Matematický ústav Slezské univerzity v Opavě
Učební texty k přednášce ALGEBRA II, letní semestr 2000/2001
Michal Marvan

15. Polynomy

Polynom jedné neurčité x nad polem P je výraz tvaru

$$a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0, \tag{$*$}$$

kde $m \in \mathbf{N}$ a $a_0, \dots, a_m$ jsou prvky pole P. Prvek $a_i \in P$ se nazývá *i-tý koeficient*. Koeficient a_0 se nazývá *absolutní člen*.

Nulové koeficienty v zápisu $(*)$ obvykle neuvádíme; neuvedené koeficienty a_i prostě považujeme je za nulové. Tak například ze zápisu $(*)$ usuzujeme, že $a_{m+1} = 0$, $a_{m+2} = 0$, atd. Polynom, jehož všechny koeficienty a_i jsou nulové, se nazývá *nulový polynom* a značí se 0.

Dva polynomy $f = a_m x^m + \cdots + a_1 x + a_0$, $g = b_n x^n + \cdots + b_1 x + b_0$ považujeme za sobě rovné, jestliže se rovnají jejich koeficienty. Tedy, $f = g \Leftrightarrow a_0 = b_0, a_1 = b_1, \dots$

Stupeň polynomu $f = a_m x^m + \cdots + a_1 x + a_0$ je největší číslo r takové že $a_r \ne 0$. Značí se $\deg f$. Tudíž,

$$\deg f = r \;\Leftrightarrow\; a_r \ne 0,\; a_{r+1} = 0,\; a_{r+2} = 0, \dots .$$

Koeficient a_r se pak nazývá *vedoucí koeficient*. Zapisujeme $a_r = \operatorname{lc} f$.

Podle definice nulový polynom *nemá* ani stupeň ani vedoucí koeficient.

Nulový polynom a polynomy stupně 0 se nazývají *konstantní*; konstantní polynom a_0 můžeme ztotožnit s odpovídajícím prvkem $a_0 \in P$. Polynomy stupně 1 se nazývají *lineární*. Polynomy stupně 2 se nazývají *kvadratické*. Polynomy stupně 3 se nazývají *kubické*. Polynomy stupně 4 se nazývají *bikvadratické*.

Množina všech polynomů neurčité x nad polem P se značí $P[x]$. Algebraické operace s polynomy se zavedou následujícím způsobem:

Definice. Buďte $f = a_m x^m + \cdots + a_1 x + a_0$ a $g = b_n x^n + \cdots + b_1 x + b_0$ polynomy.

Součet polynomů f a g je polynom $f + g = c_p x^p + \cdots + c_1 x + c_0$, kde $p = \max\{m, n\}$ a $c_k = a_k + b_k$, $k = 0, \dots, p$. Polynom *opačný* k polynomu f je polynom $-f = -a_m x^m - \cdots - a_1 x - a_0$.

Součin polynomů f a g je polynom $fg = c_p x^p + \cdots + c_1 x + c_0$, kde $p = m + n$ a

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_{k-1} b_1 + a_k b_0 = \sum_{i+j=k} a_i b_j,$$

pro $k = 0, \dots, p$. V sumě se sčítá přes všechny dvojice indexů $i, j = 0, \dots, k$ takové, že $i + j = k$.

Tvrzení. *Součin nenulových polynomů f, g je nenulový polynom a platí*

$$\deg(fg) = \deg f + \deg g,$$

$$\operatorname{lc}(fg) = \operatorname{lc} f \cdot \operatorname{lc} g.$$

Důkaz. Nechť $\operatorname{lc} f = a_m \neq 0$, $\operatorname{lc} g = b_n \neq 0$, takže $\deg f = m$, $\deg g = n$. Pro $k > m + n$ máme $c_k = 0$ (zdůvodněte). Odtud nerovnost $\deg(fg) \leq m + n$. Dále $c_{m+n} = a_m b_n \neq 0$, a tudíž $fg \neq 0$, $\operatorname{lc}(fg) = c_{m+n} = \operatorname{lc} f \cdot \operatorname{lc} g$ a $\deg(fg) = m + n = \deg f + \deg g$.

Není těžké uhodnout, proč jsou algebraické operace s polynomy zavedeny způsobem právě uvedeným. Jde o souvislost s dosazováním konkrétních hodnot za neurčitou x. Je-li $f = a_m x^m + \cdots + a_1 x + a_0 \in P[x]$ nějaký polynom a $\xi \in P$ libovolný prvek, položíme

$$f(\xi) = a_m \xi^m + \cdots + a_1 \xi + a_0 \in P.$$

Tvrzení. *Pro libovolné polynomy $f, g \in P[x]$ a libovolný prvek $\xi in P$ platí*

$$(f + g)(\xi) = f(\xi) + g(\xi), \quad (-f)(\xi) = -f(\xi), \quad (fg)(\xi) = f(\xi)\, g(\xi).$$

Důkaz. Cvičení.

