11. Existence kořenových a rozkladových nadtěles

V této kapitole bude T označovat komutativní těleso a $p \in T[x]$ bude nějaký polynom stupně $n \geq 1$. Označme I hlavní ideál generovaný polynomem p, tj. $I = pT[x] = \{ap;\ a \in T[x]\}$ je množina všech násobků polynomu p, čili množina všech polynomů dělitelných polynomem p.

V kapitole 10 jsme si již všimli, že s každým nenulovým polynomem je asociován právě jeden monický polynom (polynomy jsou totiž asociovány, liší-li se jen o násobek invertibilního prvku, přičemž invertibilní prvky z $T[x]$ jsou právě všechny nenulové prvky tělesa T). Asociované polynomy generují shodné hlavní ideály, takže při vyšetřování struktury konkrétního kvocientního okruhu $T[x]/I$ můžeme vždy zvolit polynom p monický.

Ukážeme, že ke kvocientnímu okruhu $T[x]/I = T[x]/pT[x]$ lze přistupovat podobně jako ke kvocientnímu okruhu $\mathbb{Z}/n\mathbb{Z}$.

Jsou-li $a, b \in T[x]$, tak $a \equiv b \bmod I$ znamená, že je $a - b \in I$, tedy že p dělí $a - b$. Proto je přirozené vedle $a \equiv b \bmod I$ psát také $a \equiv b \bmod p$.

11.1 Lemma. *Množina* $\{a \in T[x];\ \operatorname{st} a < n\}$ *je transversálou kongruence* $\bmod p$.

Důkaz. Je-li $b = pq + r$, kde $b, q, r \in T[x]$ jsou polynomy, platí $b \equiv r \bmod p$. Proto každý polynom $b \in T[x]$ je modulo p kongruentní s nějakým polynomem $r \in T[x]$, $\operatorname{st} r < n = \operatorname{st} p$.

Jsou-li a, b dva polynomy stupně menšího než $n = \operatorname{st} p$, tak je i $\operatorname{st}(a - b) < p$, a proto v takovém případě z $a \equiv b \bmod p$ plyne $a - b = 0$, a tedu $a = b$. $\square$

Zobrazení $a \mapsto a + I$ je tudíž bijekce mezi transversálou $\{a \in T[x];\ \operatorname{st} a < n\}$ a okruhem $T[x]/I$. Na $\{a \in T[x];\ \operatorname{st} a < n\}$ můžeme tudíž přenést strukturu okruhu $T[x]/I$. Takto vzniklý okruh budeme označovat $T[x]_p$. (Vztah $T[x]_p$ a $T[x]/pT[x]$ je tedy podobný jako vztah $\mathbb{Z}_n$ a $\mathbb{Z}/n\mathbb{Z}$. V obou případech jde o okruhy indukované transversálou ve smyslu definice v závěru 2. kapitoly.)

Pro $a, b \in T[x]_p$, kde $a = \sum_{0 \leq i < k} a_i x^i$ a $b = \sum_{0 \leq i < k} b_i x^i$ je $a + b$ rovno $\sum_{0 \leq i < k} (a_i + b_i) x^i$, čili sčítání v $T[x]_p$ se shoduje s běžným sčítáním v $T[x]$. (To plyne ze $\operatorname{st}(a + b) \leq \max\{\operatorname{st} a, \operatorname{st} b\}$.) Všimněte si, že zde je jistý rozdíl proti sčítání v $\mathbb{Z}_n$, neboť součty v $\mathbb{Z}_n$ se nemusí shodovat se součty v $\mathbb{Z}$.

