Algebra

3. mája 2017

1 Úvod

Všade v nasledujúcom texte budeme používať tieto označenia:
$\mathbb{N}$ označuje množinu všetkých prirodzených čísel.
$\mathbb{N}_0$ označuje množinu všetkých celých nezáporných čísel.
$\mathbb{Z}$ označuje množinu všetkých celých čísel aj okruh celých čísel.
$\mathbb{Q}$ označuje množinu všetkých racionálnych čísel aj pole racionálnych čísel.
$\mathbb{R}$ označuje množinu všetkých reálnych čísel aj pole reálnych čísel.
$\mathbb{C}$ označuje množinu všetkých komplexných čísel aj pole komplexných čísel.

V algebraických rovniciach s reálnymi koeficientami a jednou neznámou a tiež pri polynomických reálnych funkciách s jednou reálnou premennou sa stretávame s "výrazmi" tvaru $a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, kde pre všetky i je $a_i \in \mathbb{R}$, ktoré nazývame polynómy (s reálnymi koeficientami a s jednou neurčitou x). Polynómy sa používajú aj v ďalších oblastiach matematiky a tiež informatiky, napríklad v teórii kódovania. V informatike sú však koeficienty polynómov prvkami nejakej konečnej množiny, spravidla ide o konečné pole. Spolu s polynómami sa používajú tiež operácie sčitovania a násobenia polynómov, a je užitočné zaoberať sa polynómami spolu s týmito operáciami, teda okruhmi polynómov. Preto za najprv budeme venovať okruhom a ich vlastnostiam. Špeciálnym prípadom okruhov sú polia, s ktorými sme sa už stretli v lineárnej algebre.

Nasledujúci text je prepisom poznámok k prednáške Algebra. Nemá byť náhradou za učebnicu.

2 Okruhy, obory integrity a polia

Pripomeňme, že ak A je množina, tak ľubovoľné zobrazenie $A \times A \longrightarrow A$ sa nazýva binárna operácia na množine A. Ak toto zobrazenie označíme $\star$ $(+, .)$, tak obraz usporiadanej dvojice $(a, b) \in A \times A$ označujeme $a \star b$ $(a + b,\ a.b)$. Binárna operácia $\star$ na množine A sa nazýva asociatívna (komutatívna), ak pre všetky $a, b, c \in A$ platí $(a \star b) \star c = a \star (b \star c)$ (pre všetky $a, b \in A$ platí $a \star b = b \star a$). Prvok $e \in A$ sa nazýva neutrálny prvok operácie $\star$, ak pre všetky $a \in A$ platí $a \star e = e \star a = a$. Binárna operácia môže mať najviac jeden neutrálny prvok. Ak

binárna operácia na množine A má neutrálny prvok e a $a \in A$, tak prvok $b \in A$ sa nazýva inverzný k a, ak $a \star b = b \star a = e$. Ak $\star$ je asociatívna operácia na A, ktorá má neutrálny prvok, tak pre každé $a \in A$ existuje v A najviac jeden inverzný prvok a^{-1}, pričom platí: ak a^{-1} je inverzný prvok k a a b^{-1} je inverzný prvok k b, tak $b^{-1} \star a^{-1} = (a \star b)^{-1}$ a $(a^{-1})^{-1} = a$.

