b \cdot 1 \in a \cdot R$, $b \cdot r = a \cdot c \cdot r$.

$b \cdot 1 \in b \cdot R \Rightarrow \exists c \in R; b = a \cdot c$. Zřejmě $c \neq 0$.

Poznámka:

- $\forall a, b \in S \exists$ nejvýše jedno $c \in S; a = b \cdot c$
- $\forall a, b \in S; a||b \Leftrightarrow \exists u \in S$ invertibilní $; a = b \cdot u$
- $||$ je kongruence na S.
- $S/||(\cdot, [1]_{||})$ je opět komutativní monoid s krácením, na němž relace „dělí“ tvoří uspořádání.

$a, b, c, d, a_1, \ldots, a_n \in S$. Řekneme, že c je ***největší společný dělitel*** prvků $a_1, \ldots, a_n$ (c je $NSD(a_1, \ldots, a_n)$), $c \backslash a_i \wedge (d \backslash a_i \Rightarrow d \backslash c)$.

O prvku c řekneme, že je ***prvočinitel***, jestliže není invertibilní a platí $c \backslash (a \cdot b) \Rightarrow c \backslash a \vee c \backslash b$.

Řekneme, že c je ***nerozložitelný*** (ireducibilní), jestliže není invertibilní a platí $c = a \cdot b \Rightarrow c||a \vee c||b$.

Poznámka:
$a, b, c, d, e \in S$.

- Nechť d je $NSD(a, b)$ a e je $NSD(a \cdot c, b \cdot c) \Rightarrow d \cdot c || e$ (pokud oba dělitelé existují).
- Nechť 1 je $NSD(a, b)$ a nechť $a \backslash b \cdot c$. Pokud existuje $NSD(a \cdot c, b \cdot c) \Rightarrow a \backslash c$.

$S(\cdot, 1)$ je komutotivní monoid s krácením.

Poznámka:
Každý prvočinitel je ireducibilní. Pokud $\forall a, b \exists NSD(a, b) \Rightarrow$ každý ireducibilní prvek je prvočinitel.

Důkaz:
Nechť p je prvočinitel. $p = a \cdot b, a, b \in S$. $a \backslash p, b \backslash p$. $p \backslash a \cdot b \Rightarrow p \backslash a (p || a) \vee p \backslash b (p || b)$.

p ireducibilní. $p \backslash a \cdot b$, nechť $p \not\backslash a$. Existuje n je $NSD(p, a)$. $p = n \cdot x$, je ireducibilní, pak $p || n \vee p || x$. Dle předpokladu $p \not\backslash a$, tedy $p || x$. n je invertibilní, tedy 1.

Existuje největší společný dělitel $NSD(p \cdot b, a \cdot b)$. Tedy $p \backslash b$.

Věta:
Nechť každý ireducibilní prvek $S(\cdot, 1)$ je prvočinitelem. Nechť $p_1, \ldots, p_n$ a $q_1, \ldots, q_m \in S$ posloupnosti ireducibilních prvků, pro něž platí, že součuin $\prod_{i=1}^{n} p_i || \prod_{i=1}^{m} q_i$. Potom $n = m$ a existuje bijekce σ mezi posloupnostmi takové, že $p_i || q_{\sigma(i)}$.

Důkaz:
Indukcí dle n. $n = 1$ je zřejmý.

Je-li $R(+, \cdot, -, 0, 1)$ obor integrity, pak jeho NSD, ireducibilní prvky, prvočinitele, invertibilní prvky jsou definovány jako totéž na $R - \{0\}\,(\cdot, 1)$.

Obor integrity $R(+, \cdot, -, 0, 1)$, v němž jsou všechny ideály hlavní, tj. tvaru $aR = \{a \cdot r; r \in R\}$. Pak mu říkáme ***Obor integrity hlavních ideálů***.

Poznámka:
Je-li R obor integrity hlavních ideálů a $a_1, \ldots, a_n \in R$, pak existují $u_1, \ldots, u_n \in R$ takový, že $\sum_{i=1}^{n} a_i \cdot u_i$ je $NSD(a_1, \ldots, a_n)$.

Věta:
Nechť R je obor integrity hlavních ideálů. Každý ireducibilní prvek je prvočinitelem. Pro každý nenulový neinvertibilní prvek $a \in R$ existuje posloupnost ireducibilních prvků $p_1, \ldots, p_n$ takové, že $a = \Pi_{i=1}^{n}$. Jestliže $a = \Pi_{i=1}^{m} q_i$, pak $m = n$ a $\exists$ bijekce $\sigma; p_i || r_{\sigma(i)}$.