Pro $a, b \in T[x]_p$ uvažme nyní jejich součin c v $T[x]$, tj. $c = \sum_k (\sum_{i+j=k} a_i b_j) x^k$. Hodnotou součinu ab v $T[x]_p$ je ten polynom stupně menšího než n, který je s c kongruentní modulo p, čili je to ten (jednoznačně určený) polynom r, že $ab = pq + r$, kde $\operatorname{st} r < n$. Podobně jako v $\mathbb{Z}_n$, je tedy i v $T[x]_p$ hodnota součinu rovna zbytku po dělení příslušným generátorem hlavního ideálu (v $\mathbb{Z}_n$ je jím n, v $T[x]_p$ je jím p).

Připomeňme nyní, že polynom p je ireducibilní, jestliže nelze vyjádřit jako součin dvou vlastních dělitelů, tedy jestliže pro žádná $a, b \in T[x]$ současně neplatí $p = ab$, $\operatorname{st} a < n$ a $\operatorname{st} b < n$. V kapitole 10 jsme ukázali, že $T[x]$ je eukleidovský obor integrity, tedy obor hlavních ideálů, a tedy Gaussův okruh. Proto je každý ireducibilní polynom prvočinitel, takže podle 10.12 je ideál $I = pT[x]$ maximální právě když je p ireducibilní. Připomeňme (viz 7.14), že $T[x]/I$ je těleso právě když I je v $T[x]$ maximální ideál. Dokázali jsme:

11.2 Tvrzení. *Okruh $T[x]_p$ je tělesem právě když p je ireducibilní polynom.*

Vzhledem k závažnosti tohoto tvrzení uvedeme i přímý důkaz:

Důkaz. Pokud p není ireducibilní, pak $p = a \cdot b$, kde $\operatorname{st} a < n$ a $\operatorname{st} b < n$. V $T[x]_p$ v takovém případě máme $a \neq 0 \neq b$, $ab = 0$, takže $T[x]_p$ není ani obor integrity, natož těleso. Je-li p ireducibilní a $0 \neq a \in T[x]_p$, tak polynomy a a p jsou v $T[x]$ nesoudělné. Proto podle 10.9 existují polynomy $u, v \in T[x]$ takové, že $ua + vp = 1$. To ale znamená $ua \equiv 1 \bmod p$, takže k a lze v $T[x]_p$ nalézt inverzní prvek. $\square$

Z důvodů, které brzy ozřejmíme, je někdy potřebné psát místo x nějaký jiný symbol, například y.

Snadno lze ukázat, že polynom $t = y^3 + y + 1$ je nad $\mathbb{Z}_2[y]$ ireducibilní. (Kdyby tomu tak nebylo, polynom t by musel mít vlastní dělitel stupně 1, a tím pádem by musel mít alespoň jeden kořen. Ovšem ani 0 ani 1 kořenem zjevně nejsou.) Sčítání v $\mathbb{Z}_2[y]_{y^3+y+1}$ nečiní obtíže, a pro násobení sestrojíme multiplikační tabulku:

$\cdot$	0	1	y	$y+1$	y^2	y^2+1	y^2+y	y^2+y+1
0	0	0	0	0	0	0	0	0
1	0	1	y	$y+1$	y^2	y^2+1	y^2+y	y^2+y+1
y	0	y	y^2	y^2+y	$y+1$	1	y^2+y+1	y^2+1
$y+1$	0	$y+1$	y^2+y	y^2+1	y^2+y+1	y^2	1	y
y^2	0	y^2	$y+1$	y^2+y+1	y^2+y	y	y^2+1	1
y^2+1	0	y^2+1	1	y^2	y	y^2+y+1	$y+1$	y^2+y
y^2+y	0	y^2+y	y^2+y+1	1	y^2+1	$y+1$	y	y^2
y^2+y+1	0	y^2+y+1	y^2+1	y	1	y^2+y	y^2	$y+1$

Podle předchozího je $\mathbb{Z}_2[y]_{y^3+y+1}$ těleso, takže jsme vlastně sestrojili těleso řádu 8. Zkonstruovali jsem tedy těleso neprvočíselného řádu. V této kapitole ukážeme, že pro každé $n \in \mathbb{N}$ a každé prvočíslo q existuje komutativní těleso řádu q^n. Později ještě ukážeme, že komutativní tělesa jiných řádů neexistují a že každá dvě komutativní tělesa shodného řádu jsou izomorfní. Platí také, že každé konečné těleso je komutativní; to však dokazovat nebudeme.

