Kapitola II

POLYNOMY JEDNÉ PROMĚNNÉ

§1 : OKRUH POLYNOMŮ

Definice : *Nechť R je okruh; pak p o l y n o m e m (j e d n é p r o m ě n n é) n a d o k r u h e m R budeme nazývat každou nekonečnou posloupnost*

(1) $$f = (a_0, a_1, a_2, \dots)$$

kde $a_i \in R$, $i = 0, 1, 2, \dots$, při čemž od jistého indexu n počínaje jsou všechny prvky a_k rovny nule okruhu R, t.j. $a_k = O_R$ pro $k \geq n$.

Prvky a_0, a_1, a_2, ... posloupnosti (1) nazýváme k o e f i c i e n t y polynomu f ; koeficient a_0 nazýváme a b s o l u t n í m č l e n e m polynomu f. Polynom, jehož všechny koeficienty jsou rovny O_R nazýváme n u l o v ý m p o l y n o m e m a označujeme jej symbolem o . Tedy :

$$o = (0, 0, 0, \dots)$$

Polynom, jehož absolutní člen je roven 1_R a ostatní koeficienty jsou rovny O_R nazýváme j e d n o t k o v ý m p o l y n o m e m a označujeme jej symbolem j. Tedy :

$$j = (1, 0, 0, \dots)$$

Množinu všech polynomů jedné proměnné nad okruhem R označujeme $R[x]$.

Poznámka : zřejmě je vždy $R[x] \neq \phi$ (neboť např. $o \in R[x]$). Je-li R netriviální okruh, pak $R[x]$ obsahuje zřejmě nekonečně mnoho prvků, bez ohledu na to, je-li okruh R konečný nebo nikoliv. Je-li R triviální okruh, pak zřejmě $R[x] = \{o\}$. Tento případ budeme v dalším vylučovat.

Definice : *Nechť (1) je nenulový polynom nad R , nechť n je celé nezáporné číslo s vlastností : $a_n \neq 0$; $a_k = 0$ pro $k > n$, t.j.*

$$f = (a_0, a_1, \dots, a_n, 0, 0, \dots)$$

Pak říkáme, že p o l y n o m f j e s t u p n ě n a píšeme : $st(f) = n$.

Koeficient a_n *pak nazýváme v e d o u c í m k o e f i c i e n t e m polynomu* f. *Je-li vedoucí koeficient polynomu* f *roven* 1_R, *pak říkáme, že polynom* f *je n o r m o v a n ý .*

Poznámka : v předchozí definici byl stupeň přiřazen každému polynomu, s výjimkou nulového polynomu o . Abychom tuto neúplnost odstranili, položíme :

$$st\,(o) = -\infty$$

kde $-\infty$ chápeme formálně jakožto jistý symbol, přidaný k množině všech celých čísel, pro nějž definujeme :

$-\infty < n$; $(-\infty) + (-\infty) = (-\infty) + n = n + (-\infty) = -\infty$ pro každé celé číslo n .

Tímto způsobem máme nyní definován pojem stupně polynomu pro libovolné $f \in R[x]$.

Poznámka : polynomy stupně menšího než 1 (t.j. polynomy stupně nula a nulový polynom) obvykle nazýváme konstantní polynomy nebo též konstanty. Při tom je třeba si dobře uvědomit rozdíl mezi nulovým polynomem a polynomem stupně nula ! Dále, polynomy stupně 1 (resp. stupně 2, resp. stupně 3) nazýváme lineární (resp. kvadratické, resp. kubické) polynomy.

Na množině $R[x]$ definujeme nyní dvě operace, sčítání a násobení, které budeme označovat symboly $+$ a $.$, t.j. stejnými symboly jako sčítání a násobení v okruhu R . Z dalšího bude však patrné, že v této souvislosti nemůže dojít k nedorozumění.

Definice : *Nechť* $f = (a_0, a_1, \dots)$, $g = (b_0, b_1, \dots) \in R[x]$. *Pak :*

s o u č e t $f + g$ *definujeme :*

$$f + g = (a_0 + b_0, a_1 + b_1, \dots), \tag{2}$$

s o u č i n $f . g$ *definujeme*

$$f . g = (c_0, c_1, c_2, \dots\dots) \tag{3}$$

kde $c_0 = a_0 b_0$; $c_1 = a_1 b_0 + a_0 b_1$; $c_2 = a_2 . b_0 + a_1 . b_1 + a_0 b_2, \dots\dots$

$\dots$, $c_k = a_k b_0 + a_{k-1} . b_1 + \dots + a_0 . b_k = \sum_{i=0}^{k} a_{k-i} . b_i = \sum_{i+j=k} a_i b_j$, $\dots\dots$

Poznámka: $f+g$ je zřejmě polynomem, neboť pro $m > max\,\{st(f), st(g)\}$ dostáváme $a_m + b_m = 0$ a tedy v posloupnosti (2) je pouze konečně mnoho nenulových prvků. Podobně pro součin $f.g$; je-li $m > st(f) + st(g)$, pak pro každý součin $a_i . b_j$, kde $i + j = m$ musí být $i > st(f)$ nebo $j > st(g)$ a tedy $a_i = 0$ nebo $b_j = 0$. V důsledku toho je pak $c_m = 0$ a tedy v posloupnosti (3) je opět

pouze konečné mnoho nenulových prvků. Vidíme tedy, že $+$ a $.$ jsou operace na množině $R[x]$.

Věta 1.1. : *Množina* $R[x]$ *s operacemi sčítání a násobení polynomů je okruh (t.j. komutativní okruh s jedničkou). Stručně budeme hovořit o okruhu polynomů jedné proměnné nad* R .

[D ů k a z : nechť $f = (a_0, a_1, \dots)$, $g = (b_0, b_1, \dots)$, $h = (c_0, c_1, \dots) \in R[x]$. Z definice je ihned vidět, že operace sčítání polynomů je asociativní a komutativní. Nulový polynom o je nulovým prvkem a polynom $(-a_0, -a_1, \dots)$ je opačným prvkem k f . Je tedy $(R[x], +)$ abelovskou grupou.

Dokažme nyní asociativitu operace násobení. Označme :

$f . g = (p_0, p_1, \dots)$; $g.h = (r_0, r_1, \dots)$

$(f.g).\ h = (s_0, s_1, \dots)$; $f.(g.h) = (s'_0, s'_1, \dots)$

Potom je :

$$s_n = \sum_{i+j=n} p_i . c_j = \sum_{i+j=n} \left(\sum_{k+l=i} a_k . b_l \right) . c_j = \sum_{k+l+j=n} (a_k . b_l) . c_j =$$

$$= \sum_{k+l+j=n} a_k . (b_l c_j) = \sum_{k+m=n} a_k . \left(\sum_{l+j=m} b_l c_j \right) = \sum_{k+m=n} a_k . r_m = s'_n$$

čímž jsme dokázali rovnost : $(f.g).h = f.(g.h)$

Z definice násobení polynomů bezprostředně vyplývá, že jde o operaci komutativní a že jednotkový polynom $j = (1,0,0, \dots)$ je jedničkou. Je tedy $(R[x], .)$ komutativní pologrupa s jedničkou.

Zbývá ověřit platnost distributivního zákona ; označme : $f . (g + h) = (t_0, t_1, \dots)$.

Pak : $t_n = \sum_{i+j=n} a_i (b_j + c_j) = \sum_{i+j=n} a_i b_j + \sum_{i+j=n} a_i c_j$,

odkud plyne, že $f.(g + h) = f.g + f.h$

Dohromady jsme tedy dokázali, že $R[x] = (R[x], +, .)$ je okruh].

Poznámka : polynomy stupně menšího než 1 jsme výše nazvali konstantními polynomy. Pro sčítání a násobení těchto polynomů platí :

$(a_0, 0, \dots) + (b_0, 0, \dots) = (a_0 + b_0, 0, \dots)$

$(a_0, 0, \dots) . (b_0, 0, \dots) = (a_0 . b_0, 0, \dots)$.

Pak ovšem zobrazení $\varphi : R \to R[x]$, definované vztahem :

$\varphi(r) = (r, 0, 0, \ldots)$, pro lib. $r \in R$

je homomorfizmem okruhu R do okruhu $R[x]$. Navíc je zřejmě zobrazení φ injektivní, neboť pro $r,s \in R$, $r \neq s$ je $\varphi(r) \neq \varphi(s)$. Tedy φ je vnořením okruhu R do okruhu $R[x]$ a můžeme ztotožnit prvky okruhu R s jim odpovídajícími konstantními polynomy (při zobrazení φ), resp. můžeme okruh R považovat za unitární podokruh okruhu $R[x]$. Pokud jde o označování konstantních polynomů, můžeme tedy místo $(r,0,0, \ldots)$ psát stručně pouze symbol r a hovořit o "prvku r".

Nyní zavedeme zjednodušené, běžně známé označování polynomů a operací s nimi. Uvažme nejprve, že z definice součinu polynomů vyplývá následující pravidlo pro násobení polynomu $f = (a_0, a_1, \ldots)$ prvkem $r \in R$, t.j. konstantním polynomem $r = (r, 0, 0, \ldots)$:

$$r \,.\, f = (r, 0, 0, \ldots) \,.\, (a_0, a_1, a_2, \ldots) = (r.a_0, r.a_1, r.a_2, \ldots)$$

Dále označme polynom $(0, 1, 0, 0, \ldots)$ nějakým pevným symbolem, např. symbolem x. Z definice násobení polynomů plyne, že :

$$x^2 = x.x = (0, 0, 1, 0, \ldots) \,, \quad x^3 = (0, 0, 0, 1, 0, \ldots) \,, \quad \text{atd.}$$

Nechť nyní $f = (a_0, a_1, a_2, \ldots)$ je polynom stupně menšího nebo rovného n. Vynásobíme-li polynomy $1, x, x^2, \ldots, x^n$ postupně prvky $a_0, a_1, \ldots, a_n$, dostaneme :

$$\begin{aligned}
(a_0, 0, 0, \ldots) &= a_0 \,.\, 1 = a_0 \\
(0, a_1, 0, \ldots) &= a_1 x \\
(0, 0, a_2, 0, \ldots) &= a_2 x^2 \\
&\vdots \qquad\qquad \vdots \\
(0, \ldots, 0, a_n, 0, \ldots) &= a_n x^n
\end{aligned}$$

odkud sečtením dostáváme :

$$(a_0, a_1, \ldots, a_n, 0, \ldots) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \,,$$

t. zn. polynom f můžeme tedy vyjádřit ve tvaru :

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \qquad (4)$$

Je vidět, že vyjádření polynomu f ve tvaru (4) je jednoznačné, neboť dva zápisy tohoto typu se mohou lišit jedině formálně o sčítance tvaru $0.x^k$. Poznamenejme ještě, že součet a součin polynomů, definovaný dříve, splývá při zápisu polynomů

ve tvaru (4) s obvyklým součtem a součinem, známým ze střední školy pro polynomy nad R. Vzhledem ke komutativitě operace $+$ není zřejmě pořadí sčítanců ve (4) pevně dáno. Obvykle budeme sčítance uspořádávat podle mocnin x buď vzestupně nebo sestupně. Dále, pro polynom f budeme podle potřeby používat též označení $f(x)$.

V dalším si blíže všimneme některých vlastností stupně polynomu. Především, z poznámky za definicí součtu a součinu polynomů vyplývá, že pro $f,g \in R[x]$ je:

$$st(f+g) \leqslant max\ \{st(f), st(g)\} \qquad (5)$$

$$st(f.g) \leqslant st(f) + st(g) \qquad (6)$$

při čemž v žádné z nerovností (5) a (6) obecně nenastane rovnost, jak ukazuje následující příklad.

Příklad 1.1: Nechť $R = Z_4$, nechť $f = g = (0, 1, 2, 0, 0, \ldots) \in Z_4[x]$, t.zn. $st(f) = st(g) = 2$.

Potom : $f + g = (0, 2, 0, \ldots)$, t. zn. $st(f+g) = 1 < max\ \{st(f), st(g)\}$, resp.

$f.g = (0, 0, 1, 0, \ldots)$, t. zn. $st(f.g) = 2 < st(f) + st(g)$.

Abychom dostali silnější výsledky, bude tedy třeba klást jisté dodatečné podmínky buď na polynomy f,g nebo na okruh R, jak ukáží následující věty.

Věta 1.2: *Nechť R je okruh ; $f, g \in R[x]$. Jestliže vedoucí koeficient polynomu f nebo polynomu g není dělitelem nuly v R, pak*

$$st(f.g) = st(f) + st(g) \,.$$

[D ů k a z : nechť platí předpoklady věty; je-li $g = o$ nebo $f = o$, pak $f.g = o$ a tvrzení věty platí. Nechť tedy $f,g \neq o$, při čemž $st(f) = m$, $st(g) = n$ a nechť $f.g = (c_0, c_1, \ldots)$. Pak je :

$$c_{m+n} = (a_{m+n} \,.\, b_0 + \ldots + a_{m+1} \,.\, b_{n-1}) + a_m \,.\, b_n + (a_{m-1} \,.\, b_{n+1} + \ldots + a_0 \,.\, b_{m+n}).$$

Všechny součiny v prvé i druhé závorce jsou nulové, neboť $a_k = 0$ pro $k > m$, resp. $b_k = 0$ pro $k > n$. Tedy $c_{m+n} = a_m \,.\, b_n \neq 0$ podle předpokladu věty. Tedy je $st(f.g) \geqslant m + n = st(f) + st(g)$, odkud však vzhledem k (6) dostáváme žádanou rovnost.]

Poznámka : Obrácení předchozí věty obecně neplatí. Vezmeme-li např. v $Z_6[x]$ polynomy $f = g = 2x$, pak $f.g = 4x^2$, t. zn. $st\,(f.g) = st\,(f) + st\,(g)$, ale při tom vedoucí koeficient polynomu f i g je dělitelem nuly v Z_6.

Důsledek: Nechť R je obor integrity. Pak pro libovolné $f,g \in R[x]$ platí

$$st\,(f.g) = st\,(f) + st\,(g) .$$

[D ů k a z : je-li $f = g = o$, pak tvrzení zřejmě platí. Je-li alespoň jeden z polynomu f,g nenulový, pak jde o přímý důsledek předchozí věty.]

Věta 1.3: *Nechť R je okruh ; nechť $f \in R[x]$ je nenulový polynom. Potom : f je dělitelem nuly v $R[x]$ $\Leftrightarrow$ existuje $c \in R$, $c \neq 0$ tak, že $c.f = o$.*

[D ů k a z : " $\Leftarrow$ " zřejmé, neboť $c \in R$, $c \neq 0$ lze chápat jako nenulový polynom z $R[x]$.

" $\Rightarrow$ " označme $f(x) = a_0 + a_1 x + \ldots + a_n x^n$. Podle předpokladu existuje polynom $g \in R[x]$, $g \neq o$ takový, že $f.g = o$. Nechť $g(x) = b_0 + b_1 x + \ldots + b_m x^m$. Je-li $st\,(g) = 0$, pak je tvrzení dokázáno. Nechť tedy $st\,(g) \geq 1$. Nyní stačí dokázat, že existuje polynom $h \in R[x]$, $h \neq o$, $st\,(h) < st\,(g)$ tak, že $f.h = o$, neboť pak po konečném počtu kroků stejnou úvahou dojdeme k žádanému tvrzení.

Uvážíme-li polynomy

(7) $$a_0.g(x) , a_1.g(x) , \ldots\ldots , a_n.g(x) ,$$

pak mohou nastat dvě možnosti :

1) všechny polynomy v (7) jsou nulové a tedy mimo jiné platí :

$$a_0.b_m = a_1.b_m = \ldots\ldots = a_n.b_m = 0 ,$$

odkud pak dostáváme, že $b_m . f(x) = o$. Stačí tedy v tomto případě položit : $h(x) = b_m$.

2) existuje index r $(0 \leq r \leq n)$ takový, že

(8) $$a_r . g(x) \neq o$$

a dále pak : $$a_{r+1} . g(x) = a_{r+2} . g(x) = \ldots . = a_n . g(x) = o$$

Pak ale je :

(9) $$o = (a_0 + a_1 x + \ldots + a_n x^n) . g(x) = (a_0 + \ldots + a_r x^r) . g(x) .$$

Položme : $h(x) = a_r . g(x)$. Pak z (9) plyne, že $st\,(h) < st\,(g)$, neboť jinak by totiž polynom na pravé straně (9) nebyl nulový. Podle (8) je $h \neq o$. Při tom $f . h = a_r . f . g = o$, t. zn. h je hledaný polynom.]

Poznámka : z předchozí věty je vidět, že je-li f polynom, jehož alespoň jeden koeficient není dělitelem nuly v R , pak f není dělitelem nuly v $R[x]$.

Důsledek: R je oborem integrity $\Leftrightarrow$ $R[x]$ je oborem integrity.

[D ů k a z : "$\Rightarrow$" je přímým důsledkem předchozí věty.

"$\Leftarrow$" : plyne z toho, že prvky z R lze chápat jako (konstantní) polynomy z $R[x]$. Je-li tedy $r,s \in R$; $r,s \neq 0$, pak musí být $r.s \neq 0$, poněvadž podle předpokladu $R[x]$ je oborem integrity.]

Poznámka : okruh polynomů $R[x]$ nemůže být v žádném případě tělesem, neboť např. polynom $f(x) = x$ je nenulový a v $R[x]$ k němu neexistuje inverzní prvek. Zabýváme-li se otázkou existence jednotek v $R[x]$ (t.j. polynomů, k nimž existují v $R[x]$ inverzní), vidíme, že každá jednotka okruhu R (chápaná jakožto konstantní polynom) bude jednotkou okruhu $R[x]$. Obecně ovšem i k nekonstantním polynomům může v $R[x]$ existovat inverzní, např. v $Z_4[x]$ je :

$$(1 + 2x) . (1 + 2x) = 1$$

t. zn. lineární polynom $f = 1 + 2x$ je jednotkou v $Z_4[x]$.

Omezíme-li se však na obory integrity, pak se situace zjednoduší, jak ukazuje následující věta.

Věta 1.4. : *Nechť R je obor integrity. Pak jednotkami okruhu $R[x]$ jsou právě jednotky okruhu R .*

[D ů k a z : jednotky okruhu R jsou zřejmě jednotkami $R[x]$. Naopak, nechť polynom f je jednotkou $R[x]$, t. zn. existuje $g \in R[x]$ tak, že $f.g = j$. Podle důsledku V.1.2. je :

$$st\,(f.g) = st\,(f) + st\,(g) = 0$$

odkud však plyne, že $st\,(f) = st\,(g) = 0$, t. zn. f i g jsou konstanty z R. Tedy f je pak jednotkou R].

Poznámka : je-li R oborem integrity, pak i $R[x]$ je oborem integrity a

tedy v $R[x]$ platí zákony o krácení (podle V.1.1. kapitoly 1), t.j. je-li $f,g,h \in R[x]$, pak $f \neq o$, $f.g = f.h \Rightarrow g = h$.

Předpoklady tohoto tvrzení lze však ještě poněkud zeslabit, jak ukazuje následující věta,

Věta 1.5.: *Nechť R je okruh; $f, g, h \in R[x]$. Jestliže alespoň jeden koeficient polynomu f není dělitelem nuly v R , pak lze polynomem f krátit, t.zn. platí implikace :*

$$f.g = f.h \Rightarrow g = h$$

[D ů k a z : rovnost $f.g = f.h$ lze přepsat do tvaru : $f.(g-h) = o$. Jestliže alespoň jeden koeficient polynomu f není dělitelem nuly v R , pak $f \neq o$ a podle V.1.3. f není dělitelem nuly v $R[x]$. Pak tedy $g-h = o$, neboli $g = h$].

Pojem dělitelnosti, zavedený v kapitole 1 pro okruhy si nyní přeformulujeme specielně pro okruh polynomů $R[x]$.

Definice : *Nechť R je okruh; nechť $f, g \in R[x]$. Existuje-li polynom $h \in R[x]$ s vlastností :*

$$f = g . h$$

pak říkáme, že p o l y n o m g d ě l í p o l y n o m f a píšeme : $g|f$. V opačném případě říkáme, že g n e d ě l í f a píšeme : $g \nmid f$.

Poznámka : stejně jako v obecném případě, je-li $f = o$, pak zřejmě $g|o$, pro každý polynom $g \in R[x]$. Naopak, je-li $g = o$, pak $o|f$ jedině v případě, že $f = o$.

Vzhledem k tomu, že $R[x]$ je okruh, který nemusí být oborem integrity, a že většina vlastností dělitelnosti byla odvozena pro obory integrity, nelze obecně všechny výsledky § 2, kap. 1 přenést na polynomy.

§ 2 : DĚLENÍ SE ZBYTKEM DVOU POLYNOMŮ

Definice : *Nechť R je okruh; $f, g \in R[x]$. Říkáme, že v $R[x]$ l z e p r o v é s t d ě l e n í s e z b y t k e m polynomu f polynomem g , jestliže existují polynomy $q, r \in R[x]$, splňující :*

1. $f = g . q + r$
2. $st\,(r) < st\,(g)$

Polynom q , resp. r, se potom nazývá p o d í l , resp. z b y t e k tohoto dělení.

Poznámka : je vidět, že pro $g = o$ nelze (pro žádný polynom f) dělení se zbytkem provést, neboť nemůže být splněna podmínka 2. V dalším se budeme zajímat o to, zda pro $g \neq o$ dělení se zbytkem provést lze, resp. zda podíl q a zbytek r jsou určeny jednoznačně. Následující jednoduché příklady ukazují, že odpověď je v obou případech obecně negativní.

Příklad 2.1.: V okruhu polynomů $Z[x]$ uvažme polynomy $f = 3x$, $g = 2x$. Pak zřejmě nelze najít polynomy $q, r \in Z[x]$ tak, aby platilo

$$3x = (2x) . q + r \quad ; \quad st\,(r) < 1 = st\,(g) .$$

Příklad 2.2.: V okruhu polynomů $Z_4[x]$ vezměme polynomy :
$f = 2x^3 + 3x + 2$; $g = 2x^2 + 1$.
Pak zřejmě platí :
$2x^3 + 3x + 2 = (2x^2 + 1).(x + 2) + 2x$, $3x + 2 = (2x^2 + 1).(2x^2 + x + 1) + (2x + 1)$, atd., t. zn. dělení se zbytkem zde provést lze, ale podíl a zbytek nejsou určeny jednoznačně.

Věta 2.1.: *Nechť R je okruh, nechť $f,g \in R[x]$. Je-li vedoucí koeficient polynomu g jednotkou okruhu R, pak v $R[x]$ lze provést dělení se zbytkem polynomu f polynomem g.*

[D ů k a z : označme $f = a_0 + a_1 x + \ldots + a_n x^n$,
$g = b_0 + b_1 x + \ldots + b_m x^m$.
Podle předpokladu je b_m jednotkou R , t. zn. v R existuje prvek b_m^{-1} .

Tedy je $st\,(g) \geqslant 0$. Větu dokážeme indukcí vzhledem k $st\,(f)$.

Je-li $st\,(f) < st\,(g)$, pak věta platí, neboť stačí položit $q = o$, $r = f$. Nechť tedy je $st\,(f) \geqslant st\,(g)$, t. zn. $st\,(f) = st\,(g) + k$, kde $k \geqslant 0$ je celé číslo. Při $k = 0$ (t. zn. $st\,(f) = st\,(g)$) položíme $q(x) = a_n . b_m^{-1}$; $r\,(x) = f\,(x) - a_n . b_m^{-1} . g\,(x)$. Pak zřejmě $f = g . q + r$, $st\,(r) < st\,(g)$, jak plyne z konstrukce polynomu $r\,(x)$.

Nyní předpokládejme, že věta platí pro $st\,(f) \leqslant st\,(g) + k$ ($k \geqslant 0$ celé číslo) a dokažme její platnost pro $st\,(f) = st\,(g) + k + 1$. Položme

(1) $$f_1\,(x) = f\,(x) - a_n . b_m^{-1} . x^{k+1} . g\,(x)$$

Pak zřejmě $st\,(f_1) < st\,(f)$, t. zn. podle indukčního předpokladu existují polynomy $q_1(x)$, $r_1(x)$ s vlastností :

(2) $$f_1(x) = g(x) . q_1(x) + r_1(x) \quad ; \quad st\,(r_1) < st\,(g)$$

Z (1) a (2) však plyne :

$f\,(x) = f_1(x) + a_n . b_m^{-1} . x^{k+1} . g\,(x) = g\,(x) . (q_1(x) + a_n . b_m^{-1} . x^{k+1}) + r_1(x)$.

Položíme-li $q(x) = q_1(x) + a_n . b_m^{-1} . x^{k+1}$; resp. $r(x) = r_1(x)$, dostáváme tak hledané polynomy, c. b. d.] .

Poznámka : důkaz věty 2.1. je konstruktivní, t. zn. je z něj vidět postup pro získání podílu a zbytku při dělení polynomu f polynomem g (za předpokladu, uvedeného ve větě). Tento postup je v podstatě shodný s algoritmem dělení reálných polynomů, známým ze střední školy. Formální způsob zápisu, který budeme používat, si ukážeme na následujícím příkladu.

Příklad 2.3.: V okruhu $Z_4[x]$ proveďte dělení se zbytkem polynomu $f = 2x^3 + 3x^2 + 2x + 3$ polynomem $g = 3x^2 + 3x + 2$.

Řešení : 3 je jednotkou v okruhu Z_4, t. zn. dělení lze provést.

$$(2x^3 + 3x^2 + 2x + 3) : (3x^2 + 3x + 2) \mid 2x + 3$$

$$-2x^3 \pm 2x^2$$

$$x^2 + 2x + 3$$

$$-x^2 \pm x \pm 2$$

$$x + 1$$

Tedy $f = g\,q + r$, kde $q = 2x + 3$; $r = x + 1$.