2 Okruhy polynomů

Mějme $R(+,\cdot,-,0,1)$ okruh, $M(\cdot,e)$ monoid. $R[M] = \{p : M \to R; |\{m \in M; p(m) \neq 0\}| < \infty\}$ – všechna zobrazení z monoidu do okruhu a jen konečně mnoho jich je nenulových.

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

Členy, kde $p(m) = 0$ můžeme vynechat.

Nulární prvek je $p(?) = 0$. Jednička $1(e) = 1, 1(? \neq e) = 0$.

$p, q \in R[M]$.

$$\begin{aligned} -p &= \sum_{m \in M} -p(m) \cdot m \\ p + q &= \sum_{m \in M} (p(m) + q(m)) \cdot m \\ p \cdot q &= \sum_{m \in M} \left(\sum_{\substack{a,b \in M \\ a \cdot b = m}} p(a) \cdot q(b) \right) \cdot m \end{aligned}$$

Poznámka:
Nechť $R(+,\cdot,-,0,1)$ a $M(\cdot,e)$ monoid.

- Množina $R[M](+,\cdot,-,0,1)$ je okruh, jsou-li R a M komutativní, je i $R[M]$ komutativní.
- Zobrazení $i : R \to R[M]$, kde $i(r) = r \cdot e$ je prostý okruhový homomorfizmus.
- Zobrazení $v : M \to R[M]$, kde $v(m) = 1 \cdot m$ je prostý monoidový homomorfizmus.

Důkaz:
$R[M](+,-,0)$ je komutativní grupa. Jde přímo z definice. Také $R[M](\cdot,1)$ musí být monoid. Násobení je podezřelé, je třeba dokázat korektnost – ty sumy musí být konečné, stačí vynechat nulové prvky. Nakonec distributivitu.

Obě zobrazení jsou zřejmě prostá, stačí ověřit homomorfizmy.

$R[M]$ nazýváme ***monoidový okruh***. Uvážíme-li monoid $\mathbb{N}_0(+,0)$, pak $R[\mathbb{N}_0]$ budeme nazývat okruhem ***polynomů jedné neurčité*** a budeme často psát $R[x]$.

Poznámka:
Nechť $S(+,\cdot,-,0,1)$ je okruh. R nějaký jeho podokruh, $\alpha \in S$. Potom zobrazení $\gamma\alpha : R[x] \to S$ daná přepisem

$$\gamma\alpha(\sum_{n\in\mathbb{N}_0} a_n \times x^n) = \sum_{n\in\mathbb{N}_0} a_n \cdot \alpha^n$$

je homomorfizmus. (Toto znamená dosazení)

Důkaz:
Přímočaré ověření slučitelností s $(+,-,0,\cdot,1)$. Buď $R(+,\cdot,-,0,1)$ okruh a $p \in R[x]$. Je-li $p \neq 0$, nazvu číslo $p^\circ := \max\{n; p(n) \neq 0\}$ ***stupeň polynomu*** p.

Stupeň $0^\circ = -1$.

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

1. $$p^\circ = (-p)^\circ$$
2. $$(p+q)^\circ \leq \max\{p^\circ, q^\circ\}$$
3. je-li $p,q \neq 0$, pak
$$(p\cdot q)^\circ \leq p^\circ + q^\circ$$
4. Jestliže R je obor integrity a p a q jsou nenulové.
$$(p\cdot q)^\circ = p^\circ + q^\circ$$
5. R je obor integrity $\Leftrightarrow R[x]$ je obor integrity.
6. p je invertibilní prvek a R je obor integrity $\Leftrightarrow p^\circ = 0 \wedge p(0)$ je invertibilní v R.

Důkaz:

1. Zřejmé.
2. Sčítáme po složkách, ze dvou nulových nikdy nemůže vyjít nenula.
3. Nechť jsou oba stupně nenulové a $n >$ součet stupňů. Je zřejmé, že koeficient vyjde nulový.

4. Je-li R obor integrity, pak nejvyšší koeficient je nenulový, je to jen jeden součin, který je nenulový (součin dvou nenulových).

5. Obě implikace. Když R je obor integrity, tak $p, q \neq 0$, součet jejich stupňů je větší než -1. Opačně. Vezmu všechny polynomy stupně 0, ty zobrazím na prvky R. Pokud jsou nenulové, jejich součin není 0 v polynomech, tedy ani v R.