Definícia 2.1. *a) Usporiadaná trojica $(A, +, .)$, kde A je množina, $+$ a $.$ sú binárne operácie na A (sčitovanie a násobenie), sa nazýva okruh, ak platí:*
(1) Operácia $+$ je komutatívna a asociatívna.
(2) Existuje prvok $0 \in A$ tak, že pre všetky $a \in A$ $a + 0 = 0 + a = a$ (nulový prvok okruhu).
(3) Pre každé $a \in A$ existuje $b \in A$ tak, že $a + b = b + a = 0$ (prvok b sa nazýva opačný prvok k prvku a a označuje sa $-a$).
(4) Operácia $.$ je asociatívna.
(5) Pre každé $a, b, c \in A$ platí $a.(b + c) = a.b + a.c$ a tiež $(a + b).c = a.c + b.c$ (distributívnosť operácie $.$ vzhľadom na operáciu $+$).
b) Okruh $(A, +, .)$ sa nazýva komutatívny, ak pre každé $a, b \in A$ platí $a.b = b.a$, t. j. operácia násobenia je komutatívna.
c) Okruh $(A, +, .)$ sa nazýva okruh s jednotkou (unitárny okruh), ak existuje prvok $\mathbf{1} \in A$, $\mathbf{1} \neq 0$ tak, že pre každé $a \in A$ platí $a.\mathbf{1} = \mathbf{1}.a = a$ (jednotkový prvok okruhu; pre jeho odlíšenie od prirodzeného čísla 1 ho označujeme tučne, t. j. $\mathbf{1}$).
d) Komutatívny okruh s jednotkou $(A, +, .)$ sa nazýva obor integrity, ak pre každé $a, b \in A$ platí: Ak $a \neq 0$ a $b \neq 0$, tak aj $a.b \neq 0$ (ekvivatentne: Ak $a.b = 0$, tak $a = 0$ alebo $b = 0$).
e) Komutatívny okruh s jednotkou $(A, +, .)$ sa nazýva pole, ak pre každé $a \in A$, $a \neq 0$ existuje $c \in A$ tak, že $a.c = c.a = \mathbf{1}$ (prvok c sa nazýva inverzný prvok k a a označuje sa a^{-1}).

Príklady 2.1. *1) $(\mathbb{Z}, +, .)$ (s obvyklým sčitovaním a násobením) je obor integrity, ktorý nie je poľom, $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$ (s obvyklým sčitovaním a násobením) sú polia. $(\mathbb{N}, +, .)$ ani $(\mathbb{N}_0, +, .)$ (s obvyklým sčitovaním a násobením) nie sú okruhy.*

2) Nech $\mathcal{M}_{2x2}(\mathbb{R})$ je množina všetkých matíc typu $2x2$ nad $\mathbb{R}$, $+$ je operácia sčitovania matíc a $.$ je operácia násobenia matíc. Potom $(\mathcal{M}_{2x2}(\mathbb{R}), +, .)$ je okruh s jednotkou

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

ktorý nie je komutatívny. Platí totiž, že

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

3) Nech $n \in \mathbb{N}$, $n \geq 2$, $\mathbb{Z}_n = \{0, 1, ..., n-1\}$, pre každé $k, m \in \mathbb{Z}_n$ nech $k \oplus m$ je zvyšok po delení čísla $k + m$ číslom n a $k \odot m$ je zvyšok po delení čísla $k.m$ číslom n. Potom $\oplus$ a $\odot$ sú binárne operácie na $\mathbb{Z}_n$ a $(\mathbb{Z}_n, \oplus, \odot)$ je komutatívny okruh s jednotkou. Okruh $(\mathbb{Z}_4, \oplus, \odot)$ je komutatívny okruh s jednotkou, ktorý

nie je oborom integrity, lebo $2 \neq 0$ *a* $2 \odot 2 = 0$ *v* $(\mathbb{Z}_4, \oplus, \odot)$. *Vo všeobecnosti platí (vieme to z elementárnej teórie čísel), že ak* n *je prvočíslo, tak* $(\mathbb{Z}_n, \oplus, \odot)$ *je pole, ak* n *je zložené číslo, tak* $(\mathbb{Z}_n, \oplus, \odot)$ *nie je obor integrity.*

Z vyššie uvedených vlastností binárnych operácií (známych z lineárnej algebry) (resp. z vlastností operácie + v poliach a vektorových priestoroch) vyplýva, že v každom okruhu $(A, +, .)$ platí:

a) Existuje práve jeden nulový prvok v $(A, +, .)$.

b) Pre každé $a \in A$ existuje práve jeden opačný prvok $-a$ (lebo + je asociatívna).

c) Existuje najviac jeden jednotkový prvok v $(A, +, .)$.

d) Pre každé $a, b \in A$ platí $-(a + b) = (-a) + (-b)$ a tiež $-(-a) = a$.

e) Ak $a, b, c \in A$ a $a + b = a + c$, tak $b = c$.