Definice. Prvek $\xi \in P$ se nazývá *kořen* polynomu $f \in P[x]$, jestliže $f(\xi) = 0$.

O kořeny nám půjde především, předtím však prozkoumáme algebraické vlastnosti polynomů.

Množina $P[x]$ se zavedenými operacemi splňuje všechny axiomy pole kromě existence inverzních prvků (nemusí existovat prvek a^{-1} takový, že $aa^{-1} = 1$ kdykoliv $a \neq 0$). Odpovídající algebraická struktura se nazývá okruh (plným jménem komutativní asociativní okruh s jedničkou, ale o jiných okruzích pojednávat nebudeme).

Definice. *Okruh* je množina, řekněme R, spolu s
a) binární operací $R \times R \to R$, $(a, b) \mapsto a + b$; nazývá se *sčítání*;
b) binární operací $R \times R \to R$, $(a, b) \mapsto a \cdot b$; nazývá se *násobení*;
c) dvěma vybranými prvky 0 a $1 \in R$; nazývají se *nula* a *jednička*;
d) zobrazením $R \to R$, $a \mapsto -a$; prvek $-a$ se nazývá *opačný* k prvku a;

Přitom je požadováno, aby pro libovolné prvky $a, b, c \in P$ platilo

(1) $a + b = b + a$,	(5) $a \cdot b = b \cdot a$,
(2) $a + (b + c) = (a + b) + c$,	(6) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
(3) $a + 0 = a$,	(7) $a \cdot 1 = a$,
(4) $a + (-a) = 0$,	(8) $a \cdot (b + c) = a \cdot b + a \cdot c$.

Tvrzení. *Množina $P[x]$ spolu se zavedenými algebraickými operacemi je okruh.*

Důkaz. Cvičení.

Příklady. Okruh **Z** celých čísel, různé okruhy spojitých a diferencovatelných funkcí.

Prvek okruhu mající inverzi se nazývá *invertibilní*. Množina všech invertibilních prvků okruhu R se značí R^*. Okruh je pole právě tehdy, když $R^* = R \setminus \{0\}$.

Okruh $P[x]$ však nikdy není polem, protože nekonstantní polynomy nikdy nemají inverzi:

Tvrzení. *Invertibilní prvky okruhu $P[x]$ jsou právě nenulové konstantní polynomy.*

Důkaz. Má-li f inverzi f^{-1}, pak $ff^{-1} = 1$. a proto jsou oba polynomy f, f^{-1} nenulové, načež $\deg f \le \deg f + \deg f^{-1} = \deg(ff^{-1}) = \deg 1 = 0$. Zbytek je zřejmý.

Po ztotožnění konstantních polynomů s odpovídajícími prvky pole P máme $P[x]^* = P \setminus \{0\} = P^*$.

Ačkoliv $P[x]$ není pole a nemůžeme po libosti dělit, lze alespoň krátit nenulovými prvky.

Tvrzení. *Nechť $f, g, h \in P[x]$.*
(1) *Nechť $fg = 0$. Pak $f = 0$ nebo $g = 0$.*
(2) *Nechť $fg = fh$ a $f \ne 0$. Pak $g = h$.*

Důkaz. (1) Je-li $f = 0$ nebo $g = 0$, není co dokazovat. Připusťme opak, tj. $f \ne 0$ a zároveň $g \ne 0$. Oba polynomy f, g pak mají vedoucí koeficienty, jejichž součin je nenulový a je vedoucím koeficientem součinu fg, načež $fg \ne 0$.
(2) Máme $f(g - h) = 0$. Při $f \ne 0$ pak podle (1) nutně $g - h = 0$.

Absence inverzních prvků znamená, že má smysl uvažovat o dělitelnosti polynomů. Teorie dělitelnosti polynomů je do značné míry podobná teorii dělitelnosti celých čísel.

Definice. Říkáme, že polynom $g \in P[x]$ *dělí* polynom $f \in P[x]$, jestliže existuje polynom $h \in P[x]$ takový, že $f = gh$. Zapisujeme $g \mid f$. Říkáme též, že g je *dělitel* polynomu f.

Příklad. Platí $x - 1 \mid x^2 - 1$, protože $x^2 - 1 = (x - 1)(x + 1)$.

Cvičení. 1. Ukažte, že $x - 1 \mid x^n - 1$ pro každé celé $n > 1$.
2. Ukažte, že relace $\mid$ je reflexivní a tranzitivní.
3. Nechť $f \ne 0$. Ukažte, že z $fg \mid fh$ plyne $g \mid h$.