6. Nechť p je invertibilní. Tedy $\exists q \in R[x]; p \cdot q = 1$. $1^\circ = 0, p, q \neq 0$, tedy stupně obou musí být 0. (Vynecháváme triviální případy, kdy $0 = 1$) Zbytek plyne z homomorfizmem všech polynumů stupně 0 s R.

   Na druhou stranu je zřejmé.

O dělení se zbytkem:
Buď $R(+, \cdot, -, 0, 1)$ obor integrity. $a, b \in R[x], b \neq 0$ a všechny b_n jsou invertibilní v R.

Potom existují polynomy $q, r \in R[x]$ atkové, že $a = q \cdot b + r \wedge r^\circ < b^\circ$.

Důkaz:
Pokud stupeň a je menší, než stupeň b, pak položím $q = 0$ a $r = a$. Ostatní indukcí postupným dělením.

Buď $R(+, \cdot, -, 0, 1)$ obor integrity a necť existuje $\mu : R \to \mathbb{N} \cup \{0, -1\}$ tak, že platí $\forall a, b \in R, b \neq 0$:

1.
$$a|b : \mu(a) \leq \mu(b)$$

2.
$$\exists q, r : a = q \cdot b + r; \mu(r) < \mu(b)$$

Pak R nazvu ***euklidovským oborem integrity*** a funkce μ je ***euklidovská funkce***.

Poznámka:
Každý euklidovský obor integrity je obor integrity hlavních ideálů.

Důkaz:
Buď $R(+, \cdot, -, 0, 1)$ euklidovský obor integrity a μ je příslušná euklidovská funkce. $I = \{0\} : I = 0R$. Když I je nenulový, tak si vezmu nejmenší takové I.

Euklidův algoritmus:
Nechť $R(+, \cdot, -, 0, 1)$ je Euklidův obor integrity s euklidovskou normou μ a $a_0, a_1 \neq 0$.

Definujme posloupnost $\{a_i\}$ a $\{q_i\}$. Jestliže $a_i \not| a_{i-1}$, pak vezmu q_i a a_{i+1} : $a_{i-1} = a_i \cdot q_i + a_{i+1}$, kde $\mu(a_{i+1}) < \mu(a_i)$.

Jestliže $a_i | a_{i-1}$, posléze $n = a_i$ a proces končí.

Důkaz:
Proces končí po konečně mnoha krocích a a_n je $NSD(a_0, a_1)$.

Definujme dvojici posloupností $\{x_i\}$ a $\{y_i\}$, $x_0 = y_1 = 1, x_1 = y_0 = 0$, $x_{i+1} = x_{i-1} - x_i, y_{i+1} = y_{i-1} - y_i \cdot q_i$. Potom $x_n \cdot a_0 + y_n \cdot a_1$ je $NSD(a_0, a_1)$.

Důkaz:
NSD existuje, neboť je to obor integrity hlavních ideálů.

$NSD(a_i, a_i + 1)$ je $NSD(a_{i-1}, a_i)$.

Dále indukcí.

Buď S okruh, R podokruh S a $\alpha \in S$. Řekneme, že α je ***kořenem polynomu*** $p \in R[x]$, jestliže $j\alpha(P) = 0$.

Kořenovým činitelem nazveme polynom $x - \alpha := (-\alpha \cdot x^0 + 1 \cdot x^1)$.

Řekneme, že polynom $p \in R[x]$ se ***rozkládá*** na kořenové činitele, jestliže $\exists a, \alpha_1, \ldots \alpha_n \in R$ a platí, že $p = a \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - a_n)$.

Poznámka:
α je kořenem polynomu $p \Leftrightarrow (x - \alpha) | p$.

Buď $R(+, \cdot, -, 0, 1)$ komutativní okruh, $\sum_{n \in \mathbb{N}_0} p_n x^n \in R[x]$. Definujme ***formální derivaci***:

$$(') : R[x] \to R[x]$$
$$(\sum p_n x^n)' := \sum (n+1) p_{n+1} x^n$$

Řekneme, že $\alpha \in R$ je ***vícenásobný kořen*** polynomu p, jestliže $(x - \alpha)^2 | p$.

Poznámka:
Buď R komutativní okruh a $p, q \in R[x]$ a $c \in R$. Pak platí:

- $(p + q)' = p' + q'$
- $(c \cdot p)' = c \cdot p'$
- $(p \cdot q)' = p' \cdot q + p \cdot q'$

Důkaz:
Viz analýza.