Věta 2.2.: *Nechť R je okruh ; nechť $g \in R[x]$ je polynom, jehož vedoucí koeficient není dělitelem nuly v R . Pak pro lib. $f \in R[x]$ existuje nejvýše jedna dvojice polynomů q , r tak, že*

$$f = g . q + r \quad ; \qquad st\,(r) < st\,(g)$$

[D ů k a z : nechť platí předpoklady věty a nechť q, r resp. q', r' jsou dvě dvojice polynomů požadovaných vlastností, t. zn. platí :

(3) $$f = g . q + r = g . q' + r'$$

kde $st\,(r) < st\,(g)$, $st\,(r') < st\,(g)$. Odtud však plyne, že :

(4) $$st\,(r'-r) < st(g)$$

Přepsáním vztahu (3) dostaneme : $g\,(q-q') = r' - r$, t. zn. podle V.1.2. je :

(5) $$st\,(r'-r) = st\,(g) + st\,(q-q')$$

Ze (4) a (5) pak dostáváme : $st\,(g) + st\,(q-q') < st\,(g)$, při čemž $st(g) \geqslant 0$. Tedy musí být : $st\,(q-q') = -\infty$, t. zn. $q = q'$. Odsud pak vzhledem k (3) dostáváme, že $r = r'$, c. b. d.] .

Věta 2.3. : *Nechť R je okruh, nechť $g \in R[x]$ je polynom, jehož vedoucí koeficient je jednotkou okruhu R . Pak pro lib. $f \in R[x]$ lze provést dělení se zbytkem polynomu f polynomem g , při čemž podíl a zbytek tohoto dělení jsou určeny jednoznačně.*

[D ů k a z : tvrzení věty plyne ihned z předchozích dvou vět vzhledem k tomu, že jednotka okruhu R není nikdy dělitelem nuly v R].

Důsledek: Nechť R je těleso. Pak dělení se zbytkem polynomu f polynomem g lze provést pro libovolné polynomy $f, g \in R[x]$, kde $g \neq o$, při čemž podíl a zbytek jsou určeny jednoznačně.

[D ů k a z : tvrzení plyne ihned z předchozí věty vzhledem k tomu, že v tělese je každý nenulový prvek jednotkou] .

Poznámka : Je-li R těleso a jsou-li $f, g \in R[x]$, $g \neq o$, pak při dělení polynomu f polynomem g jsou podíl q a zbytek r opět polynomy z $R[x]$, jak plyne z algoritmu dělení. Tedy, je-li S libovolné nadtěleso tělesa R a dělíme-li

v $S[x]$ dva polynomy, jejichž koeficienty jsou z R, dostáváme podíl a zbytek, jejichž koeficienty jsou opět z R.

§ 3 : HODNOTA POLYNOMU, KOŘEN POLYNOMU

Definice : *Nechť R je okruh; $f = a_0 + a_1x + \ldots + a_nx^n$ je polynom z $R[x]$; $c \in R$ je pevný prvek. Potom prvek :*

$$a_0 + a_1c + \ldots\ldots + a_nc^n \in R$$

označujeme symbolem $f(c)$ a nazýváme h o d n o t o u p o l y n o m u f v b o d ě c.

Je-li $f(c) = O_R$, pak prvek c nazýváme k o ř e n e m p o l y n o m u f.

Poznámka : z definice je bezprostředně vidět, že každý prvek $c \in R$ je kořenem nulového polynomu o, resp. polynom stupně nula naopak nemá nikdy žádný kořen.

Lineární polynom $f \in R[x]$, t. j. polynom tvaru :

$$f = a_0 + a_1x \quad ; \quad a_1 \neq 0$$

v případě, že a_1 je jednotkou okruhu R, má jediný kořen, a to $c = a_1^{-1} \cdot a_0$. Je-li tedy specielně R tělesem, pak každý lineární polynom z $R[x]$ má právě jeden kořen. Polynomy vyšších stupňů pak obecně kořeny mít mohou, ale také nemusí, při čemž podstatně záleží na okruhu R. Problém nalezení kořenů polynomu je jedním ze základních problémů celé algebry. Obecně však neexistuje algoritmus, který by umožňoval kořeny daného polynomu určit.

Věta 3.1.: *Nechť R je okruh; nechť $f, g \in R[x]$. Pak platí :*

1. *je-li $f = g$, pak je $f(r) = g(r)$ pro každé $r \in R$*
2. $(f + g)(r) = f(r) + g(r)$
   $(f - g)(r) = f(r) - g(r)$ *pro každé $r \in R$*
   $(f.g)(r) = f(r) \cdot g(r)$

[D ů k a z : ad 1 : plyne ihned z předchozí definice.

ad 2 : dokáže se přímým rozepsáním ; proveďme si toto např. pro součin $f.g$.

Nechť tedy $f = (a_0, a_1, \ldots, a_n, 0, \ldots)$; $g = (b_0, b_1, \ldots, b_m, 0, \ldots)$. Potom :

$$f.g = (a_0b_0,\ a_0b_1 + a_1b_0, \ldots,\ \sum_{i+j=k} a_ib_j, \ldots)$$

odkud :

$$(f.g)(r) = a_0b_0 + (a_0b_1 + a_1b_0)\cdot r + \ldots + \left(\sum_{i+j=k} a_ib_j\right) \cdot r^k + \ldots =$$

$$= (a_0 + a_1r + \ldots + a_nr^n) \cdot b_0 + (a_0 + a_1r + \ldots + a_nr^n) \cdot b_1r + \ldots + (a_0 + a_1r + \ldots + a_nr^n)b_mr^m =$$

$$= (a_0 + a_1r + \ldots + a_nr^n) \cdot (b_0 + b_1r + \ldots + b_mr^m) = f(r) \cdot g(r) \qquad]$$

Věta 3.2. : *Nechť R je okruh. Pak prvek $c \in R$ je kořenem polynomu $f \in R[x]$ právě když polynom $(x-c)$ dělí f.*

[D ů k a z : I. nechť c je kořenem polynomu f. Polynom $(x-c)$ je normovaný, stupně 1, t. zn. podle V.2.3. existuje právě jedna dvojice polynomů $q, r \in R[x]$:

$$f = (x-c) \cdot q + r \quad ; \quad st(r) < 1$$

protože však $f(c) = 0$, musí být $r = o$, a tedy $(x-c) \mid f$

II. nechť $(x-c) \mid f$, t. zn. $f = (x-c) \cdot h$, kde $h \in R[x]$.

Pak ale $f(c) = 0 \cdot h(c) = 0$

t. zn. c je kořenem polynomu f.]

Definice : *Nechť R je okruh, nechť k je přirozené číslo. Prvek $c \in R$ se nazývá k - n á s o b n ý k o ř e n (nebo též k o ř e n n á s o b n o s t i k) polynomu $f \in R[x]$, jestliže platí :*

(I) $(x-c)^k \mid f$

(II) $(x-c)^{k+1} \nmid f$

Poznámka : při $k = 1$ budeme místo "1-násobný kořen" říkat též "*jednoduchý kořen*". Dále, z definice dělitelnosti polynomů ihned plyne platnost následující implikace : $(x-c)^s \mid f$ pro pevné přir. číslo $s \Rightarrow (x-c)^t \mid f$ pro lib. $t \leq s$, t přir. číslo. Specielně tedy (podle V.3.2.) : každý k - násobný kořen polynomu f je kořenem f ve smyslu původní definice.

Dále, jestliže platí : $(x-c)^s \mid f$ pro nějaké přirozené číslo s, pak můžeme říci, že c je alespoň s - násobným kořenem polynomu f (t. zn. kořenem násobnosti s

nebo vyšší). Při tom však zřejmě násobnost libovolného kořene nenulového polynomu f nemůže být větší než stupeň tohoto polynomu.

Věta 3.3 : *Nechť R je okruh. Pak prvek $c \in R$ je k - násobným kořenem polynomu $f \in R[x]$ právě když existuje polynom $h \in R[x]$ takový, že :*

$$f = (x-c)^k . h \quad a \quad h(c) \neq 0$$

[D ů k a z : I. nechť c je k - násobným kořenem f. Pak $(x-c)^k \mid f$, t. zn. existuje $h \in R[x]$ tak, že $f = (x-c)^k . h$. Kdyby $h(c) = 0$, pak podle V.3.2. $(x-c) \mid h$, t. zn. $h = (x-c) . h_1$, a po dosazení :

$$f = (x-c)^k . (x-c) . h_1 = (x-c)^{k+1} . h_1$$

t. zn. prvek c by byl alespoň $(k+1)$ - násobným kořenem polynomu f, což je spor s předpokladem. Tedy $h(c) \neq 0$.

II. nechť $f = (x-c)^k . h$, kde $h(c) \neq 0$. Je tedy $(x-c)^k \mid f$. Dále, kdyby $(x-c)^{k+1} \mid f$, pak $f = (x-c)^{k+1} . g = (x-c)^k . (x-c) . g$, t. zn. dostáváme :

$$(x-c)^k . h = (x-c)^k . (x-c) . g$$

odkud podle V.1.5., po zkrácení polynomem $(x-c)^k$ dostáváme : $h = (x-c) . g$, t. zn. $h(c) = 0$, což je spor. Tedy musí být $(x-c)^{k+1} \nmid f$ a dohromady dostáváme, že c je k - násobným kořenem polynomu f.] .

Věta 3.4. : *Nechť R je obor integrity ; nechť $f \in R[x]$, $f \neq o$. Jsou-li $c_1, c_2, \ldots, c_n$ navzájem různé kořeny polynomu f o násobnostech $k_1, k_2, \ldots, k_n$, pak polynom f je dělitelný polynomem :*

$$(x-c_1)^{k_1} . (x-c_2)^{k_2} . \ldots . (x-c_n)^{k_n}$$

[D ů k a z : provedeme matematickou indukcí vzhledem k číslu n . Je-li $n = 1$, pak tvrzení plyne z definice k - násobného kořene. Předpokládejme, že tvrzení věty platí pro $1, 2, \ldots, n-1$. Pak tedy :

$$(x-c_1)^{k_1} . \ldots . (x-c_{n-1})^{k_{n-1}} \mid f$$

t.zn.

(1) $f = (x-c_1)^{k_1} . \ldots . (x-c_{n-1})^{k_{n-1}} . h$, kde $h \in R[x]$.

Prvek c_n pak musí být kořenem polynomu h , neboť

$0 = f(c_n) = (c_n-c_1)^{k_1} . \ldots . (c_n-c_{n-1})^{k_{n-1}} . h(c_n)$, odkud, vzhledem k tomu, že R je obor integrity plyne : $h(c_n) = 0$. Nechť tedy c_n je t - násobným kořenem h .

Pak podle V. 3.3. lze psát :

(2) $h = (x-c_n)^t . h_1$; $h_1(c_n) \neq 0$

Podle předpokladu věty a V.3.3. lze psát :

(3) $f = (x-c_n)^{k_n} . h_2$; $h_2(c_n) \neq 0$

Tedy dosazením (2) do (1) a porovnáním s (3) dostáváme :

(4) $(x-c_1)^{k_1} . \ldots . (x-c_{n-1})^{k_{n-1}} . (x-c_n)^t . h_1 = (x-c_n)^{k_n} . h_2$.

Jestliže $k_n > t$, pak po zkrácení polynomem $(x-c_n)^t$ dostáváme :

$$(x-c_1)^{k_1} . \ldots . (x-c_{n-1})^{k_{n-1}} . h_1 = (x-c_n)^{k_n-t} . h_2 \quad .$$

což však vzhledem k V.3.1. vede ke sporu (neboť hodnota polynomu na levé straně v bodě c_n je nenulová, kdežto na pravé straně je nulová). Analogicky dojdeme ke sporu při $k_n < t$. Tedy musí být $k_n = t$. Pak ovšem ze (4) dostáváme :

$$(x-c_1)^{k_1} . \ldots . (x-c_{n-1})^{k_{n-1}} . (x-c_n)^{k_n} \mid f \quad].$$

Důsledek : Nechť R je obor integrity. Pak každý polynom $f \in R[x]$, stupně $m \geq 0$, má nanejvýš m kořenů.

Přesněji řečeno, jsou-li $c_1, \ldots, c_n$ navzájem různé kořeny polynomu f o násobnostech $k_1, \ldots, k_n$, pak platí :

$$k_1 + \ldots + k_n \leq m$$

[D ů k a z : nechť $c_1, \ldots, c_n$ jsou navzájem různé kořeny polynomu f o násobnostech $k_1, \ldots, k_n$. Podle předchozí věty lze polynom f vyjádřit ve tvaru :

$f = (x-c_1)^{k_1} . \ldots . (x-c_n)^{k_n} . h$, $h \in R[x]$, kde zřejmě $h \neq o$.

Tedy : $0 \leq m = st(f) = k_1 + \ldots + k_n + st(h)$, kde ale $st(h) \geq 0$. Pak je ale $m \geq k_1 + \ldots + k_n$, což je žádaná nerovnost.]

Předchozí věta a její důsledek neplatí obecně pro libovolný okruh R , t. zn. předpoklad o neexistenci dělitelů nuly v R nelze vynechat, jak ukazují následující příklady.

Příklad 3.1. : V okruhu $Z_4[x]$ uvažme polynom $f = x^3 + 2x = x(x^2+2)$, resp. polynom $g = 2x$. Pak :

1) polynom f má dva jednoduché kořeny 0 a 2, avšak součin $x.(x-2)$ neděli f

2) polynom g je stupně 1, ale má dva různé kořeny 0 a 2.

Příklad 3.2.: V okruhu $(Z\times Z)[x]$ uvažme polynom $f = (1,0)x$. Vidíme, že polynom f je stupně 1, ale má nekonečně mnoho různých kořenů, neboť zřejmě každý prvek tvaru $(0, a)$, kde $a \in Z$, je kořenem f.

Věta 3.5.: *Nechť R je nekonečný obor integrity; nechť $f \in R[x]$, $f \neq o$. Pak existuje prvek $r \in R$ takový, že $f(r) \neq 0$.*

[D ů k a z : je-li $f \neq o$, pak podle předchozího důsledku má polynom f nejvýše m různých kořenů, kde $m = st(f)$ je pevné celé nezáporné číslo. R má však podle předpokladu nekonečně mnoho prvků, t. zn. musí existovat prvek $r \in R$, který není kořenem f, a pro nějž je tedy $f(r) \neq 0$].

Definice : *Nechť R je okruh, $f \in R[x]$ polynom. Pak zobrazení :*

$$\Phi_f : R \to R$$

definované vztahem $\Phi_f(r) = f(r)$, pro libovolné $r \in R$, se nazývá polynomiální funkce polynomu f.

Je-li $\Psi : R \to R$ nějaké zobrazení, pak Ψ se nazývá polynomiální funkce, je-li polynomiální funkcí nějakého polynomu z $R[x]$, t.j. jestliže existuje $f \in R[x]$ tak, že $\Psi = \Phi_f$.

Označení : nechť R je okruh ; symbolem R^R označujeme okruh funkcí (viz příklad 1.2, kap. I.). Dále nechť $\mathcal{F}$ značí zobrazení okruhu $R[x]$ do okruhu R^R, definované vztahem :

$$\mathcal{F}(f) = \Phi_f \quad , \quad \text{pro lib. } f \in R[x]$$

t. j. zobrazení, které každému polynomu přiřazuje jeho polynomiální funkci.

Věta 3.6.: *Nechť platí výše zavedené označení. Potom :*

1. *zobrazení $\mathcal{F} : R[x] \to R^R$ je okruhový homomorfizmus*
2. *množina $\mathcal{F}(R[x])$, sestávající z polynomiálních funkcí, je unitárním podokruhem okruhu R^R.*

[D ů k a z : ad 1. : nechť $f, g \in R[x]$, pak pro libovolné $r \in R$ je :

$$(\mathcal{F}(f+g))(r) = \Phi_{f+g}(r) = (f+g)(r) = f(r) + g(r) =$$
$$= \Phi_f(r) + \Phi_g(r) = \mathcal{F}(f))(r) + (\mathcal{F}(g))(r) .$$

Tedy platí : $\mathcal{F}(f+g) = \mathcal{F}(f) + \mathcal{F}(g)$

Stejným způsobem se ukáže, že $\mathcal{F}(f.g) = \mathcal{F}(f) . \mathcal{F}(g)$, t. zn $\mathcal{F}$ je homomorfizmus okruhu $R[x]$ do okruhu R^R.

ad 2 : z 1. a z V.1.3 kapitoly I. plyne, že $\mathcal{F}(R[x])$ je podokruhem R^R.

Zbývá tedy ukázat, že je unitárním podokruhem. To však plyne ze vztahu :

$$\mathcal{F}(j) = 1_{R^R} \in \mathcal{F}(R[x])$$

kde $j \in R[x]$ značí jednotkový polynom] .

Poznámka : zobrazení $\mathcal{F}$ obecně nemusí být injektivní a tedy nemusí být vnořením. Ovšem v řadě důležitých případů (na př. pro $R = Z$, resp. Q, resp. K) vnořením je, jak dále ukážeme. V těchto případech pak můžeme polynom ztotožnit s jeho polynomiální funkcí.

Definice : *Nechť R je okruh. Říkáme, že dva polynomy $f, g \in R[x]$ jsou funkčně rovné, je-li $\Phi_f = \Phi_g$, t.j. jinými slovy, je-li $f(r) = g(r)$, pro libovolné $r \in R$.*

Poznámka : dva rovné polynomy $f = g$ jsou podle V.3.1. (část 1) vždycky funkčně rovné, opak však obecně platit nemusí. Vezmeme-li na př. v $Z_3[x]$ polynomy $f = x^3 + x + 1$; $g = 2x + 1$, pak zřejmě $f \neq g$, ale $f(0) = g(0) = 1$, $f(1) = g(1) = 0$, $f(2) = g(2) = 2$, t. zn. polynomy f a g jsou funkčně rovné. Následující věta udává dostatečnou podmínku pro to, kdy oba tyto pojmy splývají.

Věta 3.7. : *Je-li R nekonečný obor integrity, pak dva polynomy z $R[x]$ jsou rovné právě když jsou funkčně rovné.*

[D ů k a z : předpokládejme, že R je nekonečný obor integrity. Nechť polynomy $f, g \in R[x]$ jsou funkčně rovné, t.j. $f(r) = g(r)$ pro lib. $r \in R$. Uvažme polynom $h = f - g$. Zřejmě je :

$$h(r) = (f-g)(r) = f(r) - g(r) = 0$$

pro každé $r \in R$, odkud podle V.3.5. je $h = o$, t. zn. $f - g = o$ a polynomy f, g jsou rovné. Naopak, dva rovné polynomy jsou vždy funkčně rovné podle 1. části V.3.1.] .

Důsledek : Nechť R je nekonečný obor integrity. Pak zobrazení $\mathcal{F}$ z V.3.6. je vnořením okruhu $R[x]$ do okruhu R^R.

[D ů k a z : jde o přímý důsledek V.3.6., V.3.7. a definice zobrazení $\mathcal{F}$].

Vidíme tedy, že nad nekonečným oborem integrity můžeme ztotožnit daný polynom s jeho polynomiální funkcí, jak se to běžně dělá např. v matematické analýze, kde se s polynomy nad tělesem reálných, resp. komplexních čísel pracuje jako s reálnými, resp. komplexními funkcemi. Obecněji lze takovéto ztotožnění provést např. nad každým (netriviálním) číselným okruhem nebo číselným tělesem, což obojí jsou nekonečné obory integrity.

§ 4 : DĚLITELNOST POLYNOMŮ, NEJVĚTŠÍ SPOLEČNÝ DĚLITEL.

ÚMLUVA : všude v tomto paragrafu předpokládáme, že R značí těleso.

Pojem dělitelnosti polynomů byl definován nad libovolným okruhem na konci § 1. Je-li však R těleso, pak $R[x]$ je obor integrity a můžeme tedy použít všech výsledků, které jsme obecně o dělitelnosti odvodili v § 2 kapitoly I.

Poznámka : Je-li S libovolné nadtěleso tělesa R, pak můžeme polynomy $f, g \in R[x]$ zřejmě uvažovat též jako polynomy v $S[x]$ a vyšetřovat jejich dělitelnost v $S[x]$. Nedostaneme však nic nového, neboť při dělení polynomů s koeficienty z tělesa R dostaneme podíl i zbytek opět s koeficienty z R, t.j. vlastnost polynomu g být dělitelem f nezávisí na tom, vyšetřujeme-li ji nad tělesem R nebo nad libovolným jeho nadtělesem S.

Věta 4.1. : *nechť $f, g \in R[x]$ jsou polynomy takové, že $f \neq o$ a $g|f$. Pak platí :* $st(g) \leqslant st(f)$

[D ů k a z : je-li $g|f$, pak existuje $h \in R[x]$ tak, že $f = g.h$. Poněvadž $f \neq o$, musí být $g, h \neq o$, t. zn. stupně všech tří polynomů jsou celá nezáporná čísla, při čemž podle důsledku V.1.2. je : $st(f) = st(g) + st(h)$. Je tedy $st(f) \geqslant st(g)$].

Věta 4.2.: *Nechť $f, g \in R[x]$; pak následující výroky jsou ekvivalentní :*

(a) $f \sim g$

(b) $f|g, g|f$

(c) *existuje prvek $c \in R$, $c \neq 0$ tak, že : $f = c.g$*

[D ů k a z : věta bezprostředně vyplývá z definice asociovaných prvků, z V. 2. 3. kapitoly I. a z V. 1. 4., uvážíme-li, že v tělese je jednotkou každý nenulový prvek.]

Věta 4.3.: *Nechť pro polynomy z $R[x]$ platí: $g \mid f_1, \ldots, g \mid f_k$ (kde k je pevné přirozené číslo) a nechť $h_1, \ldots, h_k$ jsou libovolné polynomy z $R[x]$. Pak:*

$$g \mid (f_1 . h_1 + \ldots + f_k . h_k)$$

[Důkaz: tvrzení je specielním případem V.2.1. (část 2) kapitoly I.]

Také pojmy společný dělitel a největší společný dělitel množiny M, studované v kapitole I., lze opět přirozeným způsobem přenést na polynomy nad tělesem R. Omezíme se tentokráte na případ, že M je konečná množina.

Definice: *Nechť $h, f_1, \ldots, f_k \in R[x]$; je-li $h \mid f_i$ $(i = 1, \ldots, k)$, pak polynom h se nazývá s p o l e č n ý d ě l i t e l polynomů $f_1, \ldots, f_k$.*

Definice: *Nechť $f_1, \ldots, f_k \in R[x]$. Pak n e j v ě t š í m s p o l e č n ý m d ě l i t e l e m (zkrácně: n. s. d.) polynomů $f_1, \ldots, f_k$ nazýváme polynom $d \in R[x]$, pro nějž platí:*

(i) *d je společným dělitelem polynomů $f_1, \ldots, f_k$*

(ii) *je-li $h \in R[x]$ společným dělitelem $f_1, \ldots, f_k$, pak je $h \mid d$.*

Věta 4.4.: *K libovolným polynomům $f_1, \ldots, f_k \in R[x]$ (k přirozené číslo) existuje největší společný dělitel.*

[D ů k a z : je-li $f_1 = f_2 = \ldots = f_k = o$, pak zřejmě o je jejich největší společný dělitel. Nechť alespoň jeden z polynomů $f_1, \ldots, f_k$ je nenulový.

Označme:

$$M = \{f_1 . h_1 + \ldots + f_k . h_k \mid h_1, \ldots, h_k \in R[x] \text{ lib.}\}$$

Množina M má zřejmě tyto vlastnosti:

(α) $f_i \in M$, $i = 1, \ldots, k$

(β) je-li $g_1, g_2 \in M$, pak též $g_1 \pm g_2 \in M$

(γ) je-li $g \in M$, $q \in R[x]$ *lib.*, pak $g.q \in M$

Vzhledem k (α) obsahuje množina M nenulové polynomy; mezi nimi existuje alespoň jeden nejmenšího stupně. Označme jej $d(x)$.

Nechť $g \in M$ lib., pak podle důsledku V.2.3. existují $q, r \in R[x]$ tak, že:

$$g = d.q + r \quad ; \quad st(r) < st(d)$$

Z (β) a (γ) však plyne, že $r \in M$, a vzhledem k tomu, jak byl vybrán polynom d, musí být $r = o$. Pak $d \mid g$, t. zn. specielně $d \mid f_i$, $i = 1, \ldots, k$. Tedy d je společný dělitel $f_1, \ldots, f_k$.

Je-li $h \in R[x]$ společným dělitelem $f_1, \ldots, f_k$, pak podle V.4.3. $h \mid g$ pro libovolný polynom $g \in M$. Specielně tedy $h \mid d$.

Dohromady dostáváme, že $d(x)$ je n. s. d. polynomů $f_1, \ldots, f_k$].

Věta 4.5.: *Množinu všech největších společných dělitelů polynomů $f_1, \ldots, f_k \in R[x]$ obdržíme jako množinu všech nenulových konstantních násobků jednoho (libovolného) největšího společného dělitele polynomů $f_1, \ldots, f_k$.*

[D ů k a z : Věta je specielním případem V.2.6. kapitoly I, uvědomíme-li si, že k polynomu $d \in R[x]$ jsou asociovány právě polynomy tvaru $c.d(x)$, kde $c \in R$, $c \neq 0$].