Definice. Polynom $f \in P[x]$ se nazývá *normovaný*, je-li $f \ne 0$ a $\operatorname{lc} f = 1$.

Je-li $f = a_m x^m + a_{m-1}x^{m-1} + \cdots a_1 x + a_0$ libovolný nenulový polynom, $\operatorname{lc} f = a_m \ne 0$, pak je podíl $\bar f = f/\operatorname{lc} f = x^m + (a_{m-1}/a_m)x^{m-1} + \cdots (a_1/a_m)x + a_0/a_m$ vždy normovaný polynom. Polynomy f, $\bar f$ jsou z hlediska dělitelnosti rovnocenné (ověřte například vztahy $f \mid \bar f$ a $\bar f \mid f$). Mají také tytéž kořeny.

Lemma. *Buďte $f, g \in P[x]$ normované polynomy. Následující podmínky jsou ekvivalentní:*
(1) *$f \mid g$ a zároveň $g \mid f$;*
(2) *$f = g$.*

Důkaz. Nechť platí (1), takže $g = fp$ pro nějaké $p \in P[x]$ a současně $f = gq$ pro nějaké $q \in P[x]$. Když $f = 0$, pak $g = 0$ a (2) platí. Když $f \ne 0$, pak $f = gq = fpq$ a po zkrácení $1 = pq$, takže p je invertibilní, a tedy vlastně prvek z P^*. Potom $1 = \operatorname{lc} g = \operatorname{lc} fp = p$. Tudíž, $g = pf = f$. Opačná implikace je zřejmá.

Z lemmatu plyne, že relace dělitelnosti mezi normovanými polynomy je navíc antisymetrická. Máme proto uspořádanou množinu všech normovaných polynomů. Infimum v této uspořádané množině se nazývá největší společný dělitel.

Největší společný dělitel

Definice. Buďte $f, g \in P[x]$ polynomy. Normovaný polynom $d \in P[x]$ se nazývá *největší společný dělitel* polynomů f, g, jestliže platí:
(a) $d \mid f$ a $d \mid g$;
(b) kdykoliv $h \in P[x]$, $h \mid f$ a $h \mid g$, pak $h \mid d$.
Zapisujeme $d = D(f, g)$.

Podmínka (a) říká, že d je společný dělitel, podmínka (b) říká, že každý jiný společný dělitel h dělí d. Předpoklad normovanosti polynomu d zajišťuje, že největší společný dělitel je podmínkami (a), (b) určen jednoznačně:

Tvrzení. *Buďte $f, g \in P[x]$ dva polynomy. Pokud existuje jejich největší společný dělitel, pak je jediný.*

Důkaz. Buď d' jiný největší společný dělitel. Z definice snadno dostáváme, že $d \mid d'$ a $d' \mid d$ (cvičení). Potom $d = d'$, protože jsou oba normovány.

Definice. Polynomy $f, g \in P[x]$ takové, že $D(f, g) = 1$ se nazývají *nesoudělné*.

Příklad. Platí $D(x, x + 1) = 1$. Skutečně, polynom x je lineární a proto má jen lineární a konstantní dělitele. Lineární dělitelé jsou cx, kde $c \in P$, ale žádný z nich nedělí $x + 1$. Konstantní dělitelé jsou $c \in P \setminus \{0\}$, jejich normováním dostaneme 1.

V okruhu $P[x]$ největší společný dělitel skutečně existuje. Důkaz se vede podobně jako v okruhu $\mathbf{Z}$, máme totiž k dospozici neúplné dělení, zvané též dělení se zbytkem. Viz následující tvrzení, kde q se nazývá *neúplný podíl* a r se nazývá *zbytek*.

Tvrzení. *Buďte $f, g \in P[x]$ dva polynomy, nechť $g \neq 0$. Pak existují polynomy $q, r \in P[x]$ takové, že*
(i) $f = gq + r$;
(ii) $r = 0$ *nebo* $\deg r < \deg g$.

Lemma. *Nechť $f, g \in P[x]$ a nechť $\deg f \geq \deg g$. Pak existuje $q \in P[x]$ takové, že*

$$f - gq = 0 \ \ \textit{nebo} \ \ \deg(f - gq) < \deg f.$$

Důkaz lemmatu. Stačí položit $q = (\operatorname{lc} f / \operatorname{lc} g)\, x^{\deg f - \deg g}$. Pak $\deg gq = \deg f$ a též $\operatorname{lc} f = \operatorname{lc} gq$. V rozdílu $f - gq$ se pak vedoucí členy vzájemně zruší.

Důkaz tvrzení. Položme $q_0 = 0$ a $r_0 = f$. Pak $r := r_0$, $q := q_0$ vyhovují podmínce (i). Jestliže $r_0 = 0$ nebo $\deg r_0 < \deg g$, je vyhověno i podmínce (ii) a důkaz je hotov.