Poznámka:
Buď p polynom nad R. α je vícenásobný kořen $p \Leftrightarrow \alpha$ je kořen p' i p.

Důsledek:
Nechť $R(+,\cdot,-,0,1)$ je obor integrity, $p \in R[x]$. Jestliže 1 je $NSD(p,p')$, potom p nemá vícenásobný kořen.

Důsledek:
Nechť $R(+,\cdot,-,0,1)$ je obor integrity, jehož charakteristika nedělí číslo $n \in \mathbb{N}$. Potom polynom $x^n - 1$ a $x^{n+1} - x$ nemají vícenásobný kořen.

(Nesmí to být triviální okruh.)

Důkaz:
Zkusí se zderivovat.

Věta:
Každá konečná podgrupa grupy $T - \{0\}(\cdot,^{-1},1)$ tělesa $T(+,\cdot,-,0,1)$ je cyklická.

Důkaz:
G buď nějaká konečná podgrupa této grupy. $n := |G|$.

(viz minulý semestr) $\forall k|n\exists!$ podgrupa K grupy $\mathbb{Z}_n$.

K je také cyklická, tedy izomorfní s $\mathbb{Z}_k$.

v $\mathbb{Z}_n\exists$ právě $\varphi(k)$ prvků, které generují.

$$\forall g \in G; \langle g \rangle / n$$

$\forall k/n$ označíme $t_n := |\{g \in G; |\langle g \rangle| = k\}|$.

TODO: ?

3 Pořadová a rozkladová tělesa

Mějme okruhy $R(+,\cdot,-,0,1)$ a $S(+,\cdot,-,0,1)$ a $f : R \to S$ jejich homomorfizmus. Definujme zobrazení $f_x : R[x] \to S[x]$ přepisem $f_x\left(\sum a_i x^i\right) = \sum f(a_i)\, x^i$.

Poznámka:
Buď R, S a T okruhy a $f : R \to S, g : S \to T$ okruhové homomorfizmy. Pak platí:

1. f_x je homomorfizmus okruhů $R[x]$ a $S[x]$.
2. $(g.f)_x = g_x.f_x$
3. f_x je izomorfizmus $\Leftrightarrow$ f je izomorfizmus.

4. Pokud napřed provedu zobrazení a pak dosadím je totéž, jako když dosadím a pak převedu.

Poznámka:
Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso a $u \in T$ je polynom stupně alespoň 1. Pak faktor $T[x]/uT[x]$ je komutativní těleso $\Leftrightarrow$ u je ireducibilní polynom.

Poznámka:
Buď $T(+,\cdot,-,0,1)$ těleso a $u \in T[x]$. Pak zobrazení $\mu : T \to T[x]/uT[x]$ dané předpisem $t = \left[tx^0\right]$ je prostý okruhový homomorfizmus.

Značení: $T(+,\cdot,-,0,1)$ komutativní těleso, $u \in T[x]$ ireducibilní polynom. $T[x]/u \cdot T[x] = T[x]/\sim_u = (T[x])_u$. $a \sim_u b \equiv b - a \in T[x] \equiv u|b-a$.

$T \to (T[x])_u$, $t \to t \cdot x^] + u \cdot T[x] = \left[t \cdot x^0\right]_{\sim_u}$.

Věta:
Nechť T je komutativní těleso, $u \in T[y], u = \sum a_i y^i$ je ireducibilní, potom má polynom $\sum a_i x^i \in T[x]$ má kořen v tělese $(T[y])_u$.

Důkaz:
$1 \cdot y^1 + u \cdot T[y]$ je kořen polynomu. Dokáže se rozepsáním a dosazením.

Nechť $U(+,\cdot,-,0,1)$ je komutativní těleso. Řekneme, že $T \subseteq U$ je ***podtěleso***, je-li to podokruh $U(+,\cdot,-,0,1)$ a $T - \{0\}$ je podgrupa $U - \{0\}$ $(\cdot,^{-1},1)$. Naopak, U je ***nadtěleso*** T.

Důsledek:
Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso a $a \in T[x]$ stupně alespoň 1.

- $\exists U$ nadtěleso U, nad nímž má u kořen.
- $\exists V$ nadtěleso T, nad nímž se u rozkládá na kořenové činitele, tedy mohu ho napsat jako součin polynomů stupně 1.

Důkaz:
$T[x]$ je obor integrity hlavních ideálů. Vezmu libovolný ireducibilní polynom (dle nějakého tvrzení existuje) na něj pustím předchozí větu.