Důsledek: K libovolným k polynomům $f_1, \ldots, f_k \in R[x]$, z nichž alespoň jeden je nenulový, existuje právě jeden normovaný největší společný dělitel. Tento normovaný největší společný dělitel budeme v dalším označovat symbolem $(f_1, \ldots, f_k)$.

[D ů k a z : jde o přímý důsledek předchozí věty].

Poznámka: vidíme, že n. s. d. konečného počtu polynomů vždy existuje, ale že není určen jednoznačně (s výjimkou případu, že R je dvouprvkové těleso, sestávající z 0 a 1), resp. je určen jednoznačně až na asociovanost. Navíc, důkaz V.4.4. nebyl konstruktivní, t. zn. nepodal návod k výpočtu n. s. d. Tento si nyní uvedeme pro dva polynomy $f, g \in R[x]$, z nichž alespoň jeden je nenulový. Použitá metoda, která je založena na opakovaném dělení polynomů, se nazývá Eukleidův algoritmus.

Výpočet n.s.d. polynomů $f, g \in R[x]$ Eukleidovým algoritmem:

Nechť $f, g \in R[x]$ a nechť např. $g \neq o$. Pak podle důsledku V.2.3. můžeme provést následující dělení polynomů:

$$
\begin{aligned}
f &= g \cdot q_1 + r_1 , \quad st(r_1) < st(g) \\
g &= r_1 \cdot q_2 + r_2 , \quad st(r_2) < st(r_1) \\
r_1 &= r_2 \cdot q_3 + r_3 , \quad st(r_3) < st(r_2) \\
&\cdots\cdots\cdots\cdots \\
r_{k-2} &= r_{k-1} \cdot q_k + r_k , \quad st(r_k) < st(r_{k-1}) \\
r_{k-1} &= r_k \cdot q_{k+1}
\end{aligned}
\qquad (1)
$$

při čemž zbytek v posledním dělení je nulový. Po konečném počtu kroků musíme skutečně k nulovému zbytku dojít, neboť porovnáním nerovností na pravé straně vztahů (1) dostáváme:

$$st(r_1) > st(r_2) > \cdots\cdots > st(r_{k-1}) > st(r_k) .$$

Dokážeme nyní, že polynom r_k, t. zn. poslední nenulový zbytek v posloupnosti dělení (1) je hledaný n. s. d. polynomů f a g.

(*i*): z poslední rovnosti v (1) plyne, že $r_k \mid r_{k-1}$. Uvažíme-li, že triviálně platí $r_k \mid r_k$, pak z předposlední rovnosti, podle V.4.3. plyne, že $r_k \mid r_{k-2}$. Analogicky dostáváme, že $r_k \mid r_{k-3}$, . . . atd, až $r_k \mid g$ a $r_k \mid f$. Tedy r_k je společný dělitel polynomů f a g.

(*ii*): nechť $h \in R[x]$, při čemž $h \mid f$, $h \mid g$. Pak první rovnost z (1) můžeme přepsat ve tvaru:

$$r_1 = f + g \cdot (-q_1)$$

a užitím V.4.3. dostáváme, že $h \mid r_1$. Podobně z druhé rovnosti, vzhledem k tomu, že $h \mid g$ a $h \mid r_1$, užitím V.4.3. dostáváme, že $h \mid r_2$. Takto postupujeme dále, až nakonec z předposlední rovnosti v (1) dostáváme, že $h \mid r_k$. Tedy ukázali jsme, že polynom r_k je největším společným dělitelem polynomů f a g.

Poznámka: vzhledem k tomu, že Eukleidův algoritmus užíva pouze dělení

polynomů, největší společný dělitel dvou polynomů $f, g \in R[x]$ nezávisí na tom, vyšetřujeme-li jej v $R[x]$ nebo v $S[x]$, kde S je libovolné nadtěleso tělesa R. Přesněji řečeno, je-li d_1 největším společným dělitelem polynomů f a g v $S[x]$, pak existuje největší společný dělitel d polynomů f a g, který je asociován s d_1 a je $d \in R[x]$.

Poznámka: v Eukleidově algoritmu (1) používáme pouze dělení dvou polynomů. V konkrétních případech se poměrně často stává, že v průběhu takového dělení dojdeme k "nepříjemným" zlomkům. Na př. máme-li nad polem R reálných čísel dělit polynom $f = x^4 + x^2 - x + 1$ polynomem $g = 15x^2 + 5x + 10$, pak:

$$
\begin{array}{l|l}
(x^4 + x^2 - x + 1) : (15x^2 + 5x + 10) & \frac{1}{15}x^2 - \frac{1}{45}x + \frac{4}{135} \\
\hline
\mp x^4 \pm \frac{1}{3}x^3 \pm \frac{2}{3}x^2 & \\
\hline
\frac{1}{3}x^3 + \frac{1}{3}x^2 - x + 1 & \\
\mp \frac{1}{3}x^3 \mp \frac{1}{9}x^2 \mp \frac{2}{9}x & \\
\hline
\frac{4}{9}x^2 - \frac{7}{9}x + 1 & \\
-\frac{4}{9}x^2 \pm \frac{4}{27}x \pm \frac{8}{27} & \\
\hline
-\frac{25}{27}x + \frac{19}{27} &
\end{array}
$$

Z V.4.5. a ze vztahu (1) je vidět, že v Eukleidově algoritmu je jedno, zda k výpočtu užíváme zbytek r_i anebo jakýkoli jeho nenulový konstantní násobek. Tedy, v kterémkoliv kroku kterémkoliv dělení v Eukleidově algoritmu lze násobit kterýkoliv z polynomů libovolným nenulovým prvkem z tělesa R. Na předchozím příkladu ukážeme, jak se tím urychlí výpočet, zejména při ručním počítání. Z uvedeného bude patrný i způsob zápisu.

$(x^4 + x^2 - x + 1) : (15x^2 + 5x + 10)$ | $x^2, x, -4$

$3x^4 + 3x^2 - 3x + 3 \qquad 3x^2 + x + 2$

$-3x^4 \pm x^3 \pm 2x^2$

$-x^3 + x^2 - 3x + 3$

$3x^3 - 3x^2 + 9x - 9$

$-x^3 \pm x^2 \pm 2x$

$-4x^2 + 7x - 9$

$-12x^2 + 21x - 27$

$\mp 12x^2 \mp 4x \mp 8$

$25x - 19 = r'$

při tom $r' = 25x - 19$ je polynom asociovaný k zbytku po dělení polynomu f polynomem g. Dále je ovšem vidět, že uvedenými úpravami se "znehodnotí" podíl daného dělení, což však výpočet n. s. d. neovlivní, neboť v Eukleidově algoritmu pracujeme pouze se zbytky.

Příklad 4.1. : V $Q[x]$ nalezněte n.s.d. polynomů f a g, kde :
$f = x^4 + 3x^3 - x^2 - 4x - 3$, $g = 3x^3 + 10x^2 + 2x - 3$.

Řešení :

$(x^4 + 3x^3 - x^2 - 4x - 3) : (3x^3 + 10x^2 + 2x - 3)$ | $x, 1$

$3x^4 + 9x^3 - 3x^2 - 12x - 9$

$-3x^4 \pm 10x^3 \pm 2x^2 \mp 3x$

$-x^3 - 5x^2 - 9x - 9$

$3x^3 + 15x^2 + 27x + 27$

$-3x^3 \pm 10x^2 \pm 2x \mp 3$

$(5x^2 + 25x + 30) = r_1$

$(3x^3 + 10x^2 + 2x - 3) : (5x^2 + 25x + 30)$ | $3x, -5$

$-3x^3 \pm 15x^2 \pm 18x \qquad x^2 + 5x + 6$

$-5x^2 - 16x - 3$

$\mp 5x^2 \mp 25x \mp 30$

$\cdot (9x + 27) = r_2$

$(x^2 + 5x + 6) : (9x + 27)$ | $x, 2$

$-x^2 \pm 3x \qquad x + 3$

$2x + 6$

$-2x \pm 6$

$o = r_3$

Tedy, $r_2 = 9x + 27$ je největším společným dělitelem polynomů f a g, resp. normovaným n. s. d. těchto polynomů je pak $(f,g) = x + 3$

Věta 4.6.: *Nechť $f, g \in R[x]$, z nichž alespoň jeden je nenulový. Potom:*

1. *existují polynomy $u, v \in R[x]$ takové, že platí:*

(2) $\qquad f.u + g.v = (f,g)$

2. *je-li navíc $st(f), st(g) \geq 1$, pak lze polynomy u, v ve výrazu (2) vybrat tak, že:*

$$st(f) > st(v), \quad st(g) > st(u)$$

[D ů k a z : ad 1 : nechť na př. $g \neq o$; pak z rovnic (1) Eukleidova algoritmu dostáváme :

$r_1 = f - g.q_1 = f.u_1 + g.v_1$, označíme-li $u_1 = 1$, $v_1 = -q_1$

$r_2 = g - (f.u_1 + g.v_1)q_2 = f.(-u_1 q_2) + g(1 - v_1 q_2) = f.u_2 + g.v_2$,

označíme-li $u_2 = -u_1 q_2$, $v_2 = 1 - v_1 q_2$.

Tímto postupným dosazováním pokračujeme dále, až nakonec dostaváme (po patřičném označení) :

$r_k = f.u_k + g.v_k$.

Podle předchozího je však r_k n. s. d. polynomů f a g. Nechť c je vedoucí koeficient polynomu r_k. Pak :

$(f,g) = c^{-1}.r_k = f.(c^{-1}.u_k) + g(c^{-1}v_k) = f.u + g.v$,

označíme-li $u = c^{-1}u_k$, $v = c^{-1}v_k$.

ad 2 : nechť $st(f), st(g) \geq 1$ a nechť u, v jsou polynomy splňující (2)

Nechť $st(u) \geq st(g)$. Podle důsledku V.2.3. lze psát :

$u = g.q + r$, kde $st(r) < st(g)$

Dosazením do (2) dostáváme :

$(f,g) = f(g.q + r) + gv = f.r + g(fq + v)$

kde polynom r má již požadovanou vlastnost. Tedy můžeme předpokládat, že u,v jsou polynomy splňující (2), při čemž $st(g) > st(u)$.

Dále sporem ; nechť $st(v) \geq st(f)$. Pak je :

$st(g) + st(v) > st(u) + st(f)$, neboli $st(g.v) > st(f.u)$, odkud plyne, že musí být : $st(f.u + g.v) = st(g.v)$.

Pak ale : $st((f,g)) = st(f.u + g.v) = st(g.v) = st(g) + st(v) \geq 1 + st(f)$ $> st(f)$, což je spor, neboť podle V.4.1. je $st((f,g)) \leq st(f)$.

Tedy $st(f) > st(v)$, c.b.d.] .

Poznámka : z důkazu 1. části předchozí věty je vidět, že při konstrukci polynomů u,v splňujících (2) používáme kromě zbytků i podíly dělení z Eukleidova algoritmu. Při konkretním výpočtu nelze tedy v průběhu dělení násobit libovolně nenulovým prvkem z R , jak tomu bylo při hledání n.s.d.

Příklad 4.2. : V $Q[x]$ nalezněte polynomy u,v, splňující (2), je-li dáno :

$f = x^3 - x^2 + 3x - 10$; $g = x^3 + 6x^2 - 9x - 14$

Řešení : pomocí Eukleidova algoritmu hledáme n. s. d. polynomů f a g , při čemž si průběžně označujeme nalezené podíly a zbytky. Zde dostaneme (po výpočtu) :

$f = g.q_1 + r_1$, kde $q_1 = 1, r_1 = -7x^2 + 12x + 4$

$g = r_1 q_2 + \frac{235}{49} r_2$, kde $q_2 = -\frac{1}{7}x - \frac{54}{49}$, $r_2 = x - 2$

$r_1 = r_2 q_3$, kde $q_3 = -7x - 2$

Tedy : $(f,g) = r_2 = x - 2$, při čemž zpětným výpočtem najdeme polynomy u,v :

$r_2 = \frac{49}{235} g - \frac{49}{235} r_1 q_2 = \frac{49}{235} g - \frac{49}{235}(f - g.q_1)q_2 =$

$= f(-\frac{49}{235} q_2) + g(\frac{49}{235} + \frac{49}{235} q_1 q_2)$

Pak :

$u = -\frac{49}{235} q_2 = \frac{7}{235} x + \frac{54}{235}$

$v = \frac{49}{235} + \frac{49}{235} q_1 q_2 = -\frac{7}{235} x - \frac{5}{235}$

Definice : *Polynomy $f,g \in R[x]$ nazýváme nesoudělné, je-li $(f,g) = 1$*

Věta 4.7. : *Nechť $f,g \in R[x]$; pak polynomy f,g jsou nesoudělné, právě když existují polynomy $u,v \in R[x]$, splňující :*

(3) $f.u + g.v = 1$

[D ů k a z : jsou-li f,g nesoudělné, pak z předchozí definice a z V.4.6. plyne (3). Naopak, nechť existují polynomy $u,v \in R[x]$, splňující (3). Pak zřejmě alespoň jeden z polynomů f,g je nenulový a tedy existuje normovaný n. s. d. (f,g). Z definice n. s. d. a z V.4.3. plyne, že $(f,g) \mid f.u + g.v = 1$, a tedy $(f,g) = 1$] .

Věta 4.8. : *Nechť $f,g,h \in R[x]$. Pak platí :*

1. $(f,g) = 1$, $(f,h) = 1$ $\Rightarrow$ $(f, g.h) = 1$
2. $h \mid f.g$, $(h,f) = 1$ $\Rightarrow$ $h \mid g$
3. $g \mid f$, $h \mid f$, $(g,h) = 1$ $\Rightarrow$ $g.h \mid f$

[D ů k a z : ad 1 : je-li $(f,g) = 1$, pak podle V.4.7. existují $u,v \in R[x]$, splňující (3). Po vynásobení (3) polynomem h dostáváme :

(4) $f.u.h + g.v.h = h$

Nechť $q \in R[x]$ je polynom, pro nějž $q \mid f$; $q \mid g.h$. Pak ze (4), podle V. 4.3. je $q \mid h$. Tedy také $q \mid (f,h) = 1$, odkud však dostáváme, že $(f, g.h) = 1$.

ad 2 : Z předpokladu $(h,f) = 1$ podle V.4.7. plyne, že existují $u,v \in R[x]$ tak, že

$h.u + f.v = 1$

odkud po vynásobení polynomem g dostáváme :

(5) $h.g.u + f.g.v = g$.

Ale $h \mid h$, $h \mid f.g$, t. zn. z (5) podle V.4.3. plyne, že $h \mid g$

ad 3 : podle předpokladu je $g \mid f$, t. zn. existuje polynom $q_1 \in R[x]$ tak, že $f = g.q_1$

a dále podle předpokladu je $h \mid g.q_1$, při čemž však $(g,h) = 1$. Tedy podle právě dokázané části 2. je $h \mid q_1$, neboli $q_1 = h.q_2$, pro nějaké $q_2 \in R[x]$.

Po dosazení dostáváme :

$$f = g.(h.q_2) = (g.h).q_2$$

t. zn. $g.h \mid f$].

Na závěr ještě poznamenejme, že jsou-li $f,g \in R[x]$ polynomy nesoudělné v $R[x]$, pak f,g jsou nesoudělné rovněž v $S[x]$, kde S je libovolné nadtěleso tělesa R (jak plyne z Eukleidova algoritmu a z definice nesoudělných polynomů).

§ 5 : IREDUCIBILNÍ POLYNOMY, ROZKLAD POLYNOMU.

ÚMLUVA : Všude v tomto paragrafu předpokládáme, že R značí těleso.

Pojem reducibilního, resp. ireducibilního prvku, definovaný v kapitole I., lze opět přirozeným způsobem přenést na polynomy. Uvědomme si jen, že je-li R těleso, pak jednotky oboru integrity $R[x]$ jsou právě všechny polynomy stupně 0, resp. navzájem asociované polynomy musí mít stejný stupeň (plyne z V.1.4., V.4.2. a z důsledku V.1.2).

Definice : *Nechť $f \in R[x]; st(f) \geq 1$. Řekneme, že polynom f je reducibilní v $R[x]$ (nebo též nad tělesem R), jestliže existují polynomy $g,h \in R[x]$; $1 \leq st(g)$, $st(h) < st(f)$ takové, že platí :*

$$f = g.h$$

V opačném případě říkáme, že polynom f je ireducibilní v $R[x]$ (nebo též nad tělesem R).

Poznámka : Vidíme, že předchozí definice je speciálním případem definice reducibilního (resp. ireducibilního) prvku z §2, kapitoly I. Pak tedy na př. na základě V.2.5. kap. I můžeme říci, že polynom f je ireducibilní (resp. reducibilní) nad R, právě když $c.f$ je ireducibilní (resp. reducibilní) nad R , pro lib. $c \in R$, $c \neq 0$.

Příklad 5.1.: každý lineární polynom $f \in R[x]$ je ireducibilní nad tělesem R, jak vyplývá přímo z definice.

Opačná implikace obecně neplatí, jak ukazuje následující příklad.

Příklad 5.2.: v $R[x]$ uvažme kvadratický polynom $f = x^2 + 1$. Pak f je zřejmě ireducibilní nad tělesem R.

Uvažujeme-li tentýž polynom $f = x^2 + 1$ jako polynom z $K[x]$, pak f je reducibilní nad K, neboť $f = (x + i)(x - i)$

Poznámka : z předchozího příkladu je vidět, že při zjišťování reducibility či ireducibility podstatně záleží na tělese, nad nímž pracujeme a je tedy nutné, zejména v případech, kdy by mohlo dojít k nedorozumění, výslovně uvést, nad kterým tělesem je daný polynom reducibilní, resp. ireducibilní.

Obecně pak platí následující věta.

Věta 5.1. : *Nechť $f \in R[x]$ a nechť R_1 je libovolné nadtěleso tělesa R. Pak platí:*

1. *je-li f reducibilní v $R[x]$, pak je reducibilní v $R_1[x]$.*
2. *je-li f ireducibilní v $R_1[x]$, pak je ireducibilní v $R[x]$.*

[D ů k a z : 1. část věty plyne ihned z definice a 2. část je pouze logickým důsledkem 1. části].

Věta 5.2.: *Nechť $f,g \in R[x]$; nechť f je ireducibilní nad R.*
Pak je buď $(f,g) = 1$ nebo je $f \mid g$.

[D ů k a z : nechť platí předpoklad věty a nechť $(f,g) \neq 1$. Pak musí být $st((f,g)) \geqslant 1$. Zřejmě lze psát : $f = (f,g).q$; protože však f je ireducibilní polynom, musí být $st(q) = 0$. Označíme-li $q(x) = c \in R$, pak $c \neq 0$ a můžeme psát : $(f,g) = c^{-1}.f$, t. zn. $f \mid (f,g)$. Zřejmě je $(f,g) \mid g$ a z transitivity relace dělitelnosti pak plyne : $f \mid g$].

Věta 5.3. : *Nechť $f \in R[x]$; pak následující výroky jsou ekvivalentní :*

(a) *f je ireducibilní v $R[x]$*

(b) *je-li $f \mid g.h$, kde $g,h \in R[x]$, pak $f \mid g$ nebo $f \mid h$.*

[D ů k a z : "(a) $\Rightarrow$ (b)" : nechť f je ireducibilní a nechť $f \mid g.h$, $f \nmid g$. Pak podle V.5.2. je $(f,g) = 1$, t. zn. podle V.4.8. (část 2) je $f \mid h$.

"(b) $\Rightarrow$ (a)" : sporem; nechť platí (b) a nechť f je reducibilní. Pak existují polynomy $g, h \in R[x]$, $1 \leqslant st(g)$, $st(h) < st(f)$ takové, že platí: $f = g.h$. Tedy triviálně je $f \mid g.h$ a podle V.4.1. $f \nmid g$, $f \nmid h$, t. zn. dostáváme spor s platností (b). Polynom f musí tedy být ireducibilní.]

Důsledek: Nechť f je ireducibilní v $R[x]$ a nechť $g_1, \ldots, g_s \in R[x]$ tak, že:

$$f \mid g_1 . \ldots . g_s$$

Pak existuje přirozené číslo k: $1 \leqslant k \leqslant s$ tak, že $f \mid g_k$.

[D ů k a ž : důsledek plyne bezprostředně z V.5.3. užitím matematické indukce.]

Věta 5.4.: ("*Věta o existenci a jednoznačnosti rozkladu na ireducibilní polynomy*")
Nechť $f \in R[x]$, $st(f) \geqslant 1$. Pak :

1. *polynom f lze vyjádřit jako součin konečného počtu ireducibilních polynomů nad R, t. zn.*

(1) $$f = p_1 . \ldots . p_r$$

kde p_i je ireducibilní polynom v $R[x]$, $i = 1, \ldots, r$

2. *rozklad (1) je jednoznačný až na pořadí činitelů a asociovanost, t. zn. je-li*

(2) $$f = q_1 . \ldots . q_s$$

kde q_i je ireducibilní polynom v $R[x]$, $i = 1, \ldots, s$, pak je $k = s$ a po vhodném přečíslování činitelů v (2) je $p_i \sim q_i$, $i = 1, \ldots, r$.

[D ů k a z : ad 1 : existenci rozkladu (1) dokážeme matematickou indukcí vzhledem k stupni polynomu f. Je-li $st(f) = 1$, pak podle příkladu 5.1. je f ireducibilní, t. zn. je ve tvaru (1). Předpokládejme, že tvrzení platí pro polynomy stupně 1, 2, 3, . . . ; $n-1$. Nechť $st(f) = n$. Je-li f ireducibilní, pak je již v žádaném tvaru. Nechť tedy f je reducibilní. Pak existují polynomy $g,h \in R[x]$; $1 \leqslant st(g)$, $st(h) \leqslant st(f) = n$ tak, že $f = g.h$. Podle indukčního předpokladu existují ireducibilní polynomy $p_1, \ldots, p_l, p_{l+1}, \ldots p_r \in R[x]$ tak, že :

$$g = p_1 . \ldots . p_l \quad , \qquad h = p_{l+1} \ldots . p_r$$

odkud po dosazení dostáváme : $f = p_1 . \ldots . p_l . p_{l+1} \ldots p_r$, t. zn. f je ve tvaru (1).

ad 2 : jednoznačnost rozkladu dokážeme opět matematickou indukcí vzhledem k stupni f . Je-li $st(f) = 1$, pak jednoznačnost rozkladu (1) je zřejmá. Předpokládejme, že tvrzení o jednoznačnosti platí pro polynomy stupně 1, 2, . . , $n-1$. Nechť $st(f) = n$ a nechť (1) a (2) jsou dva rozklady polynomu f na ireducibilní polynomy, t. zn. pak :

(3) $$p_1 . p_2 . \ldots . p_r = q_1 . q_2 . \ldots . q_s$$

odkud plyne, že $p_1 \mid q_1 \ldots q_s$. Podle důsledku V.5.3. však existuje přirozené číslo i_o $(1 \leqslant i_o \leqslant s)$ tak, že $p_1 \mid q_{i_o}$. Přečíslujme polynomy q_i tak, že bude $p_1 \mid q_1$. Z definice ireducibilního polynomu však potom plyne, že $p_1 \sim q_1$, t. zn. existuje $c_1 \in R$, $c_1 \neq 0$ tak, že $q_1 = c_1 . p_1$. Po dosazení do (3) a vykrácení polynomem p_1 pak dostáváme :

$$p_2 . p_3 \ldots p_r = c_1 . q_2 . q_3 \ldots q_s$$

Podle indukčního předpokladu však odtud dostáváme, že $r-1 = s-1$, neboli $r = s$

a po vhodném přečíslování : $p_2 \sim c_1 q_2$, t. zn. rovněž $p_2 \sim q_2$ a dále pak $p_3 \sim q_3$, ... , $p_r \sim q_r$. Tím je věta dokázána.]

Poznámka : z dosavadních výsledků tohoto paragrafu je vidět značná podobnost mezi úvahami o rozkladu polynomů na ireducibilní polynomy v oboru integrity $R[x]$ a známými úvahami o rozkladu celého čísla na prvočísla. Skutečně, obecně lze ukázat, že okruhy $R[x]$ a Z jsou specielními případy t. zv. okruhu s jednoznačným rozkladem. Na rozdíl od rozkladu přirozených nebo celých čísel na prvočísla je však praktický výpočet rozkladu (1) pro daný polynom $f \in R[x]$ obvykle příliš komplikovaný. Je dokonce mnohdy velmi obtížné vůbec rozhodnout o polynomu $f \in R[x]$ zda je nad tělesem R reducibilní či ireducibilní, t. zn. podat pro dané těleso R vyčerpávající charakterizaci ireducibilních polynomů z $R[x]$. V dalším se nám to v některých konkrétních případech podaří (např. pro $R = K$, $R = R$) a v některých nikoliv (např. pro $R = Q$).

Dále se nyní budeme zabývat takovými tělesy, nad nimiž je charakterizace ireducibilních polynomů jistým způsobem nejjednodušší.

Definice : *Těleso R nazýváme algebraicky uzavřené, jestliže každý polynom $f \in R[x]$, $st\,(f) \geq 1$, má v R alespoň jeden kořen.*

Věta 5.5 : *Nechť R je těleso; pak následující výroky jsou ekvivalentní :*

(a) *těleso R je algebraicky uzavřené*

(b) *každý polynom $f \in R[x]$, $st\,(f) \geq 1$, lze vyjádřit ve tvaru součinu lineárních polynomů z $R[x]$.*

(c) *ireducibilní polynomy v $R[x]$ jsou právě všechny lineární polynomy.*

[D ů k a z : "(a) $\Rightarrow$ (b)": dokazujeme matematickou indukcí vzhledem k $st\,(f)$. Je-li $st\,(f) = 1$, pak f je lineární polynom a výrok (b) platí. Předpokládejme, že (b) platí pro polynomy stupně $1, 2, \ldots, n-1$. Nechť $st(f)=n$. Podle (a) existuje kořen $c \in R$ polynomu f , t. zn. lze psát : $f = (x-c) \cdot q$, kde $q \in R[x]$, $st\,(q) = n-1$. Podle indukčního předpokladu lze však polynom q napsat jako součin lineárních polynomů z $R[x]$, t. zn. po dosazení dostáváme žádané vyjádření.