V opačném případě $\deg r_0 \geq \deg g$. Podle lemmatu existuje $q_1 \in P$ takové, že pro $r_1 = r_0 - gq_1$ máme $r_1 = 0$ nebo $\deg r_1 < \deg r_0$. Přitom $r := r_1$, $q := q_0 + q_1$ vyhovují podmínce (i): $gq + r = 0 + gq_1 + r_1 = r_0 = f$.

Analogicky, pokud jsou již nalezeny nějaké polynomy r_i, q_i splňující (i), pak je buď splněna i podmínka (ii) a důkaz je hotov, anebo $\deg r_i \geq \deg g$ a podle lemmatu existuje q_{i+1} takové, že pro $r_{i+1} = r_i - gq_{i+1}$ máme $r_{i+1} = 0$ nebo $\deg r_{i+1} < \deg r_i$. Přitom opět $r := r_{i+1}$ a $q := q_i + q_{i+1}$ vyhovují podmínce (i): $gq + r = gq_i + gq_{i+1} + r_{i+1} = gq_i + r_i = f$.

Podmínka (ii) pak bude v některém kroku jistě splněna. Pokud nenastane dříve případ $r_i = 0$, bude to tehdy, až klesající posloupnost $\cdots < \deg r_2 < \deg r_1 < \deg r_0 = \deg f$ dosáhne hodnoty nižší než $\deg g$.

Následující tvrzení dokazuje existenci největšího společného dělitele v případě nenulových polynomů.

Tvrzení. *Buďte $f, g \in P[x]$ dva nenulové polynomy. Pak existuje jejich největší společný dělitel d a polynomy $u, v \in P[x]$ takové, že*

$$d = fu + gv.$$

Důkaz. Označme $I = \{fu + gv \mid u, v \in P[x]\}$. V množině I jistě existuje nenulový prvek minimálního stupně. Vyberme jeden takový, normujme jej a označme d. Pak jistě $d = fu+gv$ pro nějaká $u, v \in P[x]$.

Ukažme nejprve, že $d \mid f$. Dělíme-li se zbytkem, obdržíme rovnost $f = dq + r$, kde $r = 0$ nebo $\deg r < \deg d$. V prvním případě $d \mid f$ a jsme hotovi. Druhá možnost však nemůže nastat, protože $r = f - dq = f - (fu + gv)q = f(1 - uq) - (gv)q \in I$, takže r by byl nenulový prvek v I stupně nižšího než $\deg d$. Analogicky $d \mid g$.

Buď dále $h \in P[x]$ společný dělitel polynomů f a g. Pak h zřejmě dělí i výraz $fu+gv = d$. Tím je důkaz je hotov.

Ačkoliv důkaz tvrzení podával jistý návod k nalezení d, u, v, byl to návod prakticky nepoužitelný. Prakticky použitelným postupem je Eukleidův algoritmus.

Eukleidův algoritmus. *Vstup: nenulové polynomy $f, g \in P[x]$.*

Sestavme posloupnost polynomů

$$r_0,\ r_1,\ r_2,\ r_3, \dots$$

kde $r_0 = f$, $r_1 = g$ a jsou-li známy členy r_i, r_{i+1}, pak člen r_{i+2} získáme neúplným dělením polynomu r_i polynomem r_{i+1}:

$$r_i = r_{i+1} q_i + r_{i+2}, \qquad r_{i+2} = 0 \ \textit{nebo} \ \deg r_{i+2} < \deg r_{i-1}.$$

pro všechna $i = 0, \dots, N - 2$.

Výstup: polynom $r_{N-1} \neq 0$ takový, že $r_N = 0$.

Tvrzení. *Rovnosti $r_N = 0$ je dosaženo po konečném počtu kroků a platí $r_{N-1} = D(f, g)$.*

Důkaz. Kdyby $r_i \neq 0$ pro všechna $i \in \mathbf{N}$, pak bychom měli nekonečnou klesající posloupnost nezáporných čísel $\deg g > \deg r_1 > \deg r_2 > \deg r_3 > \dots$, což není možné. Tudíž, N vždy existuje.

Položme $d = \bar{r}_{N-1}$ (normovaný zbytek) a ukažme, že $d \mid f$, $d \mid g$. Zřejmě máme $d \mid r_{N-1}$, $d \mid r_N$. Protože $r_i = r_{i+1} q_i + r_{i+2}$, plyne odtud indukcí, že $d \mid r_i$ pro všechna $i = N - 2$ až $i = 0$ (cvičení). Nakonec $d \mid r_1 = g$ a $d \mid r_0 = f$.