Druhou část vezmeme indukcí podle stupně u. Najdeme kořen (nad U) a vydělíme, oba polynomy jsou z U, v má o 1 menší stupeň. Rozšíříme pro $U \subseteq V$, takže můžeme pokračovat.

Poznámka:
Všechna komutativní podtělesa libovolného komutativního tělesa tvoří uzávěrový systém. Což znamená, že je to úplný svaz a průsek je průnik, tedy průnik dvou podtěles je opět podtěleso.

Důkaz:
Podokruhy tvoří uzávěrový systém. Stejně tak i podgrupy.

Následně uvažujme tělesa $U(+,\cdot,-,0,1)$ a jeho podtěleso $T \subseteq U$, případně $V \supseteq U$ je nadtěleso U.

Nechť $S \subseteq U$ těleso. $T[S]$ bude nejmenší podokruh obsahující množinu $T \cup S$. Obdobně $T(S)$ je nejmenší podtěleso obsahující $T \cup S$.

Jestliže $S = \{\alpha_1, \ldots, \alpha_n\}$, pak $T[\alpha_1, \ldots, \alpha_n] := T[S], T(\alpha_1, \ldots, \alpha_n) := T(S)$.

Poznámka:
$T \subseteq U$ podtěleso. $\alpha \in U$. Potom $T[\alpha] = \{p(\alpha) | p \in T[x]\}$ – dosadím α do všech polynomů. $T[S] \subseteq T(S)$.

Důkaz:
Podtěleso – podokruh je zřejmý z definice.

To první je okruhový homomorfizmus. Homomorfní zobrazení podalgebry je zase podalgebry.

$T \subseteq U, p \in T[x]$. U je ***kořenové (rozkladové) nadtěleso*** polynomu p, existuje-li kořen $\alpha \in U$ (kořeny $\alpha_1, \ldots, \alpha_n$)tak, že $p = a \cdot (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$ a pro žádné menší U to neplatí.

Věta:

- $\exists$ kartézké nadtěleso p nad T.
- $\exists$ rozkaldové nadtěleso p nad T.

Důkaz:
Najít nějaké těleso, nad kterým to lze rozložit, je možné. Pak vezmeme nejmenší podtěleso obsahující všechny kořeny.

$T \subseteq U, \alpha \in U$. Řekneme, že α je ***algebraický nad*** T, existuje-li polynom $p \in T[x]$ tak, že $p(\alpha) = 0$. V opačném případě nazveme α ***transcendentní***.

Buď $m \in T[x], m^\circ \geq 0$. Řekneme, že m je ***monický***, jestliže $a_{m^\circ} = 1$.

Věta:
$T \subseteq U, \alpha \in U$ je algebraický nad T. Potom $\exists!$ monický polynom $m \in T[x]$ takový, že $\forall p \in T[x] - \{0\}; p(\alpha) = 0 \Leftrightarrow m/p$.

Nechť m je ireducibilní. Potom $T[\alpha] = T(\alpha)$ a $(T[x])_m \cong T(\alpha)$.

Důkaz:
Vezmu všechny polynomy I, kterých je α kořenem. I je uzavřené na součty,

rozdíly, nulu obsahuje, je to tedy podgrupa. Stejně tak je uzavřené na součiny, tedy je ideálem. Je neprázdný, protože α je algebraický.

$T[x]$ je obor integrity hlavních ideálů, $\exists m; m \cdot T[x] = I$, existuje právě jeden monický (všechny generátory jsou asociovány).

Pokud je m ireducibilní, pak pokud $m = a \cdot b$, pak $m|a \vee m|b$.

Dosazení je homomorfizmus okruhů.

Poznámka:
Nechť $T_1 \subseteq U_1, T_2 \subseteq U_2$ jsou tělesa, $\alpha \in U_1, \beta \in U_2$ algebraické prvky nad T_1, T_2. $f : T_1 \to T_2$ je izomorfizmus.

Potom $\exists$ také izomorfizmus $g : T_1(\alpha) \to T_2(\beta)$, že $\forall t \in T_1, f(t) = g(t)$ a $g(\alpha) = \beta \Leftrightarrow f_x(m_\alpha) = m_\beta$.

Důkaz:
$f_x : T_1[x] \to T_2[x]$ je také izomorfizmus. $f_x(m_\alpha)$ je ireducibilní, protože m_α je ireducibilní (minimální polynom). $f_x(m_\alpha)$ je monický ($g : T_1(\alpha) \to T_2(\beta)$). $f = g$ na T_1. $g(0) = 0$, β je kořenem $f_x(m_\alpha), m_\beta | f_x(m_\alpha)$.