"(b) $\Rightarrow$ (c)" : každý lineární polynom je v $R[x]$ ireducibilní (viz příklad 5.1.). Naopak, z (b) ihned vyplývá, že každý ireducibilní polynom z $R[x]$ je lineární.

"(c) $\Rightarrow$ (a)" : nechť $f \in R[x]$, $st\,(f) \geq 1$. Provedeme-li podle V.5.4. rozklad polynomu f na ireducibilní polynomy

$$f = p_1 \ldots . p_r$$

pak podle (c) jsou polynomy p_i lineární. Vezmeme-li libovolný z nich, např. p_1, pak p_1 má v R kořen (a to jediný, podle poznámky za V.3.1.), který je zřejmě také kořenem polynomu f] .

Věta 5.6.: *Nechť R je algebraicky uzavřené těleso. Pak každý polynom $f \in R[x]$, $st\,(f) = n \geq 1$ má v R právě n kořenů, počítáme-li každý kořen tolikrát, kolik je jeho násobnost.*

[D ů k a z : podle části (b) předchozí věty lze polynom f napsat jako součin lineárních polynomů, kterých však musí být právě n (vzhledem k důsledku V.1.2.) a každý z nich má v R právě jeden kořen, který je zároveň kořenem f. Odtud pak užitím definice násobného kořene plyne tvrzení.].

Vidíme, že z nejběžněji používaných těles např. tělesa R a Q nejsou algebraicky uzavřena (neboť např. polynom $f = x^2 + 1$ zřejmě nemá žádný kořen v R ani v Q). Rovněž tělesa zbytkových tříd Z_p (p prvočíslo) nejsou algebraicky uzavřena, jak plyne z následující věty.

Věta 5.7.: *Nechť R je konečné těleso (t. zn. R má konečně mnoho prvků). Pak těleso R není algebraicky uzavřené.*

[D ů k a z : nechť R je těleso o n prvcích ($n \geq 2$), kde $R = \{a_1, \ldots, a_n\}$. Pak polynom :

$$f = (x-a_1)(x-a_2) \ldots (x-a_n) + 1$$

zřejmě patří do $R[x]$, platí $st\,(f) \geq 1$ a při tom f nemá v R žádný kořen, neboť $f(a_i) = 1 \neq 0$, pro každé $a_i \in R$].

§ 6 : DERIVACE POLYNOMU, TAYLORŮV ROZVOJ, HORNEROVO SCHEMA

ÚMLUVA : všude v tomto paragrafu předpokládáme, že R značí těleso charakteristiky 0.

Definice : *Nechť* $f \in R[x]$, *kde*

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n \tag{1}$$

Pak derivací polynomu f *rozumíme polynom* $f' \in R[x]$, *definovaný vztahem :*

$$f' = \begin{cases} o & \text{je-li } st(f) \leqslant 0 \\ a_1 + 2a_2 x + \ldots + n.a_n.x^{n-1} & \text{je-li } st(f) \geqslant 1 \end{cases} \tag{2}$$

Poznámka : pojem derivace polynomu známe z matematické analýzy, kde je definován jako jistá funkční limita. V algebře zřejmě tímto způsobem postupovat nemůžeme, neboť pojem limity je vázán na těleso R reálných čísel, resp. po jistých rozšířeních ještě na těleso K komplexních čísel. Zavádíme tedy pojem derivace ryze formálním způsobem a čistě algebraickými prostředky. Nicméně je vidět, že pro $R = R$ oba pojmy splývají a lze tedy očekávat, že i některé základní vlastnosti derivace budou zde stejné, jak nakonec v dalším ukážeme.

Věta 6.1. : *Nechť* $f \in R[x]$; $st\ (f) = n \geqslant 1$. *Pak derivace* f' *je polynom stupně* $n-1$.

[D ů k a z : je-li f tvaru (1), kde $a_n \neq 0$, pak vzhledem k tomu, že R je charakteristiky nula, je $n.a_n \neq 0$ a tedy $st\ (f') = n - 1$].

Poznámka : Samotnou definici derivace by zřejmě bylo možné stejným způsobem jako výše vyslovit i pro polynomy nad tělesem libovolné charakteristiky. V takovém případě by však nebyly splněny základní vlastnosti, které na derivaci obvykle požadujeme, např. neplatila by předchozí věta (nad tělesem R charakteristiky p, kde p je prvočíslo, by pak derivací polynomu $f = x^p + 1$ byl nulový polynom, i když $st\ (f) = p > 1$). Vidíme tedy, že podstatnou roli v našich úvahách bude hrát předpoklad, že těleso R je charakteristiky 0.

Věta 6.2. : *Pro polynomy z* $R[x]$ *a jejich derivace platí :*

1. $(f+g)' = f' + g'$
2. $(f_1 + \ldots + f_k)' = f_1' + \ldots + f_k'$
3. $(f.g)' = f'.g + f.g'$
4. $(f_1 . \ldots . f_k)' = f_1' . f_2 . \ldots . f_k + \ldots + f_1 . \ldots . f_{k-1} . f_k'$
5. $(f^k)' = k . f' . f^{k-1}$

[D ů k a z : část 1. a 3. se dokáže bezprostředním rozepsáním z definice derivace ; část 2, resp. 4. plyne z 1. resp. 3. užitím matematické indukce a část 5. je přímým důsledkem 4. Pro ilustraci si dokažme 3. část věty :

ad 3 : nechť $f = a_0 + a_1 x + \ldots + a_n x^n = \sum_{s=0}^{n} a_s . x^s$, t.j. $f' = \sum_{s=1}^{n} s.a_s . x^{s-1}$.

$$g = b_0 + b_1 x + \ldots + b_m x^m = \sum_{t=0}^{m} b_t . x^t \text{ , t.j. } g' = \sum_{t=1}^{m} t.b_t . x^{t-1}$$

Potom :

$$f'.g + f.g' = \sum_{s=1}^{n} s.a_s . x^{s-1} . \sum_{t=0}^{m} b_t . x^t + \sum_{s=0}^{n} a_s . x^s . \sum_{t=1}^{m} t.b_t . x^{t-1} = \sum_{l=1}^{m+n} \Big(\sum_{s+t=l} (s+t).a_s b_t \Big) . x^{s+t-1} =$$

$$= \sum_{l=1}^{m+n} \Big(\sum_{s+t=l} l.a_s . b_t \Big) . x^{l-1}$$

Dále :

$$f.g = \sum_{l=0}^{m+n} \Big(\sum_{s+t=l} a_s . b_t \Big) . x^l \text{ , t. zn. } (f.g)' = \sum_{l=1}^{m+n} l \Big(\sum_{s+t=l} a_s . b_t \Big) . x^{l-1}$$

odkud je vidět, že platí dokazovaná rovnost].

Poznámka : obvyklým induktivním způsobem definujeme *derivace vyšších řádů* daného polynomu $f \in R[x]$, tvaru (1).

Je-li k přirozené číslo, pak definujeme $(k+1)$-ní derivaci polynomu f jako polynom :

$$f^{(k+1)} := (f^{(k)})'$$

při čemž pro $k = 1$ platí (2).

Pak zřejmě pro $k \leqslant n$ má k-tá derivace polynomu (1) tvar :

$$f^{(k)} = k.(k-1) \ldots 2.1.a_k + (k+1).k \ldots 2.a_{k+1} . x + \ldots + n.(n-1) \ldots (n-k+1).a_n . x^{n-k}$$

resp. pro $k > n$ je $f^{(k)} = o$.

Definice : *Nechť* $f(x) \in R[x]$; $c \in R$. *Je-li*

$$f(x) = a_0 + a_1(x-c) + a_2(x-c)^2 + \ldots + a_n(x-c)^n \quad ; a_i \in R \tag{3}$$

pak pravou stranu (3) *nazýváme* T a y l o r ů v r o z v o j o s t ř e d u c p o l y n o m u f .

Věta 6.3.: *Nechť* $f \in R[x]$, $st\,(f) = n \geq 1$; *nechť* $c \in R$.
Pak existuje právě jeden Taylorův rozvoj o středu c *polynomu* f , *a sice :*

$$f(x) = f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \ldots + \frac{f^{(n)}(c)}{n!}(x-c)^n \tag{4}$$

[D ů k a z : I. existence :

Proveďme opakované dělení lineárním polynomem $(x-c)$ takto :

$$\left\{\begin{array}{l} f = (x-c).q_1 + a_0 \\ q_1 = (x-c).q_2 + a_1 \\ \cdot \\ \cdot \\ \cdot \\ q_{n-2} = (x-c).q_{n-1} + a_{n-2} \\ q_{n-1} = (x-c).q_n + a_{n-1} \end{array}\right. \tag{5}$$

kde zřejmě $a_0, a_1, \ldots, a_{n-1}$ jsou konstanty, resp. $q_1, \ldots, q_{n-1}, q_n$ jsou polynomy stupně $n-1, \ldots, 1, 0$. Tedy q_n je konstantní polynom, který označme symbolem a_n. Dále, v (5) vynásobme druhou rovnost polynomem $(x-c)$, třetí polynomem $(x-c)^2$, atd., až poslední rovnost polynomem $(x-c)^{n-1}$ a takto upravené je pak sečtěme.

Po úpravě dostáváme :

$$f = a_0 + a_1(x-c) + \ldots + a_{n-1}(x-c)^{n-1} + a_n(x-c)^n ,$$

což je Taylorův rozvoj (3).

II. jednoznačnost :

Nechť polynom f má Taylorův rozvoj (3). Pak postupným tvořením derivací

dostáváme :

$$f'(x) = a_1 + 2a_2(x-c) + \ldots + n.a_n(x-c)^{n-1}$$
$$f''(x) = 2a_2 + 3.2.a_3(x-c) + \ldots + n.(n-1).a_n(x-c)^{n-2}$$
$$\cdot$$
$$\cdot$$
$$\cdot$$
$$f^{(n)}(x) = n!\,a_n$$

Potom tedy : $f(c) = a_0$; $f'(c) = a_1$; $f''(c) = 2.a_2$, . . . , $f^{(n)}(c) = n!.a_n$,

odkud pak :

$a_0 = f(c)$, $a_1 = \frac{f'(c)}{1!}$, $a_2 = \frac{f''(c)}{2!}$, . . . , $a_n = \frac{f^{(n)}(c)}{n!}$, t. zn. (3) musí být tvaru (4).]

Poznámka : zavedeme-li novou proměnnou y vztahem :

$$y = x-c \qquad \text{neboli} \qquad x = y + c$$

pak lze vztah (4) přepsat do tvaru :

$$f(y+c) = f(c) + \frac{f'(c)}{1!}.y + \frac{f''(c)}{2!}.y^2 + \ldots + \frac{f^{(n)}(c)}{n!}.y^n \tag{6}$$

Tohoto obratu se často užívá při praktických výpočtech.

Při výpočtu koeficientů Taylorova rozvoje a i jinak je v praxi často potřeba provádět dělení daného polynomu f lineárním polynomem tvaru $(x-c)$, kde $c \in R$. Je tedy potřeba určit koeficienty podílu a zbytek tohoto dělení (který je zřejmě roven $f(c)$). Obě úlohy lze řešit jednoduše početním postupem nazvaným *Hornerovo schema.* Nechť je tedy $c \in R$ libovolné a $f(x) \in R[x]$, $st\,(f) = n \geq 1$, je tvaru :

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \tag{7}$$

kde $a_i \in R$, $a_n \neq 0$. Pak je :

$$f(x) = (x-c).q(x) + b \tag{8}$$

kde $b \in R$ a platí : $b = f(c)$. Navíc $st\,(q) = n-1$, t. zn. nechť

$$q(x) = b_{n-1}x^{n-1} + \ldots + b_1 x + b_0$$

Po dosazení za q do (8) a porovnání koeficientů v (7) a (8) dostáváme :

$$a_n = b_{n-1} \qquad b_{n-1} = a_n$$
$$a_{n-1} = b_{n-2} - c.b_{n-1} \qquad b_{n-2} = c.b_{n-1} + a_{n-1}$$

neboli

$$a_1 = b_0 - c.b_1 \qquad b_0 = c.b_1 + a_1$$
$$a_0 = b - c.b_0 \qquad b = c.b_0 + a_0$$

odkud jsou koeficienty podílu q i zbytek $b = f(c)$ jednoduše určeny. Při praktickém výpočtu budeme používat přehledné tabulky tvaru :

	a_n	a_{n-1}	. . . . .	a_1	a_0
c	$a_n = b_{n-1}$	$c.b_{n-1} + a_{n-1} = b_{n-2}$	. . . . .	$c.b_1 + a_1 = b_0$	$c.b_0 + a_0 = b = f(c)$

kde do horního řádku vypisujeme všechny koeficienty a_i ($n \geq i \geq 0$) polynomu f, tedy i případné nulové koeficienty a ve spodním řádku postupně vypočítáváme koeficienty b_i podílu a zbytek b.

Příklad 6.1.: V $R[x]$ dělte polynom $f(x) = 2x^5 - 18x^3 + 5x + 7$ polynomem $(x+3)$ a najděte $f(-3)$.

Řešení : užijeme Hornerova schematu pro $c = -3$

	2	0	−18	0	5	7
−3	2	−6	0	0	5	−8

tedy : $q(x) = 2x^4 - 6x^3 + 5$; resp. $f(-3) = -8$

Hornerova schematu s výhodou využíváme v celé řadě dalších úloh, na př. při hledání Taylorova rozvoje nebo hodnot derivací daného polynomu v daném bodě, jak ukazuje následující příklad.

Příklad 6.2 : V $K[x]$ nalezněte Taylorův rozvoj o středu $c = -i$ polynomu f, kde $f(x) = x^4 + (1+i)x^2 - 2x + (7+i)$

Řešení : opakovaným užitím Hornerova schematu, vzhledem k důkazu V.6.3. dostáváme :

	1	0	$1+i$	-2	$7+i$
$-i$	1	$-i$	i	-1	$7+2i = a_0$
$-i$	1	$-2i$	$-2+i$	$2i = a_1$	
$-i$	1	$-3i$	$-5+i = a_2$		
$-i$	1	$-4i = a_3$			
$-i$	$1 = a_4$				

Tedy je : $f(x) = (7+2i) + 2i(x+i) + (-5+i)(x+i)^2 - 4i(x+i)^3 + (x+i)^4$

Navíc, poněvadž $a_k = \frac{f^{(k)}(c)}{k!}$, můžeme ihned určit hodnoty všech derivací polynomu f v bodě $c = -i$.

Je pak : $f(-i) = 7+2i$; $f'(-i) = 2i$; $f''(-i) = -10+2i$, $f'''(-i) = -24i$, $f^{(4)}(-i) = 24$.

Na závěr paragrafu uveďme nyní některé výsledky, týkající se vzájemné souvislosti mezi kořenem, resp. jeho násobností a derivací daného polynomu.

Věta 6.4. : *Nechť $f \in R[x]$ a nechť $c \in R$ je k-násobným kořenem polynomu f.*

Je-li $k = 1$, pak c není kořenem f'

je-li $k > 1$, pak c je $(k-1)$-násobným kořenem f'.

[D ů k a z : podle předpokladu a podle V.3.3. existuje polynom $h(x) \in R[x]$ takový, že :

$$f(x) = (x-c)^k . h(x) \quad , \quad \text{při čemž } h(c) \neq 0$$

Pak je : $f'(x) = k.(x-c)^{k-1}.h(x) + (x-c)^k.h'(x)$, t. zn. po úpravě :

(9) $$f'(x) = (x-c)^{k-1}.[k.h(x) + (x-c).h'(x)]$$

Nechť $k=1$; pak (9) nabývá tvaru : $f'(x) = h(x) + (x-c).h'(x)$, t. zn. $f'(c) = h(c) \neq 0$, a tedy c není kořenem f'.

Nechť $k > 1$, pak označme $t(x) = k.h(x) + (x-c).h'(x)$. Při tomto označení dostáváme podle (9) : $f'(x) = (x-c)^{k-1}.t(x)$, při čemž $t(c) = k.h(c) \neq 0$ a tedy podle V.3.3. je c $(k-1)$ - násobným kořenem polynomu f'].

Poznámka : obrácení předchozí věty zřejmě neplatí; je-li např. $f(x) = x^3+1 \in R[x]$, pak $f'(x) = 3x^2$. Tedy 0 je dvojnásobným kořenem f', ale není vůbec kořenem f.

Věta 6.5 : *Nechť $f(x) \in R[x]$; $c \in R$; nechť $k > 1$ je přirozené číslo. Pak : c je k-násobným kořenem $f(x) \Leftrightarrow c$ je $(k-1)$-násobným kořenem polynomu (f, f').*

[D ů k a z : "⇒" : nechť c je k-násobným kořenem f, kde $k > 1$. Pak podle předchozí věty je prvek c $(k-1)$-násobným kořenem f'. Tedy platí : $(x-c)^k \mid f$, $(x-c)^{k+1} \nmid f$, $(x-c)^{k-1} \mid f'$, $(x-c)^k \nmid f'$, odkud dostáváme, že $(x-c)^{k-1} \mid (f, f')$. Dále sporem ; nechť $(x-c)^k \mid (f, f')$. Ale $(f, f') \mid f'$ a z tranzitivity relace dělitelnosti pak plyne, že $(x-c)^k \mid f'$, což je spor. Tedy musí být $(x-c)^k \nmid (f, f')$ a dohromady dostáváme, že c je $(k-1)$-násobným kořenem polynomu (f, f').

"⇐" : nechť c je $(k-1)$-násobným kořenem (f, f'), t. zn. $(x-c)^{k-1} \mid (f, f')$; $(x-c)^k \nmid (f, f')$. Kdyby $(x-c)^k \mid f$, pak by tedy c bylo $(k-1)$-násobným kořenem polynomu f, t. zn. podle V.6.4. $(x-c)^{k-1} \mid f'$, což je spor. Tedy platí: $(x-c)^k \mid f$. Dále, je-li $(x-c)^{k+1} \mid f$, pak c je alespoň $(k+1)$-násobným kořenem polynomu f, t. zn. podle V.6.4. je c alespoň k-násobným kořenem polynomu f', t. zn. $(x-c)^k \mid f'$. Výše jsme však dokázali, že $(x-c)^k \mid f$, t. zn. dohromady pak dostáváme, že $(x-c)^k \mid (f, f')$, což je spor s předpokladem. Je tedy $(x-c)^{k+1} \nmid f$ a dohromady tedy dostáváme, že c je k-násobný kořen f].

Věta 6.6. : *Nechť $f \in R[x]$; $c \in R$; nechť k je přirozené číslo. Pak platí : c je k-násobným kořenem polynomu $f \Leftrightarrow f(c) = f'(c) = \ldots = f^{(k-1)}(c) = 0$; $f^{(k)}(c) \neq 0$*

[D ů k a z : "⇒" : je-li prvek c k-násobným kořenem f, pak je $f(c) = 0$. Opakovaným užitím V.6.4. pak dostaneme žádané tvrzení, neboť podle V.6.4. je c $(k-1)$-násobným kořenem f', t. zn. $f'(c) = 0$, atd., až c je jednoduchým kořenem $f^{(k-1)}$, t. zn. $f^{(k-1)}(c) = 0$ a c není kořenem $f^{(k)}$, t. zn. $f^{(k)}(c) \neq 0$.

"⇐" : nechť $f(c) = f'(c) = \ldots = f^{(k-1)}(c) = 0$; $f^{(k)}(c) \neq 0$. Nechť f je ve tvaru (1). Pak Taylorův rozvoj o středu c polynomu f má tvar :

$$f(x) = 0 + \ldots + 0 + \frac{f^{(k)}(c)}{k!}(x-c)^k + \ldots + \frac{f^{(n)}(c)}{n!}(x-c)^n$$

t. zn. :

$$f(x) = (x-c)^k \cdot \left[\frac{f^{(k)}(c)}{k!} + \ldots + \frac{f^{(n)}(c)}{n!}(x-c)^{n-k} \right]$$

při čemž zřejmě c není kořenem polynomu v hranaté závorce. Podle V.3.3. je pak prvek c k-násobným kořenem polynomu f.]

Poznámka : poslední větu spolu s Hornerovým schematem používáme k praktickému zjišťování násobnosti daného kořene c polynomu f. Z příkladu 6.2 je vidět, že při opakovaném dělení lineárním polynomem tvaru $(x-c)$ dostáváme jakožto zbytky hodnoty $a_k = \frac{f^{(k)}(c)}{k!}$. Podle předchozí věty je pak násobnost kořene c rovna počtu nulových zbytků těchto dělení.

Příklad 6.3. : Zjistěte, zda $c = 1-i$ je kořenem polynomu $f \in K[x]$ a pokud ano, určete jeho násobnost. Při tom : $f(x) = x^6 - 2x^5 + x^4 + 4x^3 - 4x^2 + 4$.

Řešení : podle předchozí poznámky opakovaně užijeme Hornerova schematu :

	1	-2	1	4	-4	0	4
$1-i$	1	$-1-i$	-1	$3+i$	$-2i$	$-2-2i$	0
$1-i$	1	$-2i$	$-3-2i$	$-2+2i$	$2i$	0	
$1-i$	1	$1-3i$	$-5-6i$	$-13+i$	$-12+16i \neq 0$		

Tedy číslo $c = 1-i$ je dvojnásobným kořenem polynomu f.

§ 7 : POLYNOMY NAD TĚLESEM KOMPLEXNÍCH ČÍSEL, ZÁKLADNÍ VĚTA ALGEBRY.

V tomto paragrafu budeme studovat základní vlastnosti polynomů s komplexními, resp. reálnými koeficienty. Připomeňme, že každé číselné těleso (specielně tedy K a R) je charakteristiky 0, t. zn. můžeme použít všech výsledků, dokázaných dříve v této kapitole.

Věta 7.1. ("Základní věta algebry ")
Každý polynom $f(x) \in K[x]$, stupně alespoň jedna, má v K alespoň jeden kořen.

[D ů k a z : neuvádíme.]

Poznámka : t. zv. základní věta algebry říká, že těleso K komplexních čísel je algebraicky uzavřené. Věta měla opravdu základní význam pro algebru v dobách, kdy se tato omezovala na algebru komplexních čísel. Její důkaz nelze provést čistě algebraickými prostředky a je vždy nutné v menší či větší míře využít topologických vlastností reálných a komplexních čísel (t.j. vlastností, souvisejících se spojitostí). Důvodem je to, že v samotné definici reálného čísla se vyskytují pojmy, které nejsou algebraické (pojem spojitého uspořádání). Poměrně jednoduchý důkaz V.7.1. bude uveden v základní přednášce o analytických funkcích.

Důsledek : Ireducibilními polynomy jsou v $K[x]$ právě lineární polynomy.

[D ů k a z : tvrzení je přímým důsledkem základní věty algebry a V.5.5.]

Věta 7.2.: *Nechť $f \in K[x]$, $st\,(f) = n \geq 1$ je polynom tvaru :*

(1) $$f = a_0 + a_1 x + \ldots + a_n x^n \quad , \quad a_n \neq 0$$

Pak platí :

1. *polynom f lze vyjádřit jako součin n lineárních normovaných polynomů a nenulové konstanty ve tvaru*

(2) $$f = a_n \cdot (x-c_1) \cdot \ldots \cdot (x-c_n) \; ; \; c_i \in K, \; i = 1, \ldots, n$$

2. *vyjádření* (2) *je jednoznačné, až na pořadí faktorů*

3. *polynom f má přesně n kořenů, počítáme-li každý kořen tolikrát, kolik je jeho násobnost.*

[D ů k a z : ad 1 : plyne ihned ze základní věty algebry a z V. 5.5.

ad 2 : plyne z V.5.4. vzhledem k tomu, že ireducibilními polynomy v $K[x]$ jsou právě lineární polynomy a že na pravé straně (1) vystupují normované polynomy.

ad 3 : plyne ze základní věty algebry a z V.5.6.]

Poznámka : ze vztahu (2) je vidět, že polynom f lze, po vhodném přečíslování hodnot c_i, přepsat do tvaru :

(3) $$f = a_n \cdot (x-c_1)^{i_1} \cdot (x-c_2)^{i_2} \cdot \ldots \cdot (x-c_r)^{i_r}$$

kde $c_1, \ldots, c_r$ jsou navzájem různá komplexní čísla a platí : $i_1 + i_2 + \ldots + i_r = n$. Je-li polynom f vyjádřen ve tvaru (3), pak z V.3.3. plyne, že c_k je i_k- násobným kořenem f, pro $k = 1, \ldots, r$.

Definice : *Vyjádření polynomu $f \in K[x]$ ve tvaru* (3) *se nazývá kanonický rozklad polynomu f.*

Věta 7.3.: *Nechť $f, g \in K[x]$ jsou polynomy, mající kanonický rozklad :*

$$f = a \cdot (x-c_1)^{i_1} \ldots (x-c_r)^{i_r}$$

$$g = b \cdot (x-d_1)^{j_1} \ldots (x-d_s)^{j_s}$$

Nechť $c_1 = d_1, \ldots, c_t = d_t$, resp. $c_{t+1}, \ldots, c_r, d_{t+1}, \ldots, d_s$ jsou navzájem různá čísla. Pak pro největší společný dělitel polynomů f a g platí :

$$(f,g) = (x-c_1)^{k_1} \ldots (x-c_t)^{k_t}$$

kde $k_1 = min\,(i_1, j_1), \ldots, k_t = min\,(i_t, j_t)$.