Buď dále $h \in P[x]$ takové, že $h \mid f = r_0$ a $h \mid g = r_1$. Protože $r_{i+2} = r_i - r_{i+1} q_i$, opět se indukcí ukáže, že $d \mid r_i$ pro $i = 0, \dots, N - 1$ (cvičení). Tudíž, $d = D(f, g)$.

Poznamenejme, že existuje rozšíření Eukleidova algoritmu, kterým lze získat i polynomy u, v:

Rozšířený Eukleidův algoritmus. *Vstup: nenulové polynomy* $f, g \in P[x]$.
Sestavme posloupnost polynomů

$$r_0 = f,\ r_1 = g,\ r_2,\ \dots,\ r_{N-1}$$

jako v obyčejném Eukleidově algoritmu. Sestavme dále posloupnosti

$$u_0 = 1,\ u_1 = 0,\ u_2,\ \dots,\ u_{N-1},$$

$$v_0 = 0,\ v_1 = 1,\ v_2,\ \dots,\ v_{N-1},$$

kde $u_i = u_{i+1}q_i + u_{i+2}$ *a* $v_i = v_{i+1}q_i + v_{i+2}$ *pro všechna* $i = 0, \dots, N-3$.
Výstup: polynomy $r_{N-1}, u_{N-1}, v_{N-1}$.

Tvrzení. $r_{N-1} = f u_{N-1} + g v_{N-1}$.

Důkaz. Cvičení. Indukcí se dokazují rovnosti $r_i = f u_i + g v_i$. Indukční krok používá platnost dokazovaného tvrzení pro $i-1$ a $i-2$.

Podobně jako přirozená čísla lze jednoznačně rozkládat na součin prvočísel, lze normované polynomy jednoznačně rozkládat na součin normovaných polynomů dále nerozložitelných.

Definice. *Reducibilní* polynom je nekonstantní polynom, který je součinem dvou (či více) nekonstantních polynomů. *Ireducibilní* polynom je nekonstantní polynom, který není reducibilní.

Cvičení. Ukažte, že normovaný reducibilní polynom lze rozložit tak, že oba činitelé jsou normováni. Návod: je-li $f = gh$, pak $\bar f = \bar g \bar h$.

Tvrzení. *Buď* $f \in P[x]$ *normovaný polynom. Pak existují normované ireducibilní polynomy* $g_1, \dots, g_n$ *takové, že* $f = g_1 \cdots g_n$.

Je-li $f = h_1 \cdots h_m$ *jiný rozklad na normované ireducibilní činitele, pak* $m = n$ *a po vhodném přečíslování platí* $h_i = g_i$ *pro všechna* $i = 1, \dots, n$. *(Přesněji, existuje bijekce* $\phi : \{1, \dots, n\} \to \{1, \dots, m\}$ *taková, že* $h_i = g_{\phi(i)}$ *pro všechna* i.*)*

Příklad. Polynom $x^2 - 1 = (x-1)(x+1)$ je reducibilní. Polynomy $x-1$ a $x+1$ jsou již ireducibilní, máme tedy rozklad na normované ireducibilní polynomy.

Tvrzení dokážeme, přitom použijeme několik pomocných tvrzení.

Cvičení. Nechť jsou $f, g \in P[x]$ normované polynomy, nechť je g ireducibilní. Jestliže $f \mid g$, pak $f = 1$ nebo $f = g$. Je-li f též ireducibilní, pak nutně $f = g$.

Lemma. *Buďte* $g, h_1, \dots, h_n$ *ireducibilní normované polynomy a nechť* $g \mid h_1 \cdots h_n$. *Pak existuje index* j *takový, že* $g = h_j$.

Důkaz lemmatu. Položme $d = D(g, h_1)$. Jelikož $d \mid g$ a g je ireducibilní, máme buď $d = g$ anebo $d = 1$ (zdůvodněte). V prvním případě $g = d \mid h_1$, načež $g = h_1$ (cvičení). Ve druhém případě

$$1 = gu + h_1 v$$

pro vhodné polynomy $u, v \in P[x]$. Násobíme-li na obou stranách součinem $h_2 \cdots h_m$, obdržíme

$$h_2 \cdots h_m \;=\; g h_2 \cdots h_m u \;+\; h_1 h_2 \cdots h_m v.$$

Podle předpokladu $g \mid h_1 h_2 \cdots h_m$, pravá strana je tedy dělitelná g, a proto i levá strana je dělitelná, to jest $g \mid h_2 \cdots h_m$. Stejným postupem pak ukážeme, že buď $g = h_2$ nebo $g \mid h_3 \cdots h_m$, což opakujeme tak dlouho, dokud nenarazíme na index j takový, že $g = h_j$.