Je ireducibilní, tedy jsou asociované.

A zpátky:

$$T_1(\alpha) = T_1[x] \cong T[x] / m_\alpha T[x]$$
$$p(\alpha) \Leftrightarrow p + mT[x]$$
$$T_1(a) \cong (T_1[x])_{m_\alpha} \cong (T_2[x])_{m_\beta} \cong T_2(\beta)$$
$$p(\alpha) \to p + m_\alpha T_1[x] \to f_x(p) \to m_\alpha T_2[x] \to j\beta(f_x(p))$$
To je izomorfizmus
$$tx^0 \in T_1[x]$$
$$g(t) = f(t)$$
$$f_x(tx^0) = f(t)x^0$$

Věta:
Nechť $T_1 \subseteq U_1, T_2 \subseteq U_2$ jsou komutativní tělesa, $p \in T_1[x], U_1$ buď rozkladové těleso polynomu p nad T_1 a U_2 rozkladové těleso $f_x(p)$ nad T_2, kde $f : T_1 \to T_2$ je izomorfizmus. Jsou-li $\alpha_1, \ldots, \alpha_n \in U_1, \beta_1, \ldots, \beta_m \in U_2$ všechny kořeny p, resp $f_x(p)$ (násobně), pak $n = m$ a existuje izomorfizmus $g : U_1 \to U_2$ takový, že $\exists \sigma$ permutace, $g \restriction T_1 = f$ a $\forall i \in 1..n; g(\alpha_i) = \beta_{\sigma_i}$.

Důkaz:
Indukcí dle n.

$n = 1$ je triviální, $p = ax - b$, $f_x(p) = f(a)x - f(b)$, oba stupně 1 a mají zjevně jeden kořen a $g = f$.

Předpoklad platí pro všechna tělesa a polynomy stupně až $n-1$. Mám polynom p stupně n. Vezmu $m_{\alpha_1} \in T_1[x]$, ten dělí p, tedy $f_x(m_{\alpha_1})$ dělí $f_x(p)$. $f_x(p)$ je nad U_2 rozložitelný na dva polynomy, protože v $U_2[x]$ máme jednoznačný rozklad na ireducibilní prvky. Tedy v rozkladu $f_x(m_{\alpha_1})$, tak se v rozkladu se mohou vyskytovat pouze $\beta_1, \ldots, \beta_n$ (až na asociovanost). BÚNO β_1 je kořenem monický ireducibilního (nad $T_2[x]$) polynomu $f_x(m_{\alpha_1})$. Dle minulého tvrzení $\exists h : T_1(\alpha_1) \to T_2(\beta_1)$ izomorfizmus. $p = (x-\alpha_1)\cdot u$, stupeň $u < n$, použiji indukční předpoklad.

$\exists g : U_1 \to U_2, g \restriction T_1(\alpha_1) = h, g(\alpha_i) = \beta_{\sigma_i}$.

Nechť $T(+,\cdot,-,0,1)$ je komutativní těleso. Řekneme, že T je ***algebraicky uzavřené***, jestliže každý neinvertibilní polynom $p \in T[x]$ má v T kořen. (Ekvivalentní, že ho lze rozložit)

Nechť U je nadtěleso tělesa T. Nazvu jej ***algebraickým uzávěrem***, jestliže je algebraicky uzavřené a žádné $V, T \subseteq V \subseteq U$, pro které to platí, $U = V$.

Věta:
Každé těleso má algebraický uzávěr.

Důkaz:
Potřebuji axiom výběru (pro transfinitní indukci). T je komutativní těleso. Konstruujeme posloupnost nadtěles $T_1 \subseteq T_2 \subseteq T_3 \ldots$ takových, že všechny polynomy z $T_i[x]$ stupně nejvýše i jsou rozložitelné v $T_{i+1}[x]$.

Nechť $T_1 = T$. Dále vyrábíme těleso o jedna větší. Vezmu si všechny polynomy nad T_1. Seřadím si je (pomocí nějakého ordinálu a axiomu výběru). $T_{i,\alpha}$ je rozkladové nadtěleso polynomu p_α. Tyto pak sjednotím.

$U = \bigcup_{i\in\mathbb{N}} T_i$. Nyní je třeba dokázat, že je algebraicky uzavřené. Vezmu si polynom, ten má nějaké koeficienty z některého tělesa T_i. Proto je rozložitelný v T_{i+1}, který ve sjednocení je.