[D ů k a z : nechť platí označení, předpokládané ve větě. Označme dále :

$$h = (x-c_1)^{k_1} \ldots (x-c_t)^{k_t}$$

Zřejmě je : $h \mid f$; $h \mid g$, t. zn. h je společným dělitelem polynomů f a g. Dokážeme, že h je největším společným dělitelem f a g. Nechť tedy $q \in K[x]$ je polynom, pro nějž je $q \mid f$, $q \mid g$ a nechť kanonický rozklad polynomu q je tvaru :

$$q = p \,.\, (x-e_1)^{u_1} \,.\, \ldots \,.\, (x-e_m)^{u_m} \,.$$

Pak ale $(x-e_1)^{u_1} \mid f$, $(x-e_1)^{u_1} \mid g$, t. zn. e_1 musí být rovno některému společnému kořenu polynomů f a g, řekněme, že $e_1 = c_1$. Přitom však $u_1 \leqslant i_1$, $u_1 \leqslant j_1$, t. zn. $u_1 \leqslant min\,(i_1 j_1) = k_1$. Analogicky pro $e_2, \ldots, e_m$, což však znamená, že $q \mid h$. Dohromady pak dostáváme, že $h = (f,g)$.]

Poznámka : známe-li všechny kořeny i s násobnostmi dvou polynomů z $K[x]$, pak největší společný dělitel těchto polynomů zjistíme podle V.7.3. prakticky okamžitě a nemusíme používat pracného výpočtu Eukleidovým algoritmem. V praxi však obvykle kořeny daného polynomu neznáme a jejich nalezení bývá většinou velmi pracné a obtížné a v obecném případě algoritmicky neřešitelné. Následující věty pomohou tyto problémy řešit alespoň částečně, využitím vlastností násobných kořenů, resp. vztahů mezi kořeny a koeficienty daného polynomu.

Věta 7.4.: *Nechť T je číselné těleso, $f \in T[x]$, $st\,(f) \geqslant 1$. Nechť dále $q \in T[x]$ je polynom splňující :*

$$f = (f,f')\,.\,q \tag{4}$$

Pak polynom q má stejné kořeny jako polynom f, ale každý pouze jednoduchý.

[D ů k a z : z Eukleidova algoritmu a z konstrukce dělení polynomů se zbytkem plyne, že polynom q splňující (4) existuje, při čemž $(f,f'), q \in T[x]$. Polynom f můžeme zřejmě uvažovat jako polynom nad K. Nechť pak kanonický rozklad polynomu f ma tvar (3), t. zn.

$$f = a_n \,.\, (x-c_1)^{i_1} \,.\, \ldots \,.\, (x-c_r)^{i_r} \,.$$

Pak z V.6.4. plyne, že :

- je-li $i_k = 1$, pak c_k není kořenem derivace f', resp.
- je-li $i_k > 1$, pak c_k je (i_k-1)-násobným kořenem f',

odkud podle předchozí věty dostáváme :

$$(f,f') = (x-c_1)^{i_1-1} \,.\, \ldots \,.\, (x-c_r)^{i_r-1}$$

kde faktorem s nulovým exponentem rozumíme číslo 1. Potom tedy zřejmě :

$$q = a_n \,.\, (x-c_1) \,.\, \ldots \,.\, (x-c_r), \tag{5}$$

t. zn. polynom q má požadovanou vlastnost.]

Důsledek : Nechť T je číselné těleso, nechť polynom $f \in T[x]$ je ireducibilním polynomem nad T.

Pak polynom f má pouze jednoduché kořeny (v K).

[D ů k a z : je-li $st\,(f) = 1$, pak polynom f má jediný kořen a tvrzení platí. Nechť tedy $st\,(f) = n \geqslant 2$ a nechť f uvažovaný jako polynom nad K má kanonický rozklad tvaru (3). Nechť q je polynom z předchozí věty, splňující :

$f = (f,f') \,.\, q$, kde $(f,f'), q \in T[x]$.

Poněvadž je však $st\,(f,f') < n$, pak z ireducibility f plyne, že musí být $st\,(f,f') = 0$, t. zn. $(f,f') = 1$. Pak ale $f = q$, t. zn. f je tvaru (5), odkud plyne tvrzení.]

Příklad 7.1. : Využitím vlastností násobných kořenů nalezněte kořeny (i s jejich násobnostmi) polynomu $f \in R[x]$, kde : $f = x^5 + x^4 - 5x^3 - x^2 + 8x - 4$.

Řešení : k výpočtu užijeme tvrzení V.7.4. Uvažme derivaci $f' = 5x^4 + 4x^3 - 15x^2 - 2x + 8$ a pomocí Eukleidova algoritmu vypočítáme největší společný dělitel polynomů f a f'. Po výpočtu (ve dvou krocích) vyjde : $(f,f') = x^3 - 3x + 2$.

Nyní vydělením polynomu f polynomem (f,f') obdržíme polynom q z V.7.4. (zajímá nás podíl tohoto dělení, a proto během výpočtu nelze násobit nenulovými prvky z R jako u Eukleidova algoritmu !).

$$(x^5 + x^4 - 5x^3 - x^2 + 8x - 4) \,:\, (x^3 - 3x + 2) \mid x^2 + x - 2$$

$$\begin{array}{l} -x^5 \mp 3x^3 \pm 2x^2 \\ \hline x^4 - 2x^3 - 3x^2 + 8x - 4 \\ -x^4 \mp 3x^2 \pm 2x \\ \hline -2x^3 + 6x - 4 \\ \mp 2x^3 \pm 6x \mp 4 \\ \hline 0 \end{array}$$

Tedy $q = x^2 + x - 2 = (x-1)(x+2)$, t. zn. polynom f má dva kořeny : $c_1 = 1$, $c_2 = -2$. Jejich násobnosti zjistíme Hornerovým schematem, při čemž zde vyjde, že $c_1 = 1$ je trojnásobný, resp. $c_2 = -2$ je dvojnásobný kořen polynomu f.

Poznámka : Věta 7.4 zřejmě neposkytuje universální algoritmus pro výpočet kořenů daného polynomu f. Má-li např. polynom f pouze jednoduché kořeny (pak $q = f$), nebo je-li polynom q příliš vysokého stupně, pak je V.7.4. pro výpočet kořenů polynomu f neúčinná.

Věta 7.5.: *Nechť* $f \in K[x]$, *st* $(f) = n \geq 1$, *kde*

$$f = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1} + a_n x^n$$

a nechť $c_1, \ldots, c_n$ *jsou kořeny polynomu* f.

Pak platí :

$$(6) \quad \begin{cases} -\frac{a_{n-1}}{a_n} = c_1 + \ldots + c_n \\ \frac{a_{n-2}}{a_n} = c_1c_2 + c_1c_3 + \ldots + c_1c_n + c_2c_3 + \ldots + c_{n-1}c_n \\ \cdots \\ (-1)^k \frac{a_{n-k}}{a_n} = \sum_{i_1 < \ldots < i_k} c_{i_1} c_{i_2} \ldots c_{i_k} \\ \cdots \\ (-1)^n \frac{a_0}{a_n} = c_1 . c_2 . \ldots . c_n \end{cases}$$

[D ů k a z : polynom f vyjádříme podle V.7.2. ve tvaru (2), tj. jako součin lineárních polynomů. Pak :

$$f = a_n(x-c_1)(x-c_2)\ldots(x-c_n) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} + a_n x^n$$

Porovnáním koeficientů u jednotlivých mocnin x dostáváme pak přímo vztahy (6)].

Příklad 7.2. : V $K[x]$ nalezněte normovaný polynom f, který má za kořeny trojnásobky kořenů polynomu $h = x^3 + 5x + 2$.

Řešení : polynom h má v K právě 3 kořeny, které označme c_1, c_2, c_3 : Pak zřejmě f bude tvaru $f = x^3 + Ax^2 + Bx + C$, kde $A,B,C \in K$. Při tom, podle zadání, f má kořeny : $3c_1, 3c_2, 3c_3$. Ze (6) pak plyne :

$0 = c_1 + c_2 + c_3$ $\qquad -A = 3c_1 + 3c_2 + 3c_3 = 3.(c_1+c_2+c_3) = 3.0 = 0$

$5 = c_1c_2 + c_1c_3 + c_2c_3$ resp. $\qquad B = 3c_1.3c_2 + 3c_1.3c_3 + 3c_2.3c_3 =$

$\qquad = 9.(c_1c_2 + c_1c_3 + c_2c_3) = 9.5 = 45$

$-2 = c_1.c_2.c_3$ $\qquad -C = 3c_1.3c_2.3c_3 = 27 . (c_1c_2c_3) = 27.(-2) = -54$

Tedy hledaný polynom je tvaru : $f = x^3 + 45x + 54$.

Nyní si všimneme některých specifických vlastností těch polynomů z $K[x]$, jejichž koeficienty jsou reálná čísla. Je-li $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ takový polynom, pak jej můžeme chápat jako komplexní funkci, jak plyne ze závěru §3. Budeme-li dále komplexně sdružené číslo k číslu $z \in K$ označovat symbolem $\overline{z}$, pak užitím známých vlastností komplexně sdružených čísel dostáváme :

$$\overline{f(x)} = \overline{a_0 + a_1 x + \ldots + a_n x^n} = a_0 + a_1 \overline{x} + \ldots + a_n \overline{x}^n = f(\overline{x}) \ ,$$

protože a_i jsou reálná čísla, t. zn. je $\overline{a_i} = a_i$.

Věta 7.6. : *Nechť* $f(x) \in K[x]$ *je polynom s reálnými koeficienty a nechť* c *je* k*-násobným kořenem polynomu* f.

Pak také číslo $\overline{c}$ *je* k*-násobným kořenem polynomu* f.

[D ů k a z : nechť $f(x) = a_n.(x-c_1)^{i_1} \ldots (x-c_r)^{i_r}$ je kanonický rozklad polynomu f. Přechodem ke komplexně sdruženým číslům dostáváme :

$$f(\overline{x}) = \overline{f(x)} = a_n.(\overline{x}-\overline{c}_1)^{i_1} \ldots (\overline{x}-\overline{c}_r)^{i_r}$$

Ale tento vztah platí pro každé komplexní číslo x ; můžeme tedy $\overline{x}$ zaměnit za x a dostáváme :

$$f(x) = a_n . (x-\overline{c}_1)^{i_1} \ldots (x-\overline{c}_r)^{i_r}$$

odkud již plyne tvrzení věty.]

Poznámka : z předchozí věty m.j. plyne, že polynom z $K[x]$, s reálnými koeficienty, musí mít vždy sudý počet imaginarních kořenů. Je-li navíc lichého stupně, pak musí mít lichý počet reálných kořenů.

Dále se zabývejme otázkami ireducibility v $R[x]$. Již dříve jsme uvedli, že těleso R není algebraicky uzavřené, t. zn. , že v $R[x]$ existují ireducibilní polynomy stupně vyššího než I. Následující věta podává vyčerpávající charakterizaci ireducibilních polynomů v $R[x]$.

Věta 7.7. : *Ireducibilními polynomy v* $R[x]$ *jsou právě všechny lineární polynomy a všechny kvadratické polynomy se záporným diskriminantem.*

[D ů k a z : je-li $f(x) \in R[x]$ lineární polynom nebo kvadratický polynom se záporným diskriminantem, pak f je zřejmě ireducibilní v $R[x]$.

Naopak, nechť $f \in R[x]$ je ireducibilní polynom nad R. Pak *st* $(f) \geq 1$.

Předpokládejme, že polynom f není lineární. Polynom f pak nemá žádný reálný kořen, ale musí mít imaginární kořen, který označme $c = a + bi$ $(b \neq 0)$. Podle V.7.6. je však kořenem f rovněž číslo $\overline{c} = a - bi$. Protože je $c \neq \overline{c}$, je polynom f v $K[x]$ dělitelný polynomem :

$$f_0 = (x-c) \cdot (x-\overline{c}) = x^2 + 2ax + (a^2 + b^2)$$

Zřejmě je však $f_0 \in R[x]$ a tedy $f_0 \mid f$ v $R[x]$, jak plyne z algoritmu dělení se zbytkem. Podle předpokladu je však polynom f ireducibilní v $R[x]$, t. zn. je $f_0 \sim f$ v $R[x]$. Existuje tedy reálné číslo $r \neq 0$ tak, že :

$$f = r \cdot f_0$$

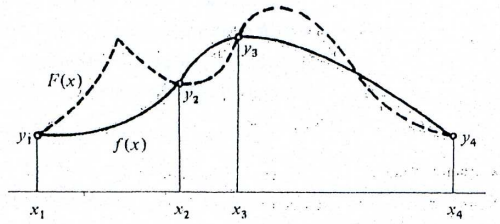
Tedy f je kvadratický polynom, jehož diskriminant $D = 4a^2r^2 - 4.r.r.(a^2+b^2) = -4r^2b^2$ je záporný, c.b.d.]

Důsledek : 1. Každý reálný polynom, t.j. polynom z $R[x]$, stupně alespoň 3, je nad tělesem R reducibilní.

2. Každý reálný polynom f lze vyjádřit jako součin reálného čísla a konečného počtu reálných normovaných lineárních polynomů a reálných normovaných kvadratických polynomů se zápornými diskriminanty. Je-li $f \neq o$, , pak je toto vyjádření jednoznačné, až na pořadí činitelů.

[D ů k a z : tvrzení plyne ihned z předchozí věty, resp. 2. část ještě z V.5.4.]

V experimentálních oborech a v praxi vůbec se často setkáváme s úlohou najít (alespoň přibližně) funkci, např. $y = F(x)$, charakterizující nějaký děj, který pozorujeme nebo měříme. Znamená to, že pro konečný počet hodnot x jsou stanoveny (naměřeny) odpovídající hodnoty y. Funkci $F(x)$ přesně neznáme, a proto ji nahrazujeme funkcí jednodušší, obvykle polynomem $f(x)$, po němž požadujeme, aby se v daných hodnotách x shodoval s hledanou funkcí přesně, v ostatních hodnotách pak přibližně (viz obrázek). Říkáme, že provádíme *interpolaci* nebo též, že funkci $F(x)$ aproximujeme polynomem $f(x)$. Polynom $f(x)$ se pak nazývá *interpolační polynom.*



V dalším se na problém interpolace podíváme čistě algebraicky jako na úlohu nad libovolným číselným tělesem T (jehož specielním případem je samozřejmě i těleso reálných čísel). Zcela stranou ponecháváme otázky, související s přesností takovéto aproximace.

Věta 7.8. : *Nechť T je číselné těleso, nechť $f,g \in T[x]$; $st(f), st(g) \leqslant n$, kde n je pevné přirozené číslo.*
Jestliže f, g nabývají stejných hodnot v alespoň $(n+1)$ různých bodech, pak je $f = g$.

[D ů k a z : nechť $c_1, \ldots, c_{n+1} \in T$ jsou navzájem různá čísla, při čemž $f(c_i) = g(c_i)$, $i = 1, \ldots, n+1$.
Uvažme polynom $h = f - g$. Zřejmě je $st(h) \leqslant n$, při čemž h má alespoň $(n+1)$ různých kořenů. Podle V.7.2. (část 3) však nemůže být $st(h) \geqslant 1$. Zřejmě také $st(h) \neq 0$. Tedy musí být $st(h) = -\infty$, t. zn. $h = o$, odkud dostáváme $f = g$] .

Věta 7.9. : *Nechť T je číselné těleso, nechť $c_1, \ldots, c_{n+1} \in T$ jsou navzájem různá čísla, resp. $y_1, \ldots, y_{n+1} \in T$ jsou libovolná čísla.*
Pak existuje právě jeden polynom $f \in T[x]$ takový, že $st(f) \leqslant n$ a platí :
$f(c_i) = y_i$, $i = 1, \ldots, n+1$.

[D ů k a z : 1. existence :

zvolme $f(x)$ takto :

$$(7)\quad f(x) = y_1 \cdot \frac{(x-c_2)(x-c_3)\cdot\ldots\cdot(x-c_{n+1})}{(c_1-c_2)(c_1-c_3)\cdot\ldots\cdot(c_1-c_{n+1})} + y_2 \cdot \frac{(x-c_1)(x-c_3)\cdot\ldots\cdot(x-c_{n+1})}{(c_2-c_1)(c_2-c_3)\cdot\ldots\cdot(c_2-c_{n+1})} +$$

$$+ \ldots\ldots + y_{n+1} \cdot \frac{(x-c_1)\cdot(x-c_2)\cdot\ldots\cdot(x-c_n)}{(c_{n+1}-c_1)(c_{n+1}-c_2)\cdot\ldots\cdot(c_{n+1}-c_n)}$$

Pak zřejmě $f(x) \in T[x]$, $st\,(f) \leqslant n$ (neboť každý sčítanec je buď o nebo polynom stupně n) a dosazením dostáváme $f(c_i) = y_i$, $i = 1, \ldots, n+1$

II. jednoznačnost :

plyne přímo z V.7.8.]

Poznámka : vyjádření polynomu f ve tvaru (7) se nazývá *Lagrangeův tvar interpolačního polynomu.*

I když V.7.9. dokazuje jednoznačnost interpolačního polynomu f, můžeme zřejmě tento polynom formálně rozepsat různými způsoby, např. podle toho, jak je to pro naše konkretní účely výhodné. Na základě následující věty ukážeme ještě jednu možnost zápisu interpolačního polynomu.

Věta 7.10. : *Nechť T je číselné těleso, nechť $c_1, \ldots, c_n \in T$. Pak polynom $f = a_0 + a_1 x + \ldots + a_n x^n \in T[x]$ lze vyjádřit ve tvaru :*

$$(8)\quad f(x) = b_0 + b_1(x-c_1) + b_2(x-c_1)(x-c_2) + \ldots + b_n(x-c_1)(x-c_2)\ldots\ldots(x-c_n).$$

[D ů k a z : postupným dělením polynomu f, resp. částečných podílů, lineárními polynomy tvaru $(x-c_i)$, $i = 1, \ldots, n$ dostáváme :

$f = b_0 + (x-c_1)\,q_1 = b_0 + (x-c_1)\cdot[b_1 + (x-c_2)\,q_2\,] = b_0 + b_1(x-c_1) +$

$+ (x-c_1)\cdot(x-c_2)\cdot q_2 = \ldots\ldots = b_0 + b_1(x-c_1) + \ldots + b_n(x-c_1)\cdot\ldots\cdot\ldots\cdot(x-c_n)$, což je žádaný tvar.]

Mějme nyní zadána navzájem různá čísla $c_1, \ldots, c_{n+1} \in T$ a jim odpovídající hodnoty $f(c_1), \ldots, f(c_{n+1})$. Těmito hodnotami jednoznačně určený polynom f z věty 7.9. lze na základě předchozí věty vyjádřit ve tvaru (8). Koeficienty $b_0, b_1, \ldots, b_n$ při tom získáme postupným dosazováním hodnot c_i (i=1, ..., n+1) za x do vztahu (8). Takto získané vyjádření polynomu f ve tvaru (8) se pak nazývá *Newtonův tvar interpolačního polynomu.*

Připomeňme ještě, že každý z obou zmiňovaných tvarů interpolačního polynomu má v praxi svoje výhody i nevýhody. Lagrangeův tvar je možné okamžitě napsat, ovšem při zvýšení n (t.j. např. při zvětšení počtu měření) je nutné jej celý znovu sestavit. Na druhé straně, u Newtonova tvaru je nutno počítat koeficienty b_i, ovšem při zvětšení n se pouze přidá jeden člen, při zachování všech členů předchozích.

§ 8 : POLYNOMY NAD OKRUHEM RACIONÁLNÍCH ČÍSEL A NAD OKRUHEM CELÝCH ČÍSEL.

V tomto paragrafu budeme nejprve studovat ireducibilitu polynomů nad Q a nad Z. Předem je ovšem nutné opět připomenout, že Z není tělesem, ale pouze oborem integrity (který má dvě jednotky, a to čísla +1, −1, t. zn. k polynomu $f \in Z[x]$ jsou asociovány právě polynomy f a $-f$), a tedy v $Z[x]$ nemůžeme obecně použít ty definice a věty, v nichž se předpokládalo, že R je těleso. Specielně tedy pro $Z[x]$ nelze použít definici reducibilního polynomu, uvedenou v § 5, nýbrž je třeba vzít obecnou definici z § 2 kapitoly I, podle níž polynom $f \in Z[x]$ je reducibilní (resp. ireducibilní) nad Z, jestliže $f \neq o$, $f \neq \pm 1$, přičemž f má (resp. nemá) vlastní dělitele, t.j. dělitele různé od ± 1 a od $\pm f$.

V dalším pak ukážeme, že ireducibilita nad Z a nad Q spolu velmi úzce souvisí, i když oba pojmy samozřejmě obecně nesplývají; na př. polynom

$$f(x) = 3x + 6 = 3.(x + 2)$$

je zřejmě ireducibilní nad Q (viz příklad 5.1), ale nad Z je reducibilní.

Definice : *Polynom $f = a_0 + a_1 x + \ldots + a_n x^n$, s celočíselnými koeficienty, se nazývá p r i m i t i v n í, jestliže jeho koeficienty jsou nesoudělné, t. zn. $(a_0, a_1, \ldots, a_n) = 1$.*

Věta 8.1. : *Nechť $f = a_0 + a_1 x + \ldots + a_n x^n \in Z[x]$ je libovolný nenulový polynom. Potom :*

1. *polynom f lze vyjádřit ve tvaru :*

$$(1)\qquad f = z \cdot f^*$$

kde $z \in Z$ *a* f^* *je primitivní polynom.*

2. *vyjádření* (1) *je jednoznačné až na asociovanost, t. zn. je-li*

(2) $$f = z \cdot f^* = z_1 \cdot f_1^*$$

kde $z, z_1 \in Z$ *a* f^*, f_1^* *jsou primitivní polynomy, pak* z, z_1 *jsou asociovány v* Z *a* f^*, f_1^* *jsou asociovány v* $Z[x]$.

[Důkaz: ad 1: symbolem z označme největší společný dělitel (v Z) všech koeficientů polynomu f, t. zn. $z = (a_0, a_1, \ldots, a_n)$. Koeficienty polynomu f^* pak obdržíme z příslušných koeficientů polynomu f vydělením číslem z. Zřejmě pak je f^* primitivní a platí (1).

ad 2: nechť platí (2), kde $z, z_1 \in Z$ a f^*, f_1^* jsou primitivní polynomy. Pak ale $z_1 \mid a_i$ pro $i = 0, 1, \ldots, n$, t. zn. také $z_1 \mid (a_0, a_1, \ldots, a_n) = z$. Nechť tedy $z = z_1 c$, kde $c \in Z$. Po dosazení: $z_1 c f^* = z_1 f_1^*$, t. zn. $c f^* = f_1^*$ a tedy číslo c dělí všechny koeficienty polynomu f_1^*, který je však primitivní. Pak ale $c = \pm 1$, t. zn. $z = \pm z_1$, resp. $f_1^* = \pm f^*$, což je žádané tvrzení].

Věta 8.2.: *('Gaussovo lemma')*

Nechť $f, g \in Z[x]$ *jsou primitivní polynomy. Pak jejich součin* $f \cdot g$ *je také primitivním polynomem.*

[Důkaz provedeme sporem, t. zn. nechť f, g jsou primitivní a předpokládejme, že $f \cdot g$ není primitivní polynom. Pak ale existuje prvočíslo p, které dělí všechny koeficienty součinu $f \cdot g$.

Označme: $$f = a_0 + a_1 x + \ldots + a_n x^n$$
$$g = b_0 + b_1 x + \ldots + b_m x^m$$

Vzhledem k předpokladu, p nedělí všechny koeficienty polynomu f resp. polynomu g. Nechť tedy a_r, resp. b_s je koeficient polynomu f, resp. g s nejmenším indexem, který není dělitelný číslem p.

Dále označme koeficient u mocniny x^{r+s} polynomu $f \cdot g$ symbolem c. Pak:

$$c = a_0 \cdot b_{r+s} + \ldots + a_r b_s + \ldots + a_{r+s} \cdot b_0 \quad , \quad \text{t. zn.}$$

(3) $$a_r \cdot b_s = c - a_0 \cdot b_{r+s} \ldots - a_{r-1} b_{s+1} - a_{r+1} b_{s-1} - \ldots - a_{r+s} b_0 \, .$$

Zřejmě p dělí každý člen na pravé straně rovnosti (3), t. zn. pak také $p \mid a_r \cdot b_s$. Podle předpokladu však $p \nmid a_r, p \nmid b_s$ a p je prvočíslo, t. zn: $p \nmid a_r \cdot b_s$, což je spor. Tedy polynom $f \cdot g$ je primitivní].

Důsledek: součin libovolného konečného počtu primitivních polynomů je primitivní polynom.

[Důkaz: tvrzení plyne z Gaussova lemmatu užitím matematické indukce].