Důkaz tvrzení. Existence rozkladu: Je-li polynom f ireducibilní, pak $n = 1$, $g_1 = f$ a jsme hotovi; je-li reducibilní, pak se dá rozložit na součin $f = f_1 f_2$ nekonstantních polynomů. Na každý z polynomů f_1, f_2 můžeme uplatnit stejný postup – opět jsou buď ireducibilní nebo se dají samy rozložit. Tak dojdeme k jistému seznamu součinitelů, který musí být konečný, protože počet nekonstantních součinitelů je shora omezen stupněm polynomu f.

Důkaz jednoznačnosti: Nechť $g_1 \cdots g_n = h_1 \cdots h_m$ a všichni součinitelé jsou ireducibilní a normováni. Zřejmě $g_1 \mid h_1 \cdots h_m$. Podle lemmatu existuje index $\phi(1)$ takový, že $g_1 = h_{\phi(1)}$. V rovnosti $g_1 \cdots g_n = h_1 \cdots h_m$ pak můžeme zkrátit g_1 proti $h_{\phi(1)}$. Dostaneme podobnou rovnost jako na počátku a stejným způsobem vyhledáme index $\phi(2)$ takový, že $g_2 = h_{\phi(2)}$, následovně index $\phi(3)$ takový, že $g_3 = h_{\phi(3)}$, atd. až $g_n = h_{\phi(n)}$. Takto vznikne zobrazení $\phi : \{1, \ldots, n\} \to \{1, \ldots, m\}$, podle způsobu své konstrukce injektivní (ověřte).

Nakonec nutně $n \le m$, protože jinak bychom dostali $g_{n-m} \mid 1$, což nemůže být je-li g_{n-m} nekonstantní. Opačnou nerovnost $m \le n$ získáme podobným postupem z rovnosti $h_1 \cdots h_m = g_1 \cdots g_n$. Tudíž $m = n$ a injektivní zobrazení ϕ je bijektivní.

Všimněme si, že reducibilita polynomů může záviset na volbě pole P.

Příklad. Polynom x^2+1 je reducibilní nad polem $\mathbf{C}$, protože $x^2+1 = (x+\mathrm{i})(x-\mathrm{i})$. Tentýž polynom je ireducibilní nad polem $\mathbf{R}$, protože jakýkoliv jeho hypotetický rozklad $x^2 + 1 = (x + \xi)(x + \eta)$, $\xi, \eta \in \mathbf{R}$ je současně rozkladem nad $\mathbf{C}$ různým od $x^2 + 1 = (x + \mathrm{i})(x - \mathrm{i})$, ve sporu s jednoznačností rozkladu.

Jako důsledek obdržíme jisté zobecnění shora uvedeného lemmatu.

Důsledek. *Buď $f \in P[x]$, buďte $g_1, \ldots, g_m \in P[x]$ ireducibilní, normované a po dvou různé, tj. $g_i \ne g_j$ pro $i \ne j$. Jestliže $g_1^{k_1} \mid f, \ldots, g_m^{k_m} \mid f$, pak $g_1^{k_1} \cdots g_m^{k_m} \mid f$.*

Ukažme si nyní souvislosti s kořeny polynomů.

Tvrzení. *Nechť $f \in P[x]$ a $\xi \in P$. Následující podmínky jsou ekvivalentní:*
(i) *ξ je kořen polynomu f;*
(ii) $(x - \xi) \mid f$.

Důkaz. Nechť platí (i). Dělme se zbytkem:

$$f = (x-\xi)\, q + r, \qquad r = 0 \ \text{ nebo } \ \deg r < \deg(x-\xi).$$

Je-li $r = 0$, pak máme (ii). Je-li $r \ne 0$, potom $\deg r < \deg(x - \xi) = 1$, takže r je konstanta a výpočet $0 = f(\xi) = (\xi - \xi)\, q(\xi) + r = r$ ukazuje, že případ $r \ne 0$ nenastane.

Naopak, předpokládejme (ii). Potom $f = (x - \xi)\,q$ pro nějaký polynom q, načež $f(\xi) = (\xi - \xi)\,q(\xi) = 0$.

Definice. Prvek $\xi \in P$ se nazývá *alespoň k-násobný kořen* polynomu $f \in P[x]$, jestliže platí $(x - \xi)^k \mid f$.

Prvek $\xi \in P$ se nazývá *k-násobný kořen* polynomu $f \in P[x]$, jestliže platí $(x - \xi)^k \mid f$, ale neplatí $(x - \xi)^{k+1} \mid f$.

Tvrzení. *Buďte $\xi_1, \dots, \xi_n \in P$ různé kořeny polynomu $f \in P[x]$ s násobnostmi po řadě $k_1, \dots, k_n$. Potom*

(1) $(x - \xi_1)^{k_1} \cdots (x - \xi_n)^{k_n} \mid f$;

(2) $k_1 + \cdots + k_n \leq \deg f$.