4 Konečná komutativní tělesa

Poznámka:
Žádné konečné komutativní těleso není algebraicky uzavřené.

Důkaz:
Vezmeme polynom $p = \prod_{t\in T}(x-t)+1$, v libovolném bodě je roven 1.

Poznámka:
Algebraický uzávěr konečného komutativního tělesa je (nekonečný) spočetný.

Důkaz:
Konstrukce viz minulou kapitolu. Každé těleso je větší, ale konečné, takže

celkem dají spočetné číslo.

Poznámka:
Nechť T je komutativní těleso prvočíselné charakteristiky a $n \in \mathbb{N}$. Pak $Q = \left\{t \in T | t^{p^n} = t\right\}$ je podtěleso T.

Důkaz:
$\varphi_p : T \to T, \varphi_p(t) = t^p$ je okruhový homomorfizmus. Složením n kopií tohoto homomorfizmu je opět homomorfizmus.

Stačí dokázat, že obsahuje $0, 1$ a z homomorfizmu uzavřenost operací.

Poznámka:

$$P = \{k \times 1 | k \in \mathbb{N}\} \subseteq T$$

Potom P podtěleso T izomorfní s $\mathbb{Z}_p$ pro nějaké prvočíselné p a $|T| = |P|^n = p^n$.

Důkaz:
$\varphi : \mathbb{Z} \to T$ je okruhový homomorfizmus.

Věta:
$q \in \mathbb{N}$, existuje konečné komutativní těleso T o q prvcích $\Leftrightarrow \exists n \in \mathbb{N}$ a prvočíslo p, že $q = p^n$. Toto těleso je izomorfní rozkladovému nadtělesu polynomu $x^{p^n} - x$ nad tělesem $\mathbb{Z}_p$.

Důkaz:
Jedním směrem minulá poznámka.

Opačně: T buď rozkladové nadtěleso, $x^{p^n} - x$ nad Z_p. Dle předchozí poznámky je jeho charakteristika p. $Q = \left\{t \in T | t^{p^n} = t\right\}$, což jsou právě všechny kořeny polynomu $x^{p^n} - x$. $Z_p \subseteq Q = T$.

Důsledek:
V T existuje podtěleso o q prvcích $\Leftrightarrow q \backslash |T| \wedge (q-1) \backslash (|T| - 1)$. Takové podtěleso je určeno jednoznačně.

Poznámka:
Nechť $k, n \in \mathbb{N}$ a p je prvočíslo. Pak $k \backslash n \Leftrightarrow p^k - 1 \backslash p^n - 1$.

Poznámka:
Je-li u ireducibilní polynom stupně k nad T, pak $u \backslash x^{|T|^k} - x$.

10.11:
Nechť T konečné komutativní těleso, $d \in \mathbb{N}$, $u \in T[x]$ je ireducibilní polynom stupně $k \in \mathbb{N}$, $q = |T|$. Pak je následující ekvivalentní:

1. $x^{q^k} - x / x^{q^d} - x$ v $T[x]$

2. $u/x^{q^d} - x$ v $T[x]$
3. $q^k - 1/q^d - 1$ v $\mathbb{Z}$
4. k/d

Důkaz:
(3) $\Leftrightarrow$ (4) – $q = p^n$, p je prvočíslo, $n \in \mathbb{N}$. $q^k - 1 = p^{nk} - 1/p^{nd} - 1 = p^d - 1 \Leftrightarrow nk/kd \Leftrightarrow k/d$

(1) $\Rightarrow$ (2) – $u/x^{q^x} - x$ dle předchozí poznámky, $x^{q^k} - x/x^{q^d} - x \Rightarrow u/x^{q^d} - x$.

(2) $\Rightarrow$ (3) – U je těleso o $q^d = p^{n \cdot d}$ prvcích. $n/n \cdot d \Rightarrow \exists!$ (až na izomorfizmus) těleso $T \subseteq U, |T| = p^n$. Mohu ho ztotožnit s původním tělesem. $\forall \alpha \in U$ jsou kořenem $x^{q^d} - x = \prod_{\alpha \in U}(x - \alpha)$. $u/x^{q^d} - x$ v $T[x]$, u lze chápat $\in U[x]$.
`TODO:`

(3) $\Rightarrow$ (1) – $\exists$ tělesa $T \subseteq U \subseteq V$, $|T| = q, |U| = q^d, |V| = q^k$. $x^{q^d} - x = (x^{q^k} - x) \cdot r + w$, $w^\circ < q^k$.