Poznámka: je-li $g \in Q[x]$ libovolný polynom s racionálními koeficienty

$$g = \frac{a_0}{b_0} + \frac{a_1}{b_1} x + \ldots + \frac{a_n}{b_n} \cdot x^n \quad , \quad \text{kde } a_i, b_i \in Z$$

pak po vynásobení společným jmenovatelem $c = b_0 \cdot b_1 \ldots b_n$ můžeme psát: $g = c^{-1} \cdot h$, kde $h \in Z[x]$. Podle V.8.1. však existuje $d \in Z$ a primitivní polynom $h^* \in Z[x]$ tak, že $h = d \cdot h^*$. Dohromady tedy lze polynom $g \in Q[x]$ psát ve tvaru:

(4) $$g = c^{-1} \cdot d \cdot h^* \, , \quad \text{kde } c, d \in Z, \; h^* \in Z[x] \text{ je primitivní.}$$

Vyjádření (4) užijeme v následující větě, která charakterizuje ireducibilní polynomy nad Z.

Věta 8.3.: *Ireducibilními prvky v* $Z[x]$ *jsou právě tyto polynomy:*
- *všechny ireducibilní prvky v* Z
- *všechny primitivní polynomy stupně alespoň 1, které jsou ireducibilní nad polem* Q *racionálních čísel.*

[Důkaz: je-li $f \in Z[x]$, $st(f) \geq 1$ a f není primitivní, pak podle V.8.1. lze psát: $f = z \cdot f^*$, kde f^* je primitivní a tedy $z \neq \pm 1$. Zřejmě ani z ani f^* není jednotkou v $Z[x]$, t. zn. polynom f je reducibilní v $Z[x]$. Ireducibilními polynomy nad Z mohou tedy být jen konstantní polynomy anebo primitivní polynomy stupně alespoň 1.

Nenulová konstanta $c \in Z$ však v $Z[x]$ může být součinem pouze celých čísel, a tedy c je ireducibilním prvkem v $Z[x]$ právě když $|c|$ je prvočíslo, t. zn. právě když c je ireducibilním prvkem v Z.

Dále, nechť $f \in Z[x]$ je primitivní polynom stupně alespoň 1. Je-li f reducibilním prvkem v $Z[x]$, pak (vzhledem k tomu, že je primitivní) je reducibilní i v $Q[x]$. Naopak, nechť f je reducibilní v $Q[x]$. Pak platí: $f = g_1 \cdot g_2$, kde $g_1, g_2 \in Q[x]$,

$1 \leqslant st(g_1), st(g_2) < st(f)$. Polynomy $g_1 . g_2$ lze však podle poznámky před větou psát ve tvaru (4), t. j.:

$$g_1 = c_1^1 . d_1 . h_1^* , \quad g_2 = c_2^1 . d_2 . h_2^*$$

kde $c_i, d_i \in Z$, $h_i^* \in Z[x]$ je primitivní $(i = 1, 2)$. Po dosazení dostáváme: $f = c_1^1 . c_2^1 . d_1 . d_2 . h_1^* . h_2^*$, t. zn.:

$$c_1 . c_2 . f = d_1 . d_2 . h_1^* . h_2^* .$$

Ale f je primitivní a podle Gaussova lemmatu je i $h_1^* . h_2^*$ primitivní, t. zn. podle V.8.1. musí být polynomy f a $h_1^* . h_2^*$ asociovány v $Z[x]$, t. zn. $f = e . h_1^* . h_2^*$, kde $e = \pm 1$. Poněvadž zřejmě je $st(g_i) = st(h_i^*)$, $i = 1, 2$, znamená to, že f je reducibilní v $Z[x]$. Tím je dokázána i 2. část tvrzení.]

Poznámka: pro polynomy s celočíselnými koeficienty stupně $\geqslant 1$ předchozí věta ukazuje úzkou souvislost mezi ireducibilitou nad Z a nad Q. Přesněji řečeno, je-li takový polynom ireducibilní nad Z, pak je ireducibilní nad Q, resp. je-li navíc ještě primitivní, pak je ireducibilní nad Z, právě když je ireducibilní nad Q.

Z posledních dvou poznámek vyplývá, že vyšetřování ireducibility polynomů v $Q[x]$ lze v podstatě převést na vyšetřování ireducibility polynomů v $Z[x]$. Následující věta udává dostatečnou podmínku pro to, aby polynom s celočíselnými koeficienty byl ireducibilní nad tělesem racionálních čísel.

Věta 8.4.: (Eisensteinovo kriterium ireducibility)

Nechť

$$(5) \qquad f = a_0 + a_1 x + \ldots + a_n x^n ; \qquad a_i \in Z , \quad i = 0, 1, \ldots, n$$

je polynom, $st(f) = n \geqslant 1$. Nechť existuje prvočíslo p, pro něž platí:

$$(6) \qquad \begin{cases} p \mid a_j , & j = 0, 1, \ldots, n-1 \\ p \nmid a_n \\ p^2 \nmid a_0 \end{cases}$$

Pak polynom f je ireducibilní nad tělesem Q racionálních čísel.

[D ů k a z : provedeme sporem; nechť polynom f splňuje předpoklady věty a nechť f je reducibilní nad tělesem Q. Pak f je reducibilní nad Z (podle V.8.3.) a tedy existují polynomy $g, h \in Z[x]$, $1 \leqslant st(g), st(h) < st(f)$, tvaru:

$$g = b_0 + b_1 x + \ldots + b_r x^r ; \quad h = c_0 + c_1 x + \ldots + c_s x^s$$

takové, že $f = g . h$. Pak ale $a_0 = b_0 . c_0$ a z (6) plyne, že $p \mid b_0 . c_0$, t. zn. $p \mid b_0$ nebo

$p \mid c_0$. Nechť tedy např. $p \mid b_0$. Pak ale $p \nmid c_0$, protože podle předpokladu $p^2 \nmid a_0$. Dále nechť b_k je koeficient s nejnižším indexem polynomu g, který není dělitelný prvočíslem p (takový koeficient jistě existuje, neboť podle (6): $p \nmid a_n = b_r . c_s$, t. zn. $p \nmid b_r$). Navíc je zřejmě $1 \leqslant k \leqslant n-1$. Platí však:

$$(7) \qquad a_k = b_k . c_0 + b_{k-1} c_1 + \ldots + b_0 c_k$$

Ale $p \mid b_l$, $l = 0, \ldots, k-1$ a dále $p \nmid b_k$, $p \nmid c_0$ a tedy ze (7) plyne, že $p \nmid a_k$, při čemž je $1 \leqslant k \leqslant n-1$, což je ale spor.]

Důsledek: Existuje polynom libovolného stupně n $(n \geqslant 1)$, s celočíselnými koeficienty, který je ireducibilní nad tělesem Q.

[D ů k a z : vezměme například polynom $f(x) = x^n + 2$; $n \geqslant 1$ lib. ; pak podle Eisensteinova kriteria (pro $p = 2$) dostáváme, že f je ireducibilní nad Q.]

Poznámka: Eisensteinovo kriterium je pouze dostatečnou, nikoliv však nutnou podmínkou ireducibility polynomu f. Např. polynom $f = x^2 + 1$ s celými koeficienty zřejmě nesplňuje předpoklady Eisensteinova kriteria a přesto je ireducibilní nad Q.

Kromě Eisensteinova kriteria existuje ještě řada dalších, méně významných dostatečných podmínek pro ireducibilitu polynomu nad Q. Existuje dokonce metoda (vypracovaná již Kroneckerem) pomocí níž lze o lib. polynomu s celými koeficienty rozhodnout, zda je ireducibilní nad tělesem Q nebo nikoliv. Je však příliš komplikovaná a těžkopádná, takže je prakticky nepoužitelná.

Někdy nelze Eisensteinova kriteria použít přímo na polynom f (s celými koeficienty), ale lze jej použít na polynom $f(x+a)$, kde $a \in Z$. Poněvadž však ireducibilita polynomu $f(x)$ je ekvivalentní ireducibilitě polynomu $f(x+a)$, můžeme tímto způsobem dokázat ireducibilitu jestě dalších polynomů, jak ukazuje následující příklad:

Příklad 8.1.: Nechť p je pevné prvočíslo. Ukažte, že polynom

$$f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$$

je ireducibilní nad tělesem Q.

Řešení: je vidět, že na polynom $f(x)$ nelze aplikovat Eisensteinovo kriterium. Zřejmě však $f(x)$ lze napsat ve tvaru: $f(x) = \frac{x^p - 1}{x - 1}$ a položíme-li $x = y + 1$, dostáváme:

$$g(y) = f(y+1) = \frac{(y+1)^p - 1}{(y+1)-1} = \frac{1}{y}.(y^p + \binom{p}{1}.y^{p-1} + \binom{p}{2}y^{p-2} + \ldots + \binom{p}{p-1}.y + 1 - 1) =$$

$$= y^{p-1} + p\,.\,y^{p-2} + \frac{p.(p-1)}{2!}\,y^{p-3} + \ldots + p$$

odkud vidíme, že prvočíslo p dělí všechny koeficienty polynomu g, kromě vedoucího a p^2 nedělí absolutní člen. Tedy podle Eisensteinova kriteria je polynom g ireducibilní nad Q, t. zn. i f je ireducibilní nad Q, neboť je-li: $f(x) = h_1(x).h_2(x)$, pak je $g(y) = h_1(y+1).h_2(y+1)$.

V závěru tohoto paragrafu se budeme zabývat hledáním racionálních kořenů polynomů s racionálními koeficienty. Na rozdíl od předchozí části tentokrát podáme úplné a při tom poměrně jednoduché řešení.

Poznámka: nechť $f(x) \in Q[x]$ je polynom tvaru:

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

kde tedy $a_0, a_1, \ldots, a_n \in Q$. Označíme-li součin jmenovatelů všech koeficientů polynomu $f(x)$ symbolem d, pak polynom:

$$d.f(x) = d.a_0 + d.a_1 x + \ldots + d.a_n x^n$$

má zřejmě všechny koeficienty celočíselné.

Z V.3.2. pak bezprostředně vyplývá, že číslo $c \in Q$ je kořenem polynomu $f(x)$ právě když c je kořenem polynomu $d.f(x)$. Tedy polynomy f a $d.f$ mají v Q stejné kořeny a problém nalezení racionálních kořenů polynomů s racionálními koeficienty jsme tímto obratem převedli na problém nalezení racionálních kořenů polynomů s celými koeficienty.

Věta 8.5.: *Nechť*

(8) $$f(x) = a_0 + a_1 x + \ldots + a_n x^n \;;\quad a_i \in Z,\quad a_n \neq 0$$

je polynom s celými koeficienty a nechť racionální číslo $\frac{r}{s}$ *(kde* r, s *jsou nesoudělná) je kořenem* f.

Pak platí: $r \mid a_0 \;;\; s \mid a_n$.

[D ů k a z : je-li $\frac{r}{s} = 0$ (t. zn. $r = 0, s = 1$) kořenem polynomu f, pak musí být $a_0 = 0$ a tvrzení věty platí.

Předpokládejme tedy, že $\frac{r}{s} \neq 0$. Pak po dosazení do f dostáváme:

(9) $$a_0 + a_1.\frac{r}{s} + \ldots + a_{n-1}.\frac{r^{n-1}}{s^{n-1}} + a_n.\frac{r^n}{s^n} = 0\,.$$

Vynásobením (9) číslem s^{n-1} a převedením posledního členu na pravou stranu dostáváme:

(10) $$a_0.s^{n-1} + a_1.r.s^{n-2} + \ldots + a_{n-1}.r^{n-1} = -\frac{a_n.r^n}{s}$$

Ale na levé straně výrazu (10) je celé číslo, t. zn. musí být: $s \mid a_n.r^n$. Podle předpokladu jsou s, r nesoudělná, t. zn. s, r^n jsou také nesoudělná a tedy musí platit $s \mid a_n$.

Zbývající část tvrzení dostaneme analogicky vynásobením (9) číslem $\frac{s^n}{r}$. Pak je:

$$a_0.\frac{s^n}{r} + a_1.s^{n-1} + a_2.s^{n-2}.r + \ldots + a_{n-1}.s.r^{n-2} + a_n.r^{n-1} = 0$$

t. zn. $a_1.s^{n-1} + a_2.s^{n-2}.r + \ldots + a_n.r^{n-1} = -\frac{a_0 s^n}{r}$, tedy $\frac{a_n.s^n}{r}$ musí být celé číslo, t. zn. $r \mid a_0.s^n$, odkud stejně jako výše plyne, že $r \mid a_0$.]

Důsledek: 1. Je-li celé číslo c kořenem polynomu (8) s celými koeficienty, pak $c \mid a_0$.

2. Je-li polynom (8) normovaný, pak každý racionální kořen f je celé číslo.

[D ů k a z : 1. i 2. jsou bezprostředními důsledky předchozí věty.]

Poznámka: Pomocí V.8.5. lze najít všechny racionální kořeny libovolného polynomu $f \in Q[x]$. Nejprve vhodným vynásobením převedeme polynom f na polynom s celými koeficienty, tvaru (8). Pak zjistíme všechny dělitele r absolutního členu a_0 a všechny dělitele s vedoucího koeficientu a_n a vytvoříme všechny možné zlomky tvaru $\frac{r}{s}$, kterých je zřejmě konečně mnoho a všechny racionální kořeny polynomu f je nutné hledat mezi nimi (výpočtem hodnoty $f(\frac{r}{s})$, např. pomocí Hornerova schematu). Vzhledem k tomu, že koeficienty a_0, resp. a_n mohou mít velký počet dělitelů, může být tato metoda někdy velmi pracná. K zredukování počtu možných racionálních kořenů polynomu f slouží následující věta.

Věta 8.6.: *Nechť racionální číslo* $\frac{r}{s}$ *(*r, s *nesoudělná) je kořenem polynomu* (8) *s celými koeficienty; nechť* m *je celé číslo. Pak:*

$$(r - ms) \mid f(m)$$

t. zn. specielně platí:

$$(r - s) \mid f(1)\;;\quad (r + s) \mid f(-1)$$

Kapitola III

POLYNOMY VÍCE PROMĚNNÝCH

§ 1 : OKRUH POLYNOMŮ n PROMĚNNÝCH

V § 1 kapitoly II jsme ukázali konstrukci pomocí níž lze nad libovolným okruhem R konstruovat okruh $R[x]$ polynomů jedné proměnné. Tuto konstrukci lze zřejmě opakovat (vezmeme-li $R[x]$ za výchozí okruh) a to libovolně konečně mnohokrát, což vede k následující definici.

Definice: *Nechť R je okruh a nechť n je pevné přirozené číslo. Okruh, který získáme z R, použijeme-li n-krát konstrukci okruhu polynomů jedné proměnné, nazýváme okruh polynomů n proměnných nad R a označujeme jej $R[x_1, ..., x_n]$.*

Prvky okruhu $R[x_1, ..., x_n]$ nazýváme polynomy n proměnných nad R (nebo též polynomy n proměnných s koeficienty z R). Nulový prvek okruhu $R[x_1, ..., x_n]$ nazýváme nulový polynom a označujeme jej o nebo též $o(x_1, ..., x_n)$.

Poznámka: rozeberme nyní podrobněji předchozí definici pro některá konkretní n.

Nechť $n = 1$; pak dostáváme známý okruh polynomů jedné proměnné, studovaný v kapitole II.

Nechť $n = 2$; uvážíme-li že polynomy jedné proměnné jsou nekonečné posloupnosti tvaru $(a_0, a_1, ...)$, kde $a_i \in R$, $a_i \neq 0$ pouze pro konečný počet indexů i, pak polynomy dvou proměnných jsou nekonečné posloupnosti

$$((a_{00}, a_{10}, ...), \quad (a_{10}, a_{11}, ...), \quad .....)$$

jejichž členy jsou rovněž posloupnosti (tj. polynomy jedné proměnné), při čemž pouze konečný počet těchto posloupností je různý od nulové posloupnosti, t.j. $(0, 0, ...)$. Vidíme tedy, že polynom dvou proměnných si můžeme vyjádřit jako jistou *nekonečnou matici* (a_{ij}), kde i, j probíhají nezávisle množinu všech celých nezáporných čísel, v níž pouze konečný počet prvků je různý od nulového prvku 0_R. Do řádků této *'matice'* vypisujeme postupně polynomy jedné proměnné, které jsou členy posloupnosti určující daný polynom. Operace + nebo . pak můžeme zapsat následujícím způsobem:

$$(a_{ij}) + (b_{ij}) = (c_{ij}), \quad \text{kde } c_{ij} = a_{ij} + b_{ij}$$

$$(a_{ij}) \cdot (b_{ij}) = (d_{ij}), \quad \text{kde } d_{ij} = \sum_{k+m=i} \sum_{r+s=j} a_{kr} \cdot b_{ms}$$

Při tom zřejmě nulovým polynomem je polynom, v jehož zápisu se vyskytují pouze 0_R a jednotkovým polynomem je polynom (e_{ij}), kde $e_{00} = 1_R$, resp. $e_{ij} = 0_R$ jinak.

Nechť $n = 3$; pak polynomy tří proměnných jsou posloupnosti, jejichž členy jsou výše popsané polynomy dvou proměnných. Je vidět, že takovéto posloupnosti lze vyjádřit indexováním prvků z R třemi indexy, t.j. ve tvaru (a_{ijk}), kde i, j, k nezávisle probíhají množinu všech celých nezáporných čísel, při čemž $a_{ijk} \in R$ a pouze konečný počet prvků a_{ijk} je různý od 0_R.

Výše uvedené úvahy lze nyní zobecnit na případ n proměnných, t. zn. polynom n proměnných lze uvažovat jako posloupnost tvaru $(a_{i_1 i_2 .... i_n})$, kde $i_1, ..., i_n$ nezávisle probíhají množinu všech celých nezáporných čísel, při čemž $a_{i_1 i_2 ... i_n} \in R$ a pouze konečný počet prvků $a_{i_1 ... i_n} \neq 0_R$.

Věta 1.1.: *Je-li okruh R oborem integrity, pak okruh $R[x_1, ..., x_n]$ je také oborem integrity.*

[D ů k a z : provedeme matematickou indukcí vzhledem k n. Pro $n = 1$ tvrzení plyne z důsledku V.1.3, kapitoly II. Nechť tedy tvrzení platí pro $1, 2, ..., n-1$. Pak je $R[x_1, ..., x_n] = (R[x_1, ..., x_{n-1}])[x_n]$, při čemž podle indukčního předpokladu je $R[x_1, ..., x_{n-1}]$ oborem integrity. Tedy opět podle důsledku V.1.3., kapitoly II, je pak $R[x_1, ..., x_n]$ oborem integrity.]

Definice: *Nechť $f = (a_{i_1 i_2 ... i_n}) \in R[x_1, ..., x_n]$ je polynom n proměnných nad okruhem R. Stupněm polynomu f nazýváme největší z čísel $i_1 + i_2 + ... + i_n$, kde $a_{i_1 i_2 ... i_n} \neq 0$, resp. $-\infty$ v případě, že f je nulový polynom. Stupeň polynomu f budeme označovat symbolem $st(f)$.*

Polynomy stupně nula a nulový polynom nazýváme konstantní polynomy; polynomy stupně jedna nazýváme lineární polynomy.

Poznámka: symbol $-\infty$ je definován stejným způsobem jako tentýž symbol, zavedený v § 1, kapitoly II. pro polynomy jedné proměnné. Rovněž vlastnosti $st(f)$ pro polynomy n proměnných budou analogické vlastnostem stupně polynomu jedné proměnné.

[D ů k a z : dělíme polynom f lineárním polynomem $(x-m)$, t. zn. pak

(11) $$f(x) = (x - m).q(x) + f(m)$$

při čemž $q(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$ musí být polynomem s celočíselnými koeficienty, jak plyne z Hornerova schematu. Dosaďme hodnotu $x = \frac{r}{s}$ do (11). Dostáváme:

$$0 = f(\tfrac{r}{s}) = (\tfrac{r}{s} - m)(b_0 + b_1\tfrac{r}{s} + \ldots + b_{n-1}\cdot\tfrac{r^{n-1}}{s^{n-1}}) + f(m)$$

odkud pak

(12) $$f(m) = -\frac{r - ms}{s}\cdot(b_0 + b_1\cdot\frac{r}{s} + \ldots + b_{n-1}\cdot\frac{r^{n-1}}{s^{n-1}})$$

Vidíme, že pro $r = m.s$ je $f(m) = 0$, t. zn. $(r - ms) \mid f(m)$ a věta platí. Nechť tedy $r \neq ms$. Vynásobíme-li (12) výrazem $\frac{s^n}{r - ms}$, dostáváme:

$$\frac{s^n . f(m)}{r - ms} = -(b_0 . s^{n-1} + b_1 . r . s^{n-2} + \ldots + b_{n-1} r^{n-1})$$

kde na pravé straně je celé číslo, t. zn. musí být $(r - ms) \mid s^n . f(m)$.

Ale $r - ms, s^n$ jsou nesoudělná čísla, neboť jinak existuje prvočíslo p s vlastností: $p \mid r - ms$; $p \mid s^n$, odkud však plyne, že $p \mid s$ (poněvadž p je prvočíslo). Pak ale také $p \mid (r - ms) + ms = r$. Máme tedy: $p \mid r$, $p \mid s$, což je spor s předpokladem věty. Jsou tedy $r - ms$, s^n nesoudělná, t. zn. ze vztahu $(r - ms) \mid s^n . f(m)$ dostáváme, že $(r - ms) \mid f(m)$.]

Příklad 8.2.: Nalezněte racionální kořeny polynomu:

$$f(x) = \frac{3}{5}x^4 + x^3 + \frac{x^2}{5} + x - \frac{2}{5}$$

Řešení: po vynásobení číslem 5 dostáváme polynom $g(x)$ s celými koeficienty, s nímž budeme dále pracovat. Tedy:

$$g(x) = 3x^4 + 5x^3 + x^2 + 5x - 2 .$$

Je-li $\frac{r}{s}$ racionálním kořenem polynomu g (a tedy i polynomu f), pak dle V.8.5.:

$$r \mid -2 \Rightarrow r = 1, -1, 2, -2$$
$$s \mid 3 \Rightarrow s = 1, 3$$

(zřejmě u jednoho z čísel r, s stačí uvažovat pouze kladné dělitele). Dále vypíšeme všechny možné hodnoty $\frac{r}{s}$ a pod ně pak hodnoty $r + s$, resp. $r - s$:

$\frac{r}{s}$ =	$\frac{1}{1}$,	$\frac{1}{3}$,	$\frac{-1}{1}$,	$\frac{-1}{3}$,	$\frac{2}{1}$,	$\frac{2}{3}$,	$\frac{-2}{1}$,	$\frac{2}{3}$	
$r+s$ =	2,	4,	0,	2,	3,	5,	-1,	1 ;	$g(-1) = -8$
$r-s$ =	0,	-2,	-2,	4,	1,	-1,	3,	5 ;	$g(1) = 12$

Užitím V.8.6. vidíme, že z původních osmi hodnot $\frac{r}{s}$ zbývají k ověření pouze tři: $\frac{1}{3}$, $-\frac{1}{3}$, -2. Toto ověření provedeme např. Hornerovým schematem:

	3	5	1	5	-2	
$\frac{1}{3}$	3	6	3	6	0	$\Rightarrow \frac{1}{3}$ je kořenem g
$\frac{1}{3}$	3	5	$\frac{4}{3}$	$\frac{50}{9}$		$\Rightarrow -\frac{1}{3}$ není kořenem g
-2	3	0	3	0		$\Rightarrow -2$ je kořenem g

Tedy polynom $f(x)$ má dva racionální kořeny: $\frac{1}{3}$, -2.

Věta 1.2.: *Nechť R je okruh, n je pevné přirozené číslo. Pak:*

1. *Množina všech konstantních polynomů tvoří podokruh okruhu $R[x_1, ..., x_n]$, který lze ztotožnit s okruhem R.*
2. *Je-li $\{k_1, ..., k_m\}$ lib. neprázdná podmnožina $\{1, 2, ..., n\}$, pak polynomy $f = (a_{i_1 i_2 ... i_n}) \in R[x_1, ..., x_n]$ pro něž $a_{i_1 ... i_n} = 0$, jestliže $i_s \neq 0$ pro nějaké $s \notin \{k_1, ..., k_m\}$, tvoří podokruh okruhu $R[x_1, ..., x_n]$. Tento podokruh lze ztotožnit s okruhem polynomů m proměnných nad R.*

[Důkaz: obě tvrzení plynou z V.1.3., kapitoly I a jí následující poznámky, neboť:

1. zobrazení
$$\varphi : R \to R[x_1, ..., x_n]$$
definované pro lib. $a \in R$ vztahem: $\varphi(a) = (a_{i_1 i_2 ... i_n})$, kde $a_{00...0} = a$, resp. $a_{i_1 ... i_n} = 0$, je-li alespoň jeden z indexů různý od nuly, je vnořením.
2. zobrazení
$$\psi : R[x_{k_1}, ..., x_{k_m}] \to R[x_1, ..., x_n]$$
definované pro lib. $(a_{i_{k_1} ... i_{k_m}}) \in R[x_{k_1}, ..., x_{k_m}]$ vztahem $\psi((a_{i_{k_1} ... i_{k_m}})) = (a_{i_1 ... i_n})$, kde
$$a_{i_1 ... i_n} = \begin{cases} 0 & \text{jestliže } i_s \neq 0 \text{ pro nějaké } s \notin \{k_1, ..., k_m\} \\ a_{i_{k_1} ... i_{k_m}} & \text{jinak} \end{cases}$$
je vnořením.]