Důkaz. Cvičení.

Lineární polynomy $x - \xi$ jsou zřejmě vždy ireducibilní. Rozložení polynomu f na lineární ireducibilní činitele je rovnocenné nalezení všech jeho kořenů.

Nad polem $\mathbf{C}$ jsou všechny polynomy stupně > 1 reducibilní. To je důsledkem následující věty:

Základní věta algebry. *Každý nekonstantní polynom $f \in \mathbf{C}[x]$ má alespoň jeden kořen.*

Není znám žádný jednoduchý důkaz, vhodný pro tuto přednášku. Věta bude dokázána později v jiné přednášce.

Důsledek. *Každý nekonstantní polynom $f \in \mathbf{C}[x]$ má rozklad na lineární ireducibilní činitele. Kořenů má se započtením násobnosti právě tolik, kolik činí jeho stupeň.*

Vidíme, že úloha nalézt rozklad polynomu $f \in \mathbf{C}[x]$ na ireducibilní činitele je rovnocenná úloze nalézt všechny jeho kořeny. Kořeny polynomů stupně dva přitom můžeme spočítat pomocí známého vzorce pro řešení kvadratické rovnice. Existují postupy pro nalezení kořenů libovolného polynomu f stupně ≤ 4. Úloha se redukuje na posloupnost řešení pomocných rovnic tvaru $x^n = c$, tedy odmocňování; hovoříme o řešení v kvadraturách. Ukazuje se však, že pro obecný polynom stupně ≥ 5 řešení v kvadraturách neexistuje (H. Abel).

Násobnost kořenů

Hledání kořenů se může drasticky zjednodušit, má-li polynom násobné kořeny. Zaveďme zobrazení $\mathbf{C}[x] \longrightarrow \mathbf{C}[x]$, které polynomu $f = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in \mathbf{C}[x]$ přiřazuje polynom $f' = m a_m x^{m-1} + (m-1) a_{m-1} x^{m-2} + \cdots + a_1 \in \mathbf{C}[x]$. Polynom f' se nazývá *derivace* polynomu f.

Cvičení. Ukažte, že platí

(a) $(f + g)' = f' + g'$,

(b) $(fg)' = f'g + fg'$,

(c) $(f^k)' = k f^{k-1} f'$.

Tvrzení. *Buď $f \in \mathbf{C}[x]$ polynom. Nechť $\xi \in \mathbf{C}$ je jeho k-násobný kořen, $k \geq 2$. Potom*
(i) *ξ je $(k-1)$-násobný kořen derivace f';*
(ii) *ξ je $(k-1)$-násobný kořen největšího společného dělitele $D(f, f')$;*

Důkaz. Je-li ξ kořen polynomu f násobnosti k, pak $f = (x-\xi)^k q$.
(i) Derivujme:

$$f' = k(x-\xi)^{k-1}q + (x-\xi)^k q' = (x-\xi)^{k-1}\big(kq + (x-\xi)q'\big).$$

Vidíme, že ξ je kořen polynomu f' s násobností alespoň $k-1$. Kdyby ξ byl kořen násobnosti k, pak bychom měli $(x-\xi) \bigm| \big(kq + (x-\xi)q'\big)$, načež $(x-\xi) \mid kq$, a tedy $(x-\xi) \mid q$ a kořen ξ polynomu f by musel mít násobnost $k+1$.
(ii) Z definice největšího společného dělitele plyne, že $(x-\xi)^{k-1} \mid D(f, f')$. Nejde o kořen násobnosti k, protože z $(x-\xi)^k \mid D(f, f')$ by plynulo $(x-\xi)^k \mid f'$ ve sporu s (i).

Cvičení. Předchozí tvrzení platí i pro $k = 1$, interpretujeme-li rčení „ξ je 0-násobný kořen“ jako „ξ není kořen.“

Protože $D(f, f')$ dělí f, existuje podíl $f/D(f, f') \in \mathbf{C}[x]$.

Tvrzení. *Buď $f \in \mathbf{C}[x]$ polynom, buď ξ jeho kořen. Pak ξ je 1-násobný kořen podílu*

$$f/D(f, f').$$

Důkaz. Je-li ξ kořen násobnosti k, pak $f = (x-\xi)^k q$ a podle předchozího tvrzení $D(f, f') = (x-\xi)^{k-1}r$, kde $r = kq + (x-\xi)q'$. Potom

$$\frac{f}{D(f, f')} = (x-\xi)\frac{q}{r},$$

kde $x - \xi$ nedělí q, a proto nedělí ani q/r.

Důsledek. *Buď $f \in \mathbf{C}[x]$ polynom.*
(i) *Množina všech kořenů polynomu $f/D(f, f')$ je rovna množině všech kořenů polynomu f;*
(ii) *Všechny kořeny polynomu $f/D(f, f')$ jsou 1-násobné.*

Důkaz. Cvičení.