Předpokládejme nyní, že $p \in T[y]$ je ireducibilní polynom. Nad tělesem $T[y]_p$ můžeme opět uvažovat polynomy, tedy můžeme pracovat s okruhem $T[y]_p[x]$. Protože T je podtělesem tělesa $T[y]_p$ (prvky tělesa T totiž ztotožňujeme s polynomy stupně 0 a -1), platí $T[x] \subseteq T[y]_p[x]$.

Polynomem ze $\mathbb{Z}_2[y]_{y^3+y+1}[x]$ tedy například je $(y^2+1)x^6 + yx^5 + x^2 + (y^2+y+1)$, ale také $x^3 + x + 1$.

Máme-li spočítat hodnotu polynomu $a \in T[y]_p[x]$ v nějakém bodě $u \in T[y]_p$, můžeme postupovat tak, že pomocí vytvořené tabulky násobení postupně vyhodnotíme všechny mocniny u^i, kde $i \leq \operatorname{st} a$, a pak opět pomocí tabulky násobení spočítáme hodnotu $a_i u^i$ v $T[y]_p$, a nakonec provedeme součet.

Je-li $a = (y^2+1)x^6 + yx^5 + x^2 + (y^2+y+1) \in \mathbb{Z}_2[y]_{y^3+y+1}[x]$ a $u = y+1$, tak tímto způsobem zjistíme, že $u^2 = y^2 + 1$, $u^3 = y^2$, $u^4 = y^2 + y + 1$, $u^5 = y$, $u^6 = y^2 + y$, $(y^2 + 1)u^6 = y + 1$, a tedy $a(y + 1) = y + 1$, takže a se v bodě $y + 1$ chová jako identické zobrazení.

Pro výpočet $a(u)$, kde $a = \sum a_i x^i \in T[y]_p[x]$ a $u \in T[y]_p$ ovšem můžeme použít i jiný postup. Pokud koeficienty a_i chápeme jako prvky okruhu $T[y]$, tak namísto polynomu a můžeme uvažovat polynom $b = \sum a_i x^i \in T[y][x]$ (grafický zápis polynomů b a a je stejný, ale jsou to polynomy nad různými okruhy). Prvek

$u = \sum_{0\le i<n} u_i y^i \in T[y]_p$ můžeme chápat jako polynom $v = \sum u_i y^i \in T[y]$. Nyní $b(v)$ je prvek $T[y]$ a existuje jediný prvek $w \in T[y]$ takový, že je $w \equiv b(v) \bmod p$ a $\operatorname{st} w < n$.

11.3 Lemma. *Platí $w = a(u)$.*

Důkaz. Hodnota $b(v)$ je rovna součtu členů $a_i v^i$, kde $a_i v^i$ počítáme v $T[y]$. Hodnota $a(u)$ je rovna součtu členů $a_i u^i$, kde $a_i u^i$ počítáme v $T[y]_p$. Pokud na $a_i u^i \in T[y]_p$ pohlédneme jako na prvek $T[y]$, tak z definice $T[y]_p$ okamžitě vyplývá, že je $a_i u^i \equiv a_i v^i \bmod p$. To ale znamená i $\sum a_i u^i \equiv \sum a_i v^i \bmod p$, čili $a(u)$ je kongruentní s $b(w)$ modulo p, pokud $a(u) \in T[y]_p$ chápeme jako prvek $T[y]$. Je tedy $w \equiv a(u) \bmod p$ a platí $\operatorname{st} w < n$ a $\operatorname{st} a(u) < n$, čili nutně $w = a(u)$. $\square$