Stejně jako u polynomů jedné proměnné, můžeme i zde zavést zjednodušený způsob zápisu polynomů z $R[x_1, ..., x_n]$. Je-li $1 \leq k \leq n$, pak polynom $(b_{i_1 i_2 ... i_n})$, kde
$$b_{i_1 ... i_n} = \begin{cases} 1 & \text{je-li } i_k = 1 \text{ a } i_j = 0 \text{ pro } j \neq k \\ 0 & \text{jinak} \end{cases}$$
označíme pevným symbolem, např. x_k (při tom žádáme pouze, aby symboly odpovídající různým indexům k byly různé). Pak libovolný polynom $f = (a_{i_1 ... i_n})$ lze napsat ve tvaru

$$f = \sum a_{i_1 i_2 ... i_n} x_1^{i_1} x_2^{i_2} ... x_n^{i_n} \tag{1}$$

při čemž sumace se provádí přes libovolnou konečnou množinu n-tic indexů $i_1, ..., i_n$ takovou, že obsahuje všechny n-tice pro něž $a_{i_1 ... i_n} \neq 0$. Dvě vyjádření polynomu f ve tvaru (1) se tedy mohou lišit nanejvýš formálně o sčítance tvaru $0 . x_1^{i_1} ... x_n^{i_n}$. Dále vidíme, že posloupnost indexů koeficientu $a_{i_1 ... i_n}$ v (1) a odpovídající posloupnost

exponentů u jednotlivých x_k jsou shodné a není tedy nutné koeficienty indexovat. Budeme tedy polynom f častěji psát ve tvaru:

$$f = \sum a . x_1^{i_1} ... x_n^{i_n} \tag{1'}$$

Definice: *Nechť R je okruh; pak výraz*

$$x_1^{i_1} . x_2^{i_2} ... x_n^{i_n} \tag{2}$$

nazýváme členem o n proměnných nebo stručně členem. Je-li $f = \sum a . x_1^{i_1} ... x_n^{i_n} \in R[x_1, ..., x_n]$, pak (2) nazýváme členem polynomu f; prvek $a \in R$ pak nazýváme koeficientem členu (2). Stupněm členu $x_1^{i_1} ... x_n^{i_n}$ nazýváme číslo $i_1 + ... + i_n$. Polynom, jehož všechny členy mají tentýž stupeň s nazýváme homogenní polynom (stupně s).

Poznámka: z předchozí definice a z definice $st(f)$ plyne, že stupeň nenulového polynomu f je roven maximálnímu ze stupňů jeho členů s nenulovými koeficienty.

Příklad 1.1.:

a) v $K[x_1, x_2, x_3, x_4]$ je $f = (2-i) . x_1^4 x_2 - x_1 x_3^4 - 3 . x_1^2 x_2 x_3^3 + (1+2i)$ polynomem stupně 6, který je nehomogenní.

b) v $Z_4[x_1, x_2, x_3]$ je $g = 2x_1^2 x_2 + 3x_1^2 x_3 + x_1 x_2 x_3$ homogenním polynomem stupně 3.

Poznámka: při vyjádření polynomu z $R[x_1, ..., x_n]$ ve tvaru (1) a při operacích s nimi se mohou ve vyjádření (1) objevit dva stejné členy s nenulovými koeficienty (při tom předpokládáme, že nezáleží na pořadí proměnných, t. zn. např. $x_1 x_2 = x_2 x_1$, atd.), které však můžeme sečíst, neboť zřejmě je:

$$b . x_1^{i_1} ... x_n^{i_n} + c . x_1^{i_1} ... x_n^{i_n} = (b + c) . x_1^{i_1} ... x_n^{i_n}$$

Na základě této úvahy budeme nyní všude v dalším předpokládat, že při vyjádření polynomu z $R[x_1, ..., x_n]$ ve tvaru (1) se nevyskytují stejné členy, ani členy s koeficientem rovným 0. Bude-li třeba tuto úmluvu zvlášť zdůraznit, řekneme, že daný *polynom je ve standartním tvaru.*

Věta 1.3.: *Každý polynom $f \in R[x_1, ..., x_n]$ lze napsat ve tvaru součtu homogenních polynomů navzájem různých stupňů, při čemž toto vyjádření je jednoznačné (až na pořadí).*

[D ů k a z : hledané vyjádření obdržíme tak, že sdružíme dohromady vždy členy polynomu f, mající stejný stupeň. Jednoznačnost daného vyjádření plyne z toho, že všechny polynomy předpokládáme zapsané ve standartním tvaru.]

Definice: *Nechť* $f = \Sigma\, a.x_1^{i_1} \dots x_n^{i_n} \in R[x_1, \dots, x_n]$ *a nechť* $(b_1, \dots, b_n)$ *je prvek kartézského součinu* R^n *(t.j. uspořádaná n-tice prvků z* R*). Pak*

$$\Sigma\, a.b_1^{i_1} \dots b_n^{i_n}$$

je prvek okruhu R*, který nazýváme* h o d n o t a p o l y n o m u f v b o d ě $(b_1, \dots, b_n)$ *a označujeme* $f(b_1, \dots, b_n)$*. Je-li* $f(b_1, \dots, b_n) = 0_R$*, říkáme, že* $(b_1, \dots, b_n)$ *je* k o ř e n e m p o l y n o m u f.

Poznámka: z definice bezprostředně vyplývá, že pro libovolné polynomy $f, g \in R[x_1, \dots, x_n]$ platí:

(3) $$(f \pm g)(b_1, \dots, b_n) = f(b_1, \dots, b_n) \pm g(b_1, \dots, b_n)$$

(4) $$(f \cdot g)(b_1, \dots, b_n) = f(b_1, \dots, b_n) \cdot g(b_1, \dots, b_n)$$

Nechť R je okruh; symbolem R^n značíme kartézský součin $R \times \dots \times R$ (n-krát). Pro lib. $f \in R[x_1, \dots, x_n]$ definujeme zobrazení:

$$\Phi_f : R^n \to R$$

takto: pro lib. $(b_1, \dots, b_n) \in R^n$ položíme

(5) $$\Phi_f((b_1, \dots, b_n)) = f(b_1, \dots, b_n)$$

Zobrazení Φ_f budeme nazývat *polynomiální funkce polynomu* f. Jestliže k nějakému zobrazení $\psi : R^n \to R$ existuje polynom $f \in R[x_1, \dots, x_n]$ tak, že $\psi = \Phi_f$, pak ψ budeme nazývat *polynomiální funkce.*

Analogicky jako u polynomů jedné proměnné lze ukázat, že polynomiální funkce tvoří unitární podokruh okruhu $(R^{(R^n)}, +, \cdot)$ z příkladu 1.2, kap. I. a že zobrazení

$$F : R[x_1, \dots, x_n] \to R^{(R^n)}$$

definované vztahem $F(f) = \Phi_f$, pro lib. $f \in R[x_1, \dots, x_n]$, je okruhovým homomorfizmem. Tento homomorfizmus však obecně nemusí být injektivní, t.j. nemusí být vnořením. V dalším pak ukážeme dostatečnou podmínku pro to, aby vnořením byl.

Věta 1.4.: *Nechť* R_0 *je nekonečný obor integrity, nechť* $f(x_1, \dots, x_n) \in R[x_1, \dots, x_n]$ *je nenulový polynom. Pak existuje prvek* $(b_1, \dots, b_n) \in R_0^n$ *tak, že* $f(b_1, \dots, b_n) \neq 0$.

[D ů k a z : provedeme matematickou indukcí vzhledem k n. Pro $n = 1$ tvrzení věty platí (viz V.3.5., kap. II.). Předpokládejme, že tvrzení věty platí pro všechny nekonečné obory integrity R a okruhy polynomů $n-1$ proměnných $R[x_1, \dots, x_{n-1}]$, kde $n \geq 2$. Poněvadž $R_0[x_1, \dots, x_n] = (R_0[x_1, \dots, x_{n-1}])[x_n]$, při čemž $R_0[x_1, \dots, x_{n-1}]$ je nekonečný obor integrity, pak z 1. části důkazu plyne, že existuje prvek $g = g(x_1, \dots, x_{n-1}) \in R_0[x_1, \dots, x_{n-1}]$ tak, že $f(x_1, \dots, x_{n-1}, g) \neq o(x_1, \dots, x_{n-1})$. Označme $f^*(x_1, \dots, x_{n-1}) = f(x_1, \dots, x_{n-1}, g)$. Pak $f^* \in R_0[x_1, \dots, x_{n-1}]$ a z indukčního předpokladu plyne, že existují prvky $b_1, \dots, b_{n-1} \in R_0$ tak, že $f^*(b_1, \dots, b_{n-1}) \neq 0$, t. zn. $f(b_1, \dots, b_{n-1}, g(b_1, \dots, b_{n-1})) \neq 0$, c.b.d.]

Věta 1.5.: *Nechť* R *je nekonečný obor integrity. Pak zobrazení*

$$F : R[x_1, \dots, x_n] \to R^{(R^n)},$$

popsané výše, je vnořením.

[D ů k a z : vzhledem k předchozím úvaha n zbývá pouze dokázat, že F je injektivní zobrazení. Nechť tedy $f, g \in R[x_1, \dots, x_n]$ jsou polynomy takové, že $F(f) = F(g)$, t. zn. $\Phi_f = \Phi_g$. Podle (5) tedy pro lib. $(b_1, \dots, b_n) \in R^n$ platí $f(b_1, \dots, b_n) = g(b_1, \dots, b_n)$, t. zn. podle (3) je pak: $(f-g)(b_1, \dots, b_n) = 0$. Odtud však podle V.1.4. plyne, že polynom $f-g$ musí být roven nulovému polynomu, t. zn. $f = g$. Zobrazení F je tedy injektivní.]

Důsledek: Nechť R je nekonečný obor integrity, nechť $f, g \in R[x_1, \dots, x_n]$. Pak $f = g$ právě když $f(b_1, \dots, b_n) = g(b_1, \dots, b_n)$, pro každé $(b_1, \dots, b_n) \in R^n$.

[D ů k a z : je-li $f(b_1, \dots, b_n) = g(b_1, \dots, b_n)$ pro každé $(b_1, \dots, b_n) \in R^n$, pak $\Phi_f = \Phi_g$, neboli $F(f) = F(g)$ a podle V.1.5. je $f = g$. Opačná implikace je triviální.]

Poznámka: V okruhu $R[x_1, \dots, x_n]$ můžeme rovněž studovat otázky dělitelnosti a ireducibility. Např. z V.1.4. kapitoly II. užitím matematické indukce plyne, že je-li R oborem integrity, pak jednotkami okruhu $R[x_1, \dots, x_n]$ jsou právě jednotky okruhu R. Tedy k polynomu $f \in R[x_1, \dots, x_n]$ jsou v tomto případě asociovány právě všechny polynomy tvaru rf, kde $r \in R$ je jednotka okruhu R. Na druhé straně ale např. otázka charakterizace ireducibilních polynomů n proměnných je značně komplikovaná a to i ve speciálních případech, např. pro $R = K$, kdy ireducibilní polynomy jedné proměnné umíme jednoduše popsat. Obecně lze totiž ukázat, že pro libovolné těleso R a pro $n \geq 2$ existují v okruhu $R[x_1, \dots, x_n]$ ireducibilní polynomy libo-

volného stupně $m \geq 1$ (např. polynom $x_1^m + x_2$ je v $R[x_1, \ldots, x_n]$ ireducibilní).

Při studiu polynomů n proměnných je často potřeba mít členy daného polynomu lineárně uspořádány. U polynomů jedné proměnné jsme, aniž to bylo nějak zvlášť zdůrazňováno, uspořádávali jednotlivé mocniny proměnné x buďto vzestupně nebo sestupně. Tuto metodu však pro polynomy n proměnných ($n \geq 2$) zřejmě nelze aplikovat a musíme tedy užít jiného postupu.

Definice: *Nechť* $A = x_1^{k_1} \ldots x_n^{k_n}$, $B = x_1^{s_1} \ldots x_n^{s_n}$ *jsou dva členy o* n *proměnných. Řekneme, že člen* A *je před členem* B *(nebo též, že člen* B *je za členem* A*), existuje-li index* i, $1 \leq i \leq n$, *splňující:*

$$k_1 = s_1, \ldots, k_{i-1} = s_{i-1}, \quad k_i > s_i .$$

Jestliže člen A *je před členem* B *nebo* $A = B$, *píšeme pak:* $A \succcurlyeq B$.

Věta 1.6.: $\succcurlyeq$ *je relací lineárního (úplného) uspořádání na množině všech členů o* n *proměnných.*

[Důkaz: $\succcurlyeq$ je zřejmě relací na (nekonečné) množině všech členů o n proměnných. Nechť $A = x_1^{k_1} \ldots x_n^{k_n}$, $B = x_1^{s_1} \ldots x_n^{s_n}$, $C = x_1^{t_1} \ldots x_n^{t_n}$ značí lib. členy o n proměnných. Relace $\succcurlyeq$ je pak:

(i) reflexivní, neboť $A = A$, t. zn. je $A \succcurlyeq A$

(ii) antisymetrická, neboť platí-li $A \succcurlyeq B$, $B \succcurlyeq A$ nemohou pak A, B být různé členy, t. zn. je $A = B$

(iii) tranzitivní, neboť je-li $A \succcurlyeq B$, $B \succcurlyeq C$, pak pokud jsou některé dva z těchto členů rovné, musí být zřejmě $A \succcurlyeq C$. Předpokládejme tedy, že členy A, B, C jsou navzájem různé. To ale znamená, že A je před B a B je před C. Tedy existují indexy i, j splňující:

$k_1 = s_1, \ldots, k_{i-1} = s_{i-1}, k_i > s_i$, resp. $s_1 = t_1, \ldots, s_{j-1} = t_{j-1}, s_j > t_j$.

Pak při $i \leq j$ je: $k_1 = t_1, \ldots, k_{i-1} = t_{i-1}, k_i > t_i$

a při $i > j$ je: $k_1 = t_1, \ldots, k_{j-1} = t_{j-1}, k_j > t_j$,

tedy v každém případě je $A \succcurlyeq C$.

(iv) lineární (úplná), neboť je-li $A \neq B$, pak existuje nějaký exponent, v němž se oba členy liší. Vezmeme-li první takový exponent, dostaneme, že buď A je před B nebo B je před A, tedy buď je $A \succcurlyeq B$ nebo $B \succcurlyeq A$.]

Definice: *Relací* $\succcurlyeq$ *nazýváme relací lexikografického uspořádání členů o* n *proměnných. Vyšetřujeme-li pouze členy daného polynomu* $f(x_1, \ldots, x_n)$, *pak hovoříme o lexikografickém uspořádání členů polynomu* f. *Člen polynomu* f, *který je před všemi ostatními členy tohoto polynomu nazýváme vedoucím členem polynomu* f.

Příklad 1.2.: Polynom $f \in R[x_1, x_2, x_3, x_4]$ tvaru

$$f = 5x_1^4 + 3x_1^2 x_2^3 x_3 - x_1^2 x_2^3 x_4^2 + 5x_1 x_3 x_4^2 + 2x_2 + x_3^2 x_4 - 2$$

je lexikograficky uspořádán a jeho vedoucím členem je člen x_1^4.

Věta 1.7.: *Nechť* R *je obor integrity a nechť* $f, g \in R[x_1, \ldots, x_n]$ *jsou lib. nenulové polynomy. Pak součin vedoucích členů polynomů* f *a* g *je vedoucím členem součinu* $f.g$.

[Důkaz: nechť $A = x_1^{k_1} \ldots x_n^{k_n}$ je vedoucí člen f, resp. $A' = x_1^{m_1} \ldots x_n^{m_n}$ je lib. další člen polynomu f. Pak existuje i, $1 \leq i \leq n$ tak, že: $k_1 = m_1, \ldots, k_{i-1} = m_{i-1}$, $k_i > m_i$. Nechť podobně $B = x_1^{s_1} \ldots x_n^{s_n}$ je vedoucí člen polynomu g, resp. $B' = x_1^{t_1} \ldots x_n^{t_n}$ je lib. další člen g. Pak existuje j: $s_1 = t_1, \ldots, s_{j-1} = t_{j-1}, s_j > t_j$.

Platí však: $A.B = x_1^{k_1+s_1} \ldots x_n^{k_n+s_n}$; $A'.B' = x_1^{m_1+t_1} \ldots x_n^{m_n+t_n}$, odkud je ihned vidět, že $A.B$ je před členem $A'.B'$. Podobně se ukáže, že $A.B$ je rovněž před $A.B'$ i před $A'.B$. Koeficient u členu $A.B$ v $f.g$ je však součinem koeficientů u A a B, t. zn. je nenulový, neboť R je podle předpokladu obor integrity. Tedy $A.B$ je vedoucí člen polynomu $f.g$.]

Poznámka: Nechť R je těleso; pak $R[x_1, \ldots, x_n]$ je obor integrity, pro který můžeme stejnou metodou jako v § 9 kapitoly II. sestrojit podílové těleso, které označujeme $R(x_1, \ldots, x_n)$ a nazýváme *těleso racionálních funkcí* n *proměnných nad* R. Při tom racionální funkcí n proměnných (nad R) rozumíme výraz

$$\frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)}$$

kde $f, g \in R[x_1, \ldots, x_n]$ a $g \neq o(x_1, \ldots, x_n)$. Rovnost racionálních funkcí n proměnných a operace na množině $R(x_1, \ldots, x_n)$ všech tříd navzájem rovných racionálních funkcí n proměnných definujeme stejně jako v § 9 kapitoly II. Platí pak i analogické výsledky, t. zn. $R[x_1, \ldots, x_n]$ můžeme chápat jako podokruh tělesa racionálních funkcí $R(x_1, \ldots, x_n)$ a libovolný prvek z $R(x_1, \ldots, x_n)$ můžeme pak vyjádřit jako podíl dvou prvků z $R[x_1, \ldots, x_n]$.

§ 2 : SYMETRICKÉ POLYNOMY

ÚMLUVA: všude v tomto paragrafu předpokládáme, že R značí těleso.

Definice: *Polynom* $f(x_1, ..., x_n) \in R[x_1, ..., x_n]$ *se nazývá s y m e t r i c k ý, jestliže se nezmění žádnou permutací proměnných, t. zn. pro libovolnou permutaci* $(\alpha_1, ..., \alpha_n)$ *indexů* $1, 2, ..., n$ *platí:*

$$f(x_{\alpha_1}, ..., x_{\alpha_n}) = f(x_1, ..., x_n) \ .$$

Množinu všech symetrických polynomů n *proměnných nad* R *budeme označovat symbolem* $R_s[x_1, ..., x_n]$.

Příklad 2.1.: V $Q[x_1, x_2]$ polynomy $f = 2x_1^2 x_2 + 2x_1 x_2^2 + x_1 + x_2$, resp. $g = 3$ jsou symetrické, kdežto polynomy $h = x_1^2$, resp. $k = x_1 + 2x_1 x_2$ symetrické nejsou.

Věta 2.1.: *$R_s[x_1, ..., x_n]$ je podokruhem oboru integrity $R[x_1, ..., x_n]$, tedy je to obor integrity, který navíc obsahuje těleso R .*

[D ů k a z : jsou-li f_1 a f_2 symetrické polynomy, pak i $f_1 + f_2$, $f_1 - f_2$, $f_1 . f_2$ se nemění žádnou permutací proměnných, t. zn. jsou to symetrické polynomy. Tedy $R_s[x_1, ..., x_n]$ je podokruhem oboru integrity $R[x_1, ..., x_n]$, t. zn. je také oborem integrity. Zbytek tvrzení je zřejmý, neboť konstantní polynomy jsou symetrické.]

Věta 2.2.: *Nechť $A = x_1^{k_1} . x_2^{k_2} ... x_n^{k_n}$ je vedoucí člen symetrického polynomu $f(x_1, ..., x_n)$. Pak platí:*

$$k_1 \geqslant k_2 \geqslant ... \geqslant k_n$$

[D ů k a z : provedeme sporem; nechť A je vedoucí člen f a nechť existuje index i , $1 \leqslant i \leqslant n-1$, takový, že $k_i < k_{i+1}$. Vzhledem k tomu, že polynom f je symetrický, musí obsahovat i člen $B = x_1^{k_1} ... x_{i+1}^{k_i} x_i^{k_{i+1}} ... x_n^{k_n} = x_1^{k_1} ... x_i^{k_{i+1}} x_{i+1}^{k_i} ... x_n^{k_n}$. Potom však člen B je před členem A , což je spor.]

Věta 2.3.: *Nechť $A = x_1^{k_1} ... x_n^{k_n}$ je člen o n proměnných. Pak existuje pouze konečně mnoho vedoucích členů symetrických polynomů o n proměnných, které jsou za členem A .*

[D ů k a z : nechť $x_1^{s_1} . x_2^{s_2} ... x_n^{s_n}$ je vedoucí člen nějakého symetrického polynomu o n proměnných, který je za členem A (při lexikografickém uspořádání členů o n proměnných). Pak musí platit:

1) existuje i , $1 \leqslant i \leqslant n$ tak, že: $k_1 = s_1 , ..., k_{i-1} = s_{i-1}$, $k_i > s_i$

2) $s_1 \geqslant s_2 \geqslant ... \geqslant s_n$ (podle V.2.2.)

Odtud vidíme, že musí jistě platit: $s_i \leqslant k_1$, $i = 1, ..., n$, t. zn. vedoucích členů symetrických polynomů, které jsou za členem A je jistě méně než $(k_1+1)^n$, t. zn. konečně mnoho.]

Definice: *Polynomy z $R[x_1, ..., x_n]$ tvaru:*

$$\sigma_1(x_1, ..., x_n) = x_1 + x_2 + ... + x_n$$
$$\sigma_2(x_1, ..., x_n) = x_1x_2 + x_1x_3 + ... + x_1x_n + x_2x_3 + ... + x_{n-1}x_n$$
$$\vdots$$
$$\sigma_k(x_1, ..., x_n) = \sum_{i_1 < i_2 < ... < i_k} x_{i_1} x_{i_2} ... x_{i_k}$$
$$\vdots$$
$$\sigma_n(x_1, ..., x_n) = x_1 . x_2 ... x_n$$

nazýváme e l e m e n t á r n í s y m e t r i c k é p o l y n o m y (n proměnných).

Poznámka: Je bezprostředně vidět, že výše definované polynomy $\sigma_k(x_1, ..., x_n)$ jsou skutečně symetrickými polynomy. S těmito polynomy jsme se setkali již dříve (při poněkud odlišném označení, což je však nepodstatné), ve V.7.5. kapitoly II., která udávala vztahy mezi kořeny a koeficienty polynomu $f \in K[x]$. Můžeme tedy říci, že koeficienty polynomu jedné proměnné (nad K) jsou, až na konstantní násobek, elementárními symetrickými polynomy jeho kořenů.

V dalším budeme řešit otázku, zda libovolný symetrický polynom $f \in R_s[x_1, ..., x_n]$ lze vyjádřit jako polynom v proměnných $\sigma_1, ..., \sigma_n$, resp. kolika způsoby. Vyčerpávající odpověď na tuto otázku dává následující věta.

Věta 2.4.: (Hlavní věta o symetrických polynomech.)
Každý symetrický polynom $f(x_1, ..., x_n) \in R_s[x_1, ..., x_n]$ lze vyjádřit jako polynom n proměnných $\sigma_1, ..., \sigma_n$ nad R , t. zn.

$$f(x_1, ..., x_n) = \varphi(\sigma_1, ..., \sigma_n)$$

při čemž toto vyjádření je jednoznačné.

[D ů k a z : 1. existence: nechť $f(x_1, ..., x_n)$ je symetrický polynom nad R a nechť

(2) $$a . x_1^{k_1} . x_2^{k_2} ... x_n^{k_n}$$

je jeho vedoucí člen s koeficientem $a \in R$, $a \neq 0$. Podle V.2.2. je: $k_1 \geqslant k_2 \geqslant ... \geqslant k_n$.

Uvažme polynom:

(3) $$\varphi_1 = a \cdot \sigma_1^{k_1-k_2} \cdot \sigma_2^{k_2-k_3} \cdot \ldots \cdot \sigma_{n-1}^{k_{n-1}-k_n} \cdot \sigma_n^{k_n}$$

Pak podle předchozího jsou všechny exponenty v (3) celá nezáporná čísla a navíc po dosazení z (1) je φ_1 symetrickým polynomem v proměnných $x_1, \ldots, x_n$ (plyne z V.2.1, neboť pak je φ_1 součinem symetrických polynomů proměnných $x_1, \ldots, x_n$). Napišme nyní vedoucí člen (i s koeficientem) polynomu φ_1. Podle V.1.7. je to:

(4) $$a \cdot x_1^{k_1-k_2} \cdot (x_1x_2)^{k_2-k_3} \cdot \ldots \cdot (x_1x_2 \ldots x_{n-1})^{k_{n-1}-k_n} \cdot (x_1 \cdot x_2 \ldots x_n)^{k_n} = a \cdot x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$$

Vidíme, že je roven (i co do koeficientu) vedoucímu členu polynomu f. Utvořme polynom:

(5) $$f_1 = f - \varphi_1$$

Pak f_1 je symetrickým polynomem v proměnných $x_1, \ldots, x_n$ nad R, při čemž vedoucí člen f_1 stojí za vedoucím členem polynomu f, jak plyne z (2), (4) a (5). Dále, vyjdeme-li z vedoucího členu polynomu f_1, zkonstruujeme analogicky polynom φ_2 a označíme: $f_2 = f_1 - \varphi_2$. Pak vedoucí člen f_2 stojí za vedoucím členem polynomu f_1 a platí:

$$f = \varphi_1 + f_1 = \varphi_1 + \varphi_2 + f_2$$

Takto postupujeme dále, až obdržíme $f_r = o$, což podle V.2.3. po konečném počtu kroků musí nastat. Po dosazení pak dostáváme:

$$f = \varphi_1 + \varphi_2 + \ldots + \varphi_r + f_r = \varphi_1 + \varphi_2 + \ldots + \varphi_r = \varphi(\sigma_1, \ldots, \sigma_n)$$

což je hledané vyjádření.