Podobne ako v poliach sa ukáže, že v každom okruhu $(A, +, .)$ platí:

f) Pre každé $a \in A$ platí $a.0 = 0.a = 0$.

Skutočne, $a.0 + a.0 = a.(0 + 0) = a.0 = a.0 + 0$. Teda $a.0 + a.0 = a.0 + 0$ a podľa e) potom $a.0 = 0$. Podobne sa ukáže, že $0.a = 0$.

g) Pre každé $a, b \in A$ platí $(-a).b = a.(-b) = -(a.b)$.

K tomu stačí overiť, že $(-a).b$ $(a.(-b))$ je opačný prvok k $a.b$. Overme to pre $(-a).b$: $a.b + (-a).b = (a + (-a)).b = 0.b = 0$. Teda $(-a).b = -(a.b)$.

Okrem toho, pretože operácie + a . sú asociatívne, nemusíme písať zátvorky (stačí písať napr. $a + b + c + d$ resp. $a.b.c.d$, nezáleží ani na poradí prvkov v súčte a v prípade komutatívneho okruhu ani na poradí prvkov v súčine.

Odteraz sa budeme zaoberať hlavne komutatívnymi okruhmi s jednotkou (skrátene KOJ).

Veta 2.1. *1) KOJ* $(A, +, .)$ *je obor integrity vtedy a len vtedy, keď pre každé* $a, b, c \in A$, $a \neq 0$ *z rovnosti* $a.b = a.c$ *vyplýva* $b = c$ *(z rovnosti* $b.a = c.a$ *vyplýva* $b = c$*), t.j. v okruhu* $(A, +, .)$ *sa dá krátiť nenulovým prvkom zľava (aj sprava).*

2) Každé pole je obor integrity.

Dôkaz. 1) "⇒" Z rovnosti $a.b = a.c$ vyplýva, že platí $a.b + (-(a.c)) = a.b + a.(-c) = a.(b + (-c)) = 0$. Pretože $a \neq 0$ musí platiť $b + (-c) = 0$ a teda $b = c$.

"⇐" Nech $a \neq 0$, $b \neq 0$ a $a.b = 0$. Potom $a.b = a.0$ a pretože $a \neq 0$ dostávame, že $b = 0$. Dostali sme spor.

2) Nech $(A, +, .)$ je pole $a, b, c \in A$, $a \neq 0$ a $a.b = a.c$. K nenulovému prvku a existuje inverzný prvok a^{-1}. Potom $b = \mathbf{1}.b = a^{-1}.a.b = a^{-1}.a.c = \mathbf{1}.c = c$. Teda $b = c$ a preto, podľa 1)), je $(A, +, .)$ obor integrity. □

Nech $(A, +, .)$ je KOJ, $a \in A$. Prvok $a + a$ označujeme aj $2a$ a nazývame dvojnásobok prvku a, prvok $a.a$ označujeme aj a^2 a nazývame druhá mocnina prvku a. Je možné definovať ľubovoľný celočíselný násobok prvku a, respektíve ľubovoľnú mocninu a^n pre $n \in \mathbb{N}_0$.

Definícia 2.2. *Nech* $(A, +, .)$ *je KOJ,* $a \in A$ *a* $z \in \mathbb{Z}$. *Definujme z-násobok za prvku a nasledovne:*

1) Nech $z = n \in \mathbb{N}_0$. *Potom pre* $n = 0$ *definujeme* $0a = 0$ *(*0 *na pravej strane rovnosti je nulový prvok okruhu* $(A, +, .)$, 0 *na ľavej strane je celé číslo) . Pre*

každé $n \in \mathbb{N}_0$ definujeme $(n+1)a = na + a$. Tým je definované na pre všetky $n \in \mathbb{N}_0$.