Použijeme-li předchozí lemma na polynom $a = (y^2{+}1)x^6 + yx^5 + x^2 + (y^2{+}y{+}1) \in \mathbb{Z}_2[y]_{y^3+y+1}[x]$, a na $u = y + 1$, tak obdržíme $b(v) = (y^2{+}1)(y{+}1)^6 + (y{+}1)^5 + (y{+}1)^2 + (y^2{+}y{+}1) = y^8 + y^6 + y^5 + y^4 + y^2 + 1 = (y^3{+}y{+}1)(y^5{+}y) + (y{+}1)$, takže vskutku platí $a(u) = y{+}1 \equiv b(v) \bmod y^3 + y + 1$.

Lemma 11.3 má jeden velmi významný důsledek:

11.4 Tvrzení. *Buďte T komutativní těleso a $a = \sum a_i x^i \in T[x]$ polynom ireducibilní nad T. Položme $p = \sum a_i y^i$ a uvažme těleso $T[y]_p \supseteq T$. Pak $a = \sum a_i x^i$ má v $T[y]_p[x]$ kořen y.*

Důkaz. Vyhodnotíme-li polynom $\sum a_i x^i$ v $T[y][x]$, dostaneme po dosazení y hodnotu $\sum a_i y^i = p$. Ovšem jistě je $p \equiv 0 \bmod p$, a proto je podle 11.3 hodnota polynomu $a \in T[y]_p[x]$ v bodě $y \in T[y]_p$ rovna 0. $\square$

Předchozí tvrzení tedy například říká, že polynom $x^3 + x + 1 \in \mathbb{Z}_2[y]_{y^3+y+1}[x]$ má v $\mathbb{Z}_2[y]_{y^3+y+1}$ kořen y. Pokud se o této skutečnosti chceme přesvědčit přímo z multiplikační tabulky tělesa $T[y]_p$, vidíme, že y^3 je rovno $y{+}1$, takže je $y^3 + y + 1 = (y{+}1) + y + 1 = 0$. Mohli bychom se také dále ptát (i když to v tuto chvíli není podstatné), zda se polynom $x^3{+}x{+}1$ rozkládá v $\mathbb{Z}_2[y]_{y^3+y+1}[x]$ na kořenové činitele. Tak tomu skutečně je, a platí $x^3 + x + 1 = (x - y)(x - y^2)(x - (y^2{+}y))$.

Každý polynom stupně alespoň 1 je součinem ireducibilních polynomů, a proto 11.4 okamžitě implikuje:

11.5 Důsledek. *Buď T komutativní těleso a $a \in T[x]$ polynom stupně alespoň 1. Potom existuje komutativní těleso $U \supseteq T$ takové, že a má v U alespoň jeden kořen.*

Nemalá péče, kterou jsme věnovali důkazu 11.5, byla motivována snahou po předložení snadno pochopitelného postupu, který by využíval analogií s počítáním dle celočíselných modulů. Existují samozřejmě daleko kratší důkazy, které nevyžadují definici tělesa $T[y]_p$. Například následujícím důkazem 11.5 by bylo možno nahradit celou předcházející část této kapitoly.

Důkaz. Protože a je součinem polynomů ireducibilních v $T[x]$, lze předpokládat, že a je ireducibilní. Pak $I = aT[x]$ je maximální ideál a $U = T[x]/I$ je těleso. Zobrazení $t \mapsto t + I$ je homomorfismus těles $T \to U$, takže při ztotožnění t a $t + I$ můžeme T chápat jako podtěleso U. Pak máme $T[x] \subseteq U[x]$, a dosadíme-li do $a \in U[x]$ hodnotu $x + I$, dostaneme $a + I$. Ovšem a je prvek I, takže $a + I = I = \mathbf{0}_U$, a proto je $a(x + I) = \mathbf{0}_U$. $\square$

Buď U komutativní těleso a T jeho podtěleso. Pro $S \supseteq U$ se podtěleso generované $T \cup S$ značí $T(S)$. Je-li $S = \{\alpha_1, \dots, \alpha_k\}$, tak vedle $T(S)$ píšeme též $T(\alpha_1, \dots, \alpha_k)$.