Je-li podezření, že polynom f má násobné kořeny, pak je nejsnáze určíme tak, že vypočteme polynom $f/D(f, f')$, jehož stupeň je roven počtu (různých) kořenů polynomu f. Nelze sice očekávat, že „náhodně“ zvolený polynom bude mít násobné kořeny, ale polynomy vyskytující se v praktických úlohách často násobné kořeny mají (v souvislosti se symetričností úlohy).

Polynomy s reálnými koeficienty

Na závěr se věnujme kořenům polynomů s reálnými koeficienty a ukažme, jak rozklad na ireducibilní činitele polynomu $f \in \mathbf{R}[x]$ nad polem $\mathbf{R}$ souvisí s jeho rozkladem nad polem $\mathbf{C}$.

Zaveďme zobrazení $\mathbf{C}[x] \longrightarrow \mathbf{C}[x]$, které polynomu $f \in \mathbf{C}[x]$ přiřazuje polynom f^*, jehož koeficienty jsou čísla komplexně sdružená ke koeficientům polynomu f. To jest, je-li $f = a_m x^m + \cdots + a_1 x + a_0$, pak $f^* = a_m^* x^m + \cdots + a_1^* x + a_0^*$.

Cvičení. Ukažte, že platí
(a) $(f+g)^* = f^* + g^*$,
(b) $(fg)^* = f^* g^*$.

Tvrzení. *Buď $f \in \mathbf{R}[x]$ polynom s reálnými koeficienty. Nechť $\xi \in \mathbf{C}$ je jeho kořen. Pak komplexně sdružené číslo ξ^* je též kořen, přičemž stejné násobnosti.*

Důkaz. Jestliže ξ je kořen násobnosti k, pak $f = (x-\xi)^k q$. Aplikujme komplexní sdružení na obou stranách. Protože f má reálné koeficienty, je

$$f = f^* = (x-\xi^*)^k q^*$$

(cvičení). Vidíme, že ξ^* je alespoň k-násobný kořen polynomu f. Kdyby ξ^* byl větší násobnosti, tj. alespoň $k+1$, pak by bylo $f = (x-\xi^*)^{k+1} r$, načež $f = f^* = (x-\xi)^{k+1} r^*$, a ξ by též musel mít násobnost $k+1$.

Rozklad polynomu $f \in \mathbf{R}[x]$ na ireducibilní činitele nad $\mathbf{C}$ pak obsahuje lineární ireducibilní činitele $x - \alpha_i$ odpovídající reálným kořenům α_i a dvojice lineárních ireducibilních činitelů $x - \xi_i$, $x - \xi_i^*$, odpovídající dvojicím komplexně sdružených kořenů ξ_i, ξ_i^*:

$$f = (x-\alpha_1)^{l_1} \cdots (x-\alpha_r)^{l_r} (x-\xi_1)^{k_1} (x-\xi_1^*)^{k_1} \cdots (x-\xi_s)^{k_s} (x-\xi_s^*)^{k_s}. \qquad (*)$$

Vidíme, že $\deg f = l_1 + \cdots + l_r + 2(k_1 + \cdots + k_s)$.

Cvičení. Ukažte, že každý polynom $f \in \mathbf{R}[x]$ lichého stupně má alespoň jeden reálný kořen.

Cvičení. Nechť $\xi \in \mathbf{C}$, $\xi \notin \mathbf{R}$. Ukažte, že $(x-\xi)(x-\xi^*) = x^2 - 2\operatorname{re}\xi + |\xi|^2$ je kvadratický polynom s reálnými koeficienty a záporným diskriminantem.
Návod: pište $\xi = \alpha + \beta\mathrm{i}$, kde $\alpha, \beta \in \mathbf{R}$.

Na základě posledního cvičení můžeme formuli $(*)$ přepsat jako

$$f = (x-\alpha_1)^{l_1} \cdots (x-\alpha_r)^{l_r} (x^2 - 2\operatorname{re}\xi_1 + |\xi_1|^2)^{k_1} \cdots (x^2 - 2\operatorname{re}\xi_s + |\xi_s|^2)^{k_s}.$$

Tento součin představuje rozklad polynomu f na ireducibilní činitele nad polem $\mathbf{R}$. Jak totiž víme, každý kvadratický polynom $q \in \mathbf{R}[x]$ se záporným diskriminantem je ireducibilní.

Cvičení. Ukažte, že reálné polynomy řádu > 2 jsou vždy reducibilní nad $\mathbf{R}$.

Cvičení. Rozložte polynom $x^4 + 1$ na ireducibilní činitele nad polem $\mathbf{C}$ a nad polem $\mathbf{R}$.