2) Nech $z < 0$. Potom existuje $n \in \mathbb{N}$ také, že $z = -n$ a definujeme $za = -(na)$.

Z definície je zrejmé, že pre každé $z \in \mathbb{Z}$ je $za \in A$. Ďalej je napríklad zrejmé, že $3a = a+a+a$, $(-3)a = -(3a) = -(a+a+a) = (-a)+(-a)+(-a) = 3(-a)$. Matematickou indukciou sa ľahko dokáže, že pre každé $n \in \mathbb{N}$ platí $(-n)a = n(-a)$. Ak $z \in \mathbb{Z}$, $z < 0$ a $a \in A$, tak $-z \in N$ a potom $z.(-a) = (-(-z))(-a) = (-z)a$. Teda pre každé $z \in \mathbb{Z}$ a $a \in A$ platí $(-z)a = z(-a)$.

Veta 2.2. *Nech $(A, +, .)$ je KOJ, $a, b \in A$ a $z, z_1, z_2 \in \mathbb{Z}$ Potom platí:*
1) $(za).b = z(a.b) = a.(zb)$,
2) $za = (z\mathbf{1}).a$.
3) $z(a+b) = za + zb$.
4) $(z_1 + z_2)a = z_1 a + z_2 a$.
5) $(z_1(z_2 a) = (z_1.z_2)a$.

Dôkaz. 1) Ukážeme, že platí $(za).b = z(a.b)$. Najprv matematickou indukciou dokážeme, že výrok platí pre každé $n \in \mathbb{N}_0$: Pre $n = 0$ dostávame $0.b = 0$ a to platí. Nech výrok platí pre $n \in \mathbb{N}_0$, t. j. platí $(na).b = n(a.b)$. Potom $((n+1)a).b = ((na + a).b = (na).b + a.b = n(a.b) + a.b = (n+1)(a.b)$.

Nech teraz $z < 0$. Potom existuje $n \in N$ tak, že $z = -n$. Potom $(za).b = ((-n)a).b = (-(na)).b = (na).(-b) = n(a.(-b)) = n(-(a.b)) = (-n)(a.b) = z(a.b)$ (použili sme vlastnosť e) okruhov a platnosť pre n).

Rovnosť $a.(zb) = z(a.b)$ vyplýva teraz z dokázanej rovnosti a komutatívnosti násobenia.

2) $za = z(\mathbf{1}.a) = (z\mathbf{1}).a$ (podľa a)).

3) $z(a+b) = (z\mathbf{1}).(a+b) = (z\mathbf{1}).a + (z\mathbf{1}).b = za + zb$.

4) a 5) - cvičenie.

□

Definícia 2.3. *Nech $(A, +, .)$ je KOJ, $a \in A$ a $n \in \mathbb{N}_0$. Definujme n-tú mocninu a^n prvku a nasledovne:*

Pre $n = 0$ definujeme $a^0 = \mathbf{1}$. Pre každé $n \in \mathbb{N}_0$ definujeme $a^{n+1} = a^n.a$. Tým je definované a^n pre všetky $n \in \mathbb{N}_0$.

Z definície je zrejmé, že pre každé $n \in \mathbb{N}_0$ je a^n jednoznačne definovaný prvok okruhu $(A, +, .)$.

Matematickou indukciou sa ľahko dokážu nasledujúce vlastnosti mocnín v KOJ.

Veta 2.3. *Nech $(A, +, .)$ je KOJ, $a, b \in A$ a $m, k \in \mathbb{N}_0$ Potom platí:*
1) $(a.b)^n = a^n.b^n$.
2) $a^{n+k} = a^n.a^k$.
3) $(a^n)^k = a^{n.k}$.

V nasledujúcom texte bude niekedy užitočné používať pre KOJ označenie $(A, +, ., \mathbf{1})$, kde $\mathbf{1}$ je jednotkový prvok tohoto okruhu, namiesto označenia $(A, +, .)$. často tiež budeme pre okruhy aj KOJ používať zjednodušené označenie A.