Je-li $a \in T[x]$ a $\alpha \in U$ je kořenem polynomu a, tak se těleso $T(\alpha)$ nazývá *kořenové nadtěleso* polynomu a. Jestliže se polynom $a \in T[x]$ v $U[x]$ rozkládá na kořenové činitele a $\alpha_1, \dots, \alpha_k$ jsou všechny jeho kořeny, tak se těleso $T(\alpha_1, \dots, \alpha_k)$ nazývá *rozkladové nadtěleso* polynomu a.

Z 11.5 plyne, že ke každému polynomu $a \in T[x]$ lze sestrojit kořenové nadtěleso. Indukcí nyní snadno dokážeme existenci rozkladových nadtěles.

11.6 Tvrzení. *Buď T komutativní těleso a $a \in T[x]$ ať je polynom stupně alespoň 1. Pak existuje komutativní těleso $U \supseteq T$ takové, že a se v $U[x]$ rozkládá na kořenové činitele.*

Důkaz. Postupujme indukcí podle $n = \operatorname{st} a$. Je-li $n = 1$, stačí položit $U = T$. Ať je $n > 1$ a ať $V \supseteq T$ je kořenové nadtěleso polynomu a, přičemž $\alpha \in V$ je kořen a. Pak a je rovno $(x - \alpha)b$, kde $b \in V[x]$ je stupně $n - 1$. Podle indukčního předpokladu existuje komutativní těleso $U \supseteq V$, ve kterém se b (a tím pádem i a), rozkládá na kořenové činitele. $\square$

11.7 Tvrzení. *Buď p prvočíslo a $n \in \mathbb{N}$. Rozkladové nadtěleso polynomu $x^{p^n} - x \in \mathbb{Z}_p[x]$ má právě p^n prvků.*

Důkaz. Ať U je nějaké rozkladové nadtěleso polynomu $x^{p^n} - x$. Z $U \supseteq \mathbb{Z}_p$ plyne, že charakteristika U je rovna p. Ať M označuje množinu všech kořenů polynomu $x^{p^n} - x$. Protože p nedělí $p^n - 1$, plyne z 10.16, že $x^{p^n} - x$ má vesměs různé kořeny, takže M má p^n prvků. Přitom $a \in U$ leží v M tehdy, je-li $a^{p^n} = a$. Ze 7.22 vyplývá, že M je těleso, takže M obsahuje i prvotěleso $\mathbb{Z}_p$. Ovšem U má být nejmenší těleso, které obsahuje $\mathbb{Z}_p$ a M, a proto musí být rovno M. $\square$

11.8 Tvrzení. *Ať U je nějaké komutativní těleso řádu p^n, kde p je prvočíslo a $n \in \mathbb{N}$. Ať $P \simeq \mathbb{Z}_p$ je prvotěleso tělesa U. Pak U je rozkladovým nadtělesem polynomu $x^{p^n} - x \in P[x]$.*

Důkaz. Řád grupy U^* je $p^n - 1$, takže $a^{p^n - 1} = 1$ platí pro každé nenulové $a \in U$. To znamená, že každé $a \in U$ splňuje $a^{p^n} = a$, a tedy U je tvořeno právě všemi kořeny polynomu $x^{p^n} - x$. $\square$

V následujících kapitolách dokážeme, že

(1) každé konečné komutativní těleso charakteristiky p musí mít řád p^n, kde $n \in \mathbb{N}$, a že
(2) dvě rozkladová tělesa nad týmž polynomem jsou vždy izomorfní.

Z 11.7 a 11.8 tudíž poté vyplyne, že konečné komutativní těleso řádu m existuje právě když $m = p^n$ je mocnina prvočísla, a že libovolná dvě komutativní tělesa stejného konečného řádu jsou navzájem izomorfní.