Důsledek:
Každý polynom $x^{q^d} - x$ je nad konečným tělesem o q prvcích součinem právě všech monických ireducibilních polynomů stupně k pro $\forall k/d$.

Důkaz:
(2) $\Leftrightarrow$ (4) z minulé věty dokazuje, že jsou všechny dělitele.

Rozkladovým nadtělesem $x^{q^d} - x$ jsou všechny kořeny jednonásobné.

$f \in T[x]$, T je komutativní těleso. Řekneme, že f je ***bez čtverců***, jestliže g^2/f pro $g \in T[x] \Rightarrow g^\circ = 0$. Rozklad $f = \prod_{i \in \mathbb{N}} f_i^i$ nazveme ***bezčtvercový rozklad***, jestliže f_i jsou bezčtvercové polynomy.

Poznámka:
Každý polynom $f \in T[x]$, kde T je komutativní těleso, má bezčtvercový rozklad.

Poznámka:
Polynom $f \in T[x]$ je bez čtverců právě tehdy, když f, f' jsou nesoudělné.

10.16:
Nechť $f \in T[x]$ je bezčtvercový monický polynom, kde T je nějaké konečné těleso. $V = T[x]/f \cdot T[x]$ a $W = \left\{[u]_f \in V \,|\, [u]_f^{|T|} = [u]\right\}$.

V je vektorový prostor nad T, W je jeho podprostor. Je-li f součinem právě k ireducibilních polynomů. Je-li $[u]_f \in W, 1 \in u^\circ < f^\circ$, pak $f = \Pi_{t \in T} nsd(u - s, f)$. Jsou-li $[u_1]_f, \ldots, [u_k]_f$ báze W a f_1, f_2 dva neasociované ireducibilní faktory f, $(f_1, f_2|f)$, pak $\exists i \leq k$ a $t \in T : f_1|w_i - t, f_2 \not| (w_i - t)$.

5 Booleovy algebry

Nechť $S(\wedge, \vee)$ je svaz. Řekneme, že je ***distributivní***, platí-li $\forall a, b, c \in S; a \vee (b \wedge c) = (a \vee b) \wedge (a \vee b)$.

Poznámka:
Je-li $S(\wedge, \vee)$ distributivní svaz $\Leftrightarrow$ i druhá distributivita $(\forall a, b, c; a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c))$.

Důkaz:
Stačí jedna implikace, pro druhé stačí vzít opačný svaz.

Nechť je tedy svaz distributivní.

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

Poznámka:
Každý distributivní svaz je modulární.

Nechť $S(\wedge, \vee)$ je svaz, 0 jeho nejmenší, 1 jeho největší prvek. Pak řekneme, že $a' \in S$ je ***doplněk (komplement)*** prvku a, jestliže $a \wedge a' = 0, a \vee a' = 1$.

Poznámka:
V distributivním svazu existuje pro každý prvek nejvýše jeden komplement.

$S(\vee, \wedge, 0, 1, ')$ nazveme Booleovou algebrou, je-li $S(\wedge, \vee)$ distributivní svaz, 0 je nejmenší prvek, 1 je největší prvek a $' : S \to S$ komplement.

Poznámka:
Je-li $S(\vee, \wedge, 0, 1, ')$ Booleova algebra, pak $\forall a, b \in S$ platí:

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

11.5:
Nechť $S(\vee, \wedge, 0, 1, ')$ je konečná Booleova algebra, A buď množina všech atomů $S(\wedge, \vee)$. Potom $a \in A \equiv a \neq 0, b \leq a, b \neq 0 \Rightarrow b = a$.

Okruhu $R(+, \cdot, -, 0, 1)$ budeme říkat ***Booleův okruh***, jestliže je komutativní, je charakteristiky 2 $(r + r = 0)$ a $r \cdot r = r$.

Poznámka:
Nechť $S(\vee, \wedge, 0, 1, ')$ je Booleova algebra. Definujeme-li operaci $+ : a + b = (a \wedge b') \vee (a' \wedge b)$, pak $S(+, \wedge, Id_S, 0, 1)$ je Booleův okruh. Navíc kongruence obou algeber splývají.

Vezmeme-li $S(+,\cdot,-,0,1)$ Booleův okruh. Definujeme operaci $\vee : a \vee b = a+b+a\cdot b$ a operaci $' : a' = 1+a$. Potom $S(\vee,\cdot,0,1,')$ je Booleova algebra. Navíc kongruence obou algeber splývají.