Príklad 2.1. *Okruh $(\mathbb{Z}, +, .)$ je príkladom podokruhu okruhu $(Q, +, .)$. To znamená, že $\mathbb{Z} \subseteq \mathbb{Q}$, operácie sčitovania a násobenia v okruhu $(\mathbb{Z}, +, .)$ sú na množine $\mathbb{Z}$ totožné s operáciami sčitovania a násobenia v okruhu $(\mathbb{Q}, +, .)$. Podobne platí, že okruh $(\mathbb{Z}, +, .)$ je podokruh okruhu $(\mathbb{R}, +, .)$ a okruh $(\mathbb{Q}, +, .)$ je podokruh okruhu $(\mathbb{R}, +, .)$.*

Na druhej strane, okruh $(\mathbb{Z}_2, \oplus, \odot)$ nie je podokruh okruhu $(\mathbb{Z}_5, \oplus, \odot)$ lebo, napríklad, $1 \oplus 1 = 0$ v $(\mathbb{Z}_2, \oplus, \odot, 1)$ a $1 \oplus 1 = 2$ v $(\mathbb{Z}_5, \oplus, \odot, 1)$.

Definícia 2.4. *1) Okruh $(B, \oplus, \odot)$ sa nazýva podokruh okruhu $(A, +, .)$, ak $B \subseteq A$, pre každé $a, b \in B$ platí $a \oplus b = a + b$ aj $a \odot b = a.b$. V takomto prípade okruh $(A, +, .)$ sa nazýva rozšírením okruhu $(B, \oplus, \odot)$. Označenie: $(B, \oplus, \odot) \leq (A, +, .)$ alebo $B \leq A$ pri skrátenom označení okruhov.*

2) KOJ $(B, \oplus, \odot, \mathbf{1}_B)$ sa nazýva J-podokruh KOJ $(A, +, ., \mathbf{1})$, ak $(B, \oplus, \odot)$ je podokruh okruhu $(A, +, .)$ a $\mathbf{1}_B = \mathbf{1}$. Označenie: $(B, \oplus, \odot, \mathbf{1}_B) \leq_1 (A, +, ., \mathbf{1})$.

3) Ak $(B, \oplus, \odot, \mathbf{1}_B)$ aj $(A, +, ., \mathbf{1})$ sú polia a $(B, \oplus, \odot, \mathbf{1}_B) \leq_1 (A, +, ., \mathbf{1})$, tak j-podokruh $(B, \oplus, \odot, \mathbf{1}_B)$ sa nazýva podpole poľa $(A, +, ., \mathbf{1})$ a pole $(A, +, ., \mathbf{1})$ sa nazýva rozšírením poľa $(B, \oplus, \odot, \mathbf{1}_B)$.

3) KOJ $(B, \oplus, \odot, \mathbf{1}_B)$ sa nazýva J-podokruh KOJ $(A, +, ., \mathbf{1})$, ak $(B, \oplus, \odot)$ je podokruh okruhu $(A, +, .)$ a $\mathbf{1}_B = \mathbf{1}$. Označenie: $(B, \oplus, \odot, \mathbf{1}_B) \leq_1 (A, +, ., \mathbf{1})$.

V nasledujúcej vete budeme charakterizovať tie podmnožiny B okruhu $(A, +, .)$, ktoré určujú podokruh tohoto okruhu, t. j. na množine B existujú binárne operácie $\oplus$, $\odot$ tak, že $(B, \oplus, \odot$ je okruh a $(B, \oplus, \odot) \leq (A, +, .)$. Namiesto "$B$ určuje podokruh okruhu $(A, +, .)$" budeme hovoriť, že "B je podokruh okruhu $(A, +, .)$". Podobne pre podpole a J-podokruh.

Veta 2.4. *1) Neprázdna podmnožina B okruhu $(A, +, .)$ je podokruh okruhu $(A, +, .)$ práve vtedy, keď sú splnené nasledujúce podmienky:*
(p1) Pre všetky $a, b \in B$ platí $a + b \in B$.
(p2) Pre každé $a \in B$ platí $-a \in B$.
(p3) Pre všetky $a, b \in B$ platí $a.b \in B$.

2) Podmnožina B KOJ $(A, +, ., \mathbf{1})$ je J-podokruh KOJ $(A, +, ., \mathbf{1})$, práve vtedy, keď platia podmienky (p1), (p2), (p3) a tiež podmienka
(p4) $\mathbf{1} \in B$.

3) Podmnožina B poľa $(A, +, ., \mathbf{1})$ je podpole poľa $(A, +, ., \mathbf{1})$ práve vtedy keď sú splnené podmiedky (p1), (p2), (p3), (p4) a tiež podmienka
(p5) Pre každé $a \in B$, $a \neq 0$ platí $a^{-1} \in B$.

Dôkaz. 1) "⇒": Nech $B \subseteq A$ je podokruh okruhu $(A, +, .)$. Potom existujú binárne operácie $\oplus$, $\odot$ na B tak, že $(B, \oplus, \odot)$ je okruh a $(B, \oplus, \odot) \leq (A, +, .)$. Nech $a, b \in B$. Potom $a + b = a \oplus b \in B$ a tiež $a.b = a \odot b \in B$ a teda platí (p1) a (p3). Nech 0_B je nulový prvok v $(B, \oplus, \odot)$ a 0 je nulový prvok v $(A, +, .)$. Zrejme $0_B + 0_B = 0_B \oplus 0_B = 0_B = 0_B + 0$. Teda platí $0_B + 0_B = 0_B + 0$ a

preto $0_B = 0$. Nech teraz $a \in B$. Potom existuje opačný prvok $\ominus a \in B$, ktorý je opačným prvkom k a v okruhu $(B, \oplus, \odot)$. Ak $-a$ je opačný prvok k a v $(A, +, .)$, tak $a + (-a) = 0 = 0_B = a \oplus (\ominus a) = a + (\ominus a)$. Teda $a + (-a) = a + (\ominus a)$ a $(A, +, .)$ a preto $-a = \ominus a \in B$. Podmienka (p2) je dokázaná.

"$\Leftarrow$": Definujme pre každé $a, b \in B$ $a \oplus b = a + b$ a $a \odot b = a.b$. Pretože $a + b$ a $a.b$ sú jednoznačne určené prvky, ktoré podľa (p1) a (p3) patria do B, sú týmto definované binárne operácie na množine B. Ukážeme, že $(B, \oplus, \odot)$ je okruh. Ľahko sa overí, že operácie $\oplus$ a $\odot$ sú komutatívne, asociatívne a $\odot$ je distributívna vzhľadom na $\oplus$. Overme, napríklad, distributívnosť zľava. Nech $a, b, c \in B$. Potom $a \odot (b \oplus c) = a.(b + c) = a.b + a.c = a \odot b \oplus a \odot c$. Pretože B je neprázdna, existuje $a \in B$ a podľa (p2) potom aj $-a \in B$. Podľa (p1) $a + (-a) = 0 \in B$ a je zrejmé, že 0 je nulový prvok v $(B, \oplus, \odot)$. Teda $(B, \oplus, \odot)$ je okruh a z definície tohoto okruhu je jasné, že $(B, \oplus, \odot) \leq (A, +, .)$.

2) a 3) podobne, s využitím 1). □

Príklady 2.2. *1) Na množine $\mathbb{Z} \times \mathbb{Z}$ definujme operácie $+$ a $.$ tak, že pre každé $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$, $(a, b) + (c, d) = (a + c, b + d)$ a $(a, b).(c, d) = (a.c, b.d)$. Ľahko sa overí, že $(\mathbb{Z} \times \mathbb{Z}, +, .)$ je KOJ, jednotkovým prvkom v tomto okruhu je prvok $(1, 1)$. Uvažujme o podmnožine $B = \{(a, 0) : a \in \mathbb{Z}\}$ v tomto KOJ. Táto podmnožina spĺňa podmienky (p1), (p2) aj (p3) a preto je podokruhom okruhu $(