II. jednoznačnost: důkaz jednoznačnosti hledaného vyjádření provedeme sporem. Nechť: $f(x_1, \ldots, x_n) = \varphi(\sigma_1, \ldots, \sigma_n) = \psi(\sigma_1, \ldots, \sigma_n)$, při čemž $\varphi \neq \psi$, t. zn. polynomy φ a ψ se liší alespoň v jednom koeficientu u stejného členu. Označme:

$$\tau(\sigma_1, \ldots, \sigma_n) = \varphi(\sigma_1, \ldots, \sigma_n) - \psi(\sigma_1, \ldots, \sigma_n).$$

Označíme-li $g(x_1, \ldots, x_n)$ polynom získaný z $\tau(\sigma_1, \ldots, \sigma_n)$ substitucí (1), pak je zřejmě $g(x_1, \ldots, x_n) = o$. Podle předpokladu je $\tau(\sigma_1, \ldots, \sigma_n) \neq o(\sigma_1, \ldots, \sigma_n)$, t. zn. alespoň jeden koeficient u některého členu polynomu τ je nenulový. Nechť

(6) $$a \cdot \sigma_1^{t_1} \cdot \sigma_2^{t_2} \ldots \sigma_n^{t_n}, \text{ kde } a \neq 0$$

vystupuje v $\tau(\sigma_1, \ldots, \sigma_n)$. Po dosazení (1) do (6) dostáváme zřejmě symetrický polynom v proměnných $x_1, \ldots, x_n$, jehož vedoucí člen nechť je:

(7) $$x_1^{v_1} \cdot x_2^{v_2} \ldots x_n^{v_n}$$

Podle V.1.7. je však:

$$x_1^{v_1} \cdot x_2^{v_2} \ldots x_n^{v_n} = x_1^{t_1} \cdot (x_1x_2)^{t_2} \ldots (x_1x_2 \ldots x_n)^{t_n},$$

odkud po úpravě pravé strany dostáváme:

$$\begin{aligned} v_1 &= t_1 + t_2 + \ldots + t_n \\ v_2 &= \quad t_2 + \ldots + t_n \\ &\vdots \\ v_n &= \quad\quad\quad t_n \end{aligned}$$

což jinak zapsáno dává:

(8) $$\begin{aligned} t_1 &= v_1 - v_2 \\ t_2 &= v_2 - v_3 \\ &\vdots \\ t_{n-1} &= v_{n-1} - v_n \\ t_n &= v_n \end{aligned}$$

Vidíme tedy, že exponenty $t_1, \ldots, t_n$ členu (6) lze jednoznačně zkonstruovat z exponentů $v_1, \ldots, v_n$ vedoucího členu (7). Tedy, různé členy polynomu $\tau(\sigma_1, \ldots, \sigma_n)$, uvažované jako symetrické polynomy v $x_1, \ldots, x_n$ (t. zn. po substituci (1)) musí mít různé vedoucí členy (jinak totiž podle (8) z rovnosti vedoucích členů (7) plyne i rovnost původních členů (6)).

Uvažme nyní všechny členy s nenulovými koeficienty polynomu τ, každý z nich substitucí (1) převeďme na polynom v proměnných $x_1, \ldots, x_n$ a vezměme vždy vedoucí člen tohoto polynomu. Dostaneme tak neprázdnou množinu navzájem různých členů, které uspořádáme lexikograficky. Vezmeme-li nyní v tomto uspořádání vedoucí člen, pak tento musí být před vůbec všemi členy, které při substituci (1) do $\tau(\sigma_1, \ldots, \sigma_n)$ dostaneme; při tom jeho koeficient je zřejmě nenulový. Pak ale polynom $g(x_1, \ldots, x_n)$ definovaný výše je nenulový, což je spor. Musí tedy být $\varphi(\sigma_1, \ldots, \sigma_n) = \psi(\sigma_1, \ldots, \sigma_n)$, t. zn. vyjádření polynomu f ve tvaru polynomu proměnných $\sigma_1, \ldots, \sigma_n$ nad R je jednoznačné.]

Důsledek: Nechť $f(x_1, \ldots, x_n) = \varphi(\sigma_1, \ldots, \sigma_n)$ je vyjádření symetrického polynomu $f \in R_s[x_1, \ldots, x_n]$ pomocí elementárních symetrických polynomů. Pak koeficienty polynomu φ získáme z koeficientů polynomu f pomocí operací sčítání a odečítání (v R).

[Důkaz: z první části důkazu předchozí věty plyne, že polynom φ_1 má za koeficient přímo koeficient vedoucího členu polynomu f. Provedeme-li ve (3) substituci (1), pak po rozepsání dostaneme polynom v proměnných $x_1, \ldots, x_n$, jehož

koeficienty jsou celými násobky koeficientu vedoucího členu polynomu f. Pak ale z (5) plyne, že koeficienty polynomu f_1 získáme z koeficientů polynomu f pomocí sčítání a odečítání a totéž tedy platí pro koeficient polynomu φ_2. Podobně pro polynomy $\varphi_3, ..., \varphi_r$, t. zn. i pro polynom φ.]

Poznámka: důkaz první části předchozí věty je konstruktivní, t. zn. lze jej aplikovat při konkretním výpočtu, jak ukazuje následující příklad.

Příklad 2.2.: Symetrický polynom $f(x_1, x_2, x_3) = x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 \in Q[x_1, x_2, x_3]$ vyjádřete pomocí elementárních symetrických polynomů.

Řešení:

$$\varphi_1 = 1 . \sigma_1^{2-1} . \sigma_2^{1-0} . \sigma_3^0 = \sigma_1 . \sigma_2 = (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) =$$
$$= x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 + 3x_1x_2x_3$$

Pak: $f_1 = f - \varphi_1 = -3 . x_1x_2x_3$

$$\varphi_2 = -3\sigma_3 = -3x_1x_2x_3$$

Pak: $f_2 = f_1 - \varphi_2 = o$

a tedy výsledné vyjádření je tvaru: $f = \varphi_1 + \varphi_2 = \sigma_1\sigma_2 - 3\sigma_3$.

Z příkladu je vidět, že zejména při vyšším stupni polynomu f bude uvedený postup velmi pracný. Odvodíme proto nyní jinou metodu, která při praktickém výpočtu bude jednodušší.

Z důkazu hlavní věty je vidět, že členy hledaného polynomu $\varphi(\sigma_1, ..., \sigma_n)$ jsou vyjadřovány pomocí vedoucích členů symetrických polynomů $f, f_1, ..., f_{r-1}$. Přitom vedoucí členy polynomů $f_1, ..., f_{r-1}$ jsou za vedoucím členem polynomu f. Všechny takové členy můžeme však lehce vypsat a z posloupnosti jejich exponentů u proměnných $x_1, ..., x_n$ můžeme ihned psát jim odpovídající členy hledaného polynomu $\varphi(\sigma_1, ..., \sigma_n)$. Koeficienty takto nalezených členů jsou jisté prvky z R, které zjistíme postupným dosazováním konkretních hodnot (z tělesa R) za proměnné $x_1, ..., x_n$. Uvedená metoda se proto nazývá *metoda neurčitých koeficientů*.

Je-li $f(x_1, ..., x_n)$ navíc homogenním polynomem stupně k, pak polynomy $f_1, ..., f_{r-1}$ musí být též homogenní, stupně k a tedy i jejich vedoucí členy jsou stupně k. Stačí tedy v tomto případě vypisovat pouze vedoucí členy stupně k.

Není-li polynom $f(x_1, ..., x_n)$ homogenní, pak je zřejmě výhodné rozdělit jej na homogenní části navzájem různých stupňů a pro každou část provést výpočet zvlášť.

Shrneme-li to, co jsme právě řekli, dostáváme praktický návod k vyjádření symetrického polynomu $f(x_1, ..., x_n)$ pomocí elem. sym. polynomů $\sigma_1, .., \sigma_n$:

1. Polynom f rozdělíme na homogenní části různých stupňů a pro každou z nich řešíme zvlášť.
2. Napíšeme posloupnosti exponentů vedoucího členu A polynomu f a všech vedoucích členů symetrických polynomů daného stupně, stojících za A.
3. Ke každé posloupnosti exponentů vypíšeme odpovídající člen v proměnných $\sigma_1, ..., \sigma_n$ (viz (3) v důkazu V.2.4.).
4. Hledané vyjádření je lineární kombinací členů z 3., při čemž koeficient u prvního z nich je roven koeficientu členu A a ostatní koeficienty zjistíme postupným dosazováním vhodných hodnot (z R) za $x_1, ..., x_n$.
5. Sečtením nalezených vyjádření pro jednotlivé homogenní části dostaneme řešení.

Příklad 2.3.: Symetrický polynom $f(x_1, x_2, x_3) = (x_1^2 + x_2^2)(x_1^2 + x_3^2)(x_2^2 + x_3^2) + (x_1 + x_2)(x_1 + x_3)(x_2 + x_3) \in R[x_1, x_2, x_3]$ vyjádřete pomocí elem. symetrických polynomů.

Řešení: polynom f rozdělíme na dvě homogenní části: $f = g + h$, kde:

a) $g(x_1, x_2, x_3) = (x_1^2 + x_2^2)(x_1^2 + x_3^2)(x_2^2 + x_3^2) = x_1^4 . x_2^2 + ...$

$$\left.\begin{array}{llll} 4 & 2 & 0 & \Rightarrow \sigma_1^2\sigma_2^2 \\ 4 & 1 & 1 & \Rightarrow \sigma_1^3\sigma_3 \\ 3 & 3 & 0 & \Rightarrow \sigma_2^3 \\ 3 & 2 & 1 & \Rightarrow \sigma_1\sigma_2\sigma_3 \\ 2 & 2 & 2 & \Rightarrow \sigma_3^2 \end{array}\right\} \quad g = \sigma_1^2\sigma_2^2 + A.\sigma_1^3\sigma_3 + B.\sigma_2^3 + C.\sigma_1\sigma_2\sigma_3 + D.\sigma_3^2$$

$(-1, 1, 0) \Rightarrow \sigma_1 = 0, \sigma_2 = -1, \sigma_3 = 0, g = 2 \Rightarrow 2 = -B$, tzn. $B = -2$
$(2, -1, -1) \Rightarrow \sigma_1 = 0, \sigma_2 = -3, \sigma_3 = 2, g = 50 \Rightarrow 50 = -2.(-27) + 4D$, tzn. $D = -1$
$(-1, 2, 2) \Rightarrow \sigma_1 = 3, \sigma_2 = 0, \sigma_3 = -4, g = 200 \Rightarrow 200 = A.(27).(-4) - 16$, tzn. $A = -2$
$(-1, 1, 1) \Rightarrow \sigma_1 = 1, \sigma_2 = -1, \sigma_3 = -1, g = 8 \Rightarrow 8 = 1 + 2 + 2 + C - 1$, tzn. $C = 4$

Tedy: $g = \sigma_1^2\sigma_2^2 - 2\sigma_1^3\sigma_3 - 2\sigma_2^3 + 4\sigma_1\sigma_2\sigma_3 - \sigma_3^2$

b) $h(x_1, x_2, x_3) = (x_1 + x_2)(x_1 + x_3)(x_2 + x_3) = x_1^2x_2 + ...$

$$\left.\begin{array}{lll} 2 & 1 & 0 \Rightarrow \sigma_1\sigma_2 \\ 1 & 1 & 1 \Rightarrow \sigma_3 \end{array}\right\} \quad h = \sigma_1\sigma_2 + K\sigma_3$$

$(1, 1, 1) \Rightarrow \sigma_1 = 3, \sigma_2 = 3, \sigma_3 = 1, h = 8 \Rightarrow 8 = 9 + K$, tzn. $K = -1$

Tedy: $h = \sigma_1\sigma_2 - \sigma_3$

Dodatek

ALGEBRAICKÉ ROVNICE

§ 1 : ALGEBRAICKÉ ŘEŠENÍ ALGEBRAICKÝCH ROVNIC

Problém řešení rovnic je jedním z nejstarších a při tom nejdůležitějších matematických problémů vůbec, který rovněž souvisí s teorií polynomů. Poznamenejme, že všechny úvahy v této kapitole budeme provádět nad polem K komplexních čísel, nebude-li výslovně řečeno jinak. Dále, na rozdíl od předchozích kapitol bude podaný výklad tentokrát pouze stručným přehledem, při čemž důkladný rozbor lze najít např. v [6] nebo [8].

Je-li $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ polynom s komplexními koeficienty, stupně $n \geqslant 1$, pak rovnici

(1) $$f(x) = 0$$

budeme nazývat *algebraickou rovnicí* (n-tého stupně, o jedné neznámé). Při tom (1) bude vyjadřovat příkaz vyhledat všechny (obecně komplexní) kořeny polynomu $f(x)$, které budeme též nazývat kořeny nebo *řešení rovnice* (1). Je vidět, že polynom $f(x)$ v (1) lze v tomto případě, bez újmy na obecnosti, předpokládat v normovaném tvaru.

Poznámka: je důležité si uvědomit, že zápis (1) neznamená tentokrát rovnost dvou polynomů (totiž polynomu f a nulového polynomu). Dále připomeňme, že kromě algebraických rovnic existují i nealgebraické rovnice, t.j. rovnice tvaru (1), kde však $f(x)$ není polynom, nýbrž nějaká jiná komplexní funkce. Takovými rovnicemi se zde nebudeme zabývat.

Příklad 1.1.: Rovnice

(2) $$x^n - 1 = 0$$

je algebraickou rovnicí, jejímiž kořeny, jak známo, jsou právě všechny n-té odmocniny z jedné, t.j. čísla: $\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$, $k = 0, 1, \ldots, n-1$. V dalším budeme pro jednu z těchto hodnot používat pevného označení, a sice:

$$\epsilon_n = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} .$$

Při tomto označení pak zřejmě všechny kořeny rovnice (2) jsou: $1, \epsilon_n, \epsilon_n^2, \ldots, \epsilon_n^{n-1}$.

V dalším nyní naznačíme metody řešení pro několik nejjednodušších, resp. speciálních typů algebraických rovnic.

(a) *Kvadratická rovnice*

t. j. rovnice tvaru $x^2 + px + q = 0$ (kde p, q jsou obecně komplexní čísla!) se dá přepsat do tvaru: $(x + \frac{p}{2})^2 - (\frac{p^2}{4} - q) = 0$, odkud ihned dostáváme její kořeny:

$$x_{1,2} = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

kde $\sqrt{\frac{p^2}{4} - q}$ znamená libovolnou (ale pevnou) z obou druhých odmocnin z komplexního čísla $\frac{p^2}{4} - q$. Připomeňme, že druh kořenů kvadratické rovnice záleží na hodnotě diskriminantu D polynomu na levé straně (viz § 3, kap. III.). Má-li kvadratická rovnice navíc reálné koeficienty, pak při $D \geqslant 0$ má pouze reálné kořeny, resp. při $D < 0$ pouze nereálné (imaginární) kořeny.

(b) *Kubická rovnice*

(3) $$z^3 + az^2 + bz + c = 0$$

se jednoduchou substitucí:

(4) $$z = x - \frac{a}{3}$$

převede na jednodušší rovnici (samozřejmě ovšem rovněž kubickou) tvaru:

(5) $$x^3 + px + q = 0$$

Stačí nyní najít všechny kořeny rovnice (5), neboť pak užitím (4) určíme všechny kořeny původní rovnice (3). Po několika úpravách dostáváme nakonec tento výsledek: nechť $K = \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ značí jednu (pevnou) z obou hodnot napsaného symbolu; nechť dále u značí libovolnou (pevnou) ze tří třetích odmocnin $\sqrt[3]{-\frac{q}{2} + K}$ a konečně v značí tu z třetích odmocnin $\sqrt[3]{-\frac{q}{2} - K}$, která splňuje vztah: $3uv = -p$. Potom kořeny rovnice (5) jsou:

(6) $$x_1 = u + v \; ; \quad x_2 = \epsilon_3 . u + \epsilon_3^2 . v \; ; \quad x_3 = \epsilon_3^2 . u + \epsilon_3 . v ,$$

kde $\epsilon_3 = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = -\frac{1}{2} + \frac{1}{2} i\sqrt{3}$. Vzorce (6), pomocí nichž můžeme algebraicky explicitně najít kořeny kubické rovnice, se nazývají *Cardanovy vzorce*.

O druhu kořenů rovnice (5) lze opět rozhodnout podle hodnoty diskriminantu D polynomu na levé straně (5), přičemž $D = -4p^3 - 27q^2$, jak plyne z příkladu 3.3, kap. III. Podle V.3.4., kap. III. jsou kořeny navzájem různé právě když $D \neq 0$.

Obzvlášť důležitý je případ, kdy koeficienty kubické rovnice (5) jsou reálná čísla. Potom při $D<0$ dostáváme (rozborem Cardanových vzorců), že jeden kořen (5) je reálný a zbývající dva jsou imaginární (a to komplexně sdružené, vzhledem k V.7.6., kap. II.). Je-li $D>0$, pak jsou všechny tři kořeny rovnice (5) reálné a různé. Cardanovy vzorce však tyto reálné kořeny vyjadřují ve tvaru součtu třetích odmocnin z komplexních čísel, což je v praxi nepříjemné. Dokonce lze ukázat, že žádnou metodou užívající pouze základních aritmetických operací (t. j. $+, -, ., :$) a tvoření aritmetických (reálných) odmocnin nelze v tomto případě vyjádřit kořeny rovnice (5) pomocí jejích koeficientů. Tento problém je však možno řešit poměrně jednoduše pomocí goniometrických funkcí.

(c) *Rovnice čtvrtého stupně*

(7) $$x^4 + ax^3 + bx^2 + cx + d = 0$$

se dá opět řešit celou řadou algebraických metod. Například, označíme-li x_1, x_2, x_3, x_4 kořeny rovnice (7) a uvážíme polynom $g(x)$ tvaru:

$$g(x) = (x-(x_1+x_2)).(x-(x_1+x_3)).(x-(x_1+x_4)).(x-(x_2+x_3)).(x-(x_2+x_4)).(x-(x_3+x_4))$$

pak koeficienty polynomu $g(x)$ jsou zřejmě symetrickými polynomy kořenů rovnice (7). Substitucí

(8) $$x = t - \frac{a}{2}$$

přejde polynom $g(x)$ v polynom $F(t) = g(t-\frac{a}{2})$, který obsahuje pouze sudé mocniny proměnné t. Položíme-li: $t^2 = u$, dostáváme pak kubickou rovnici o neznámé u. Tuto umíme řešit a z jejích tří kořenů u_1, u_2, u_3 obdržíme 6 kořenů rovnice $F(t) = 0$, a sice $\pm\sqrt{u_1}$, $\pm\sqrt{u_2}$, $\pm\sqrt{u_3}$, odkud pomocí (8) dostaneme 6 kořenů: $\alpha_1, \alpha_2, \ldots, \alpha_6$ rovnice $g(x) = 0$. Nakonec, pro nalezení kořenů původní rovnice (7) stačí řešit tento jednoduchý systém rovnic:

$$x_1 + x_2 = \alpha_1\ ,\ x_1 + x_3 = \alpha_2\ ,\ x_1 + x_4 = \alpha_3\ ,\ x_2 + x_3 = \alpha_4\ ,\ x_2 + x_4 = \alpha_5\ ,\ x_3 + x_4 = \alpha_6\ ,$$

z něhož již snadno vypočítáme x_1, x_2, x_3, x_4.

(d) *Binomická rovnice*

je algebraická rovnice tvaru

(9) $$x^n + a = 0\ ,$$

kde $a \neq 0$ je pevné komplexní číslo. Případ $a = 1$ jsme rozebrali v příkladu 1.1. Obecně, označíme-li libovolnou (ale pevnou) z n-tých odmocnin z komplexního čísla a symbolem $\sqrt[n]{a}$, pak všechny kořeny rovnice (9) jsou: $\sqrt[n]{a}$, $\epsilon_n \cdot \sqrt[n]{a}$, $\epsilon_n^2 \cdot \sqrt[n]{a}$, .., $\epsilon_n^{n-1} \cdot \sqrt[n]{a}$,

kde $\epsilon_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$, jak bylo zavedeno výše.

(e) *Reciproká rovnice*

Rovnici tvaru: $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$ nazýváme reciprokou rovnicí 1. druhu (resp. 2. druhu), jestliže platí: $a_n = a_0$, $a_{n-1} = a_1$, $a_{n-2} = a_2$, ... (resp. $a_n = -a_0$, $a_{n-1} = -a_1$, $a_{n-2} = -a_2$, ...).

Zřejmě, má-li reciproká rovnice (ať 1. nebo 2. druhu) kořen c, pak má také kořen $\frac{1}{c}$. Dále, reciproká rovnice 1. druhu, lichého stupně, má vždy kořen $c = -1$ a po jejím vydělení kořenovým činitelem $(x+1)$ obdržíme reciprokou rovnici 1. druhu, sudého stupně. Podobně, reciproká rovnice 2. druhu má vždy kořen $c = 1$, a po vydělení činitelem $(x-1)$ obdržíme reciprokou rovnici 1. druhu. Z těchto úvah vyplývá, že při studiu reciprokých rovnic se stačí omezit pouze na reciproké rovnice 1. druhu a sudého stupně, např. $2m$. Řešení takové rovnice lze však jednoduchou substitucí převést na řešení algebraické rovnice polovičního, t. j. m-tého stupně a řešení m kvadratických rovnic.

Výše jsme ukázali, jak lze explicitně vyjádřit kořeny algebraické rovnice z jejích koeficientů 'algebraickými' metodami (t. j. metodami, užívajícími v konečném počtu čtyř základních aritmetických operací a tvoření odmocnin) pro rovnice až do 4. stupně. Problém najít 'algebraické' řešení rovnice 5. stupně se stal po objevu řešení rovnic 3. a 4. stupně v XVI. století jedním z ústředních matematických problémů. V letech 1700-1701 francouzský matematik Lagrange podal obecnou metodu jak vyjádřit kořeny algebraické rovnice metodou symetrických funkcí pomocí kořenů jiných algebraických rovnic, které nazýváme *resolventami*. Ukazuje se, že resolventy rovnic 3. a 4. stupně jsou o jedničku menšího stupně než daná rovnice, zatímco resolventa rovnice 5. stupně má stupeň 6. Nesčetné pokusy o obecné 'algebraické' řešení rovnic stupně pátého a vyšších selhávaly a vedly nakonec k opačným pokusům, dokázat nemožnost nalezení takové metody. Správnost druhé domněnky potvrdil norský matematik H. Abel ve dvacátých letech minulého století. Tím ovšem není řečeno, že by nebylo možno některé speciální typy algebraických rovnic vyšších stupňů řešit 'algebraickými' metodami. Ucelenou odpověď na otázky tohoto druhu podal francouzský matematik E. Galois (1811-1832). Z teorie po něm nazvané plyne, že pro každé $n \geq 5$ existuje algebraická rovnice stupně n, která není řešitelná 'algebraickými' metodami.

§ 2: NUMERICKÉ ŘEŠENÍ ALGEBRAICKÝCH ROVNIC

V předchozím paragrafu jsme poukázali na nemožnost obecně 'algebraicky' řešit algebraické rovnice stupně $n \geq 5$. Ale i metody a vzorce pro řešení algebraických rovnic stupně menšího než 5 mají význam spíše teoretický než praktický. Proto je nutné hledat jiné způsoby výpočtu kořenů algebraických rovnic. Při těchto úvahách, které většinou přesahují rámec základního kurzu algebry, je obvykle nutné použít aparátu a metod matematické analýzy.

V dalším alespoň schematicky naznačíme postup získání (přibližných) hodnot reálných kořenů algebraické rovnice s reálnými koeficienty, t. j. rovnice:

(1) $$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0 , \qquad a_i \in R ,$$

což je sice specielní, ovšem v praxi nejčastější případ. Postup sestává ze tří kroků:

a) *ohraničení kořenů*

b) *separace kořenů*

c) *aproximace kořenů.*

Ohraničením kořenů se rozumí nalezení intervalu na reálné ose, v němž leží všechny reálné kořeny dané rovnice (1). Lze například ukázat, že reálné kořeny rovnice (1) leží v intervalu $< -(1 + \frac{M}{|a_n|}), (1 + \frac{M}{|a_n|}) >$, kde $M = \max \{|a_0|, \ldots, |a_{n-1}|\}$. Podobných odhadů existuje celá řada. Separace kořenů znamená nalezení intervalů na reálné ose, z nichž každý obsahuje právě jeden reálný kořen rovnice (1). Obecné metody pro separaci kořenů bývají dosti těžkopádné a pracné. Někdy vystačíme s pouhým horním odhadem počtu kořenů, který může dokonce vést i k přesným výsledkům, spojíme-li jej s dolním odhadem počtu kořenů. Poslední odhad lze nejjednodušeji provést pouhým sledováním znaménkových změn hodnot polynomu na levé straně (1) v libovolné konečné posloupnosti bodů. Konečně, jestliže jsme nalezli interval obsahující právě jeden kořen rovnice (1), který označíme např. x_0, pak provádíme aproximaci tohoto kořene s jistou předem danou přesností. Znamená to zkonstruovat dvě posloupnosti reálných čísel:

$$c_1 \leq c_2 \leq \ldots \leq c_n \leq \ldots \leq x_0 \leq \ldots \leq d_n \leq \ldots \leq d_2 \leq d_1 ,$$

obě konvergující k hodnotě x_0. Existuje opět celá řada t. zv. přibližných metod, které umožňují aproximovat hledaný kořen s libovolnou přesností.

Všechny numerické metody řešení algebraických rovnic získaly na významu v poslední době především možností využití moderní výpočetní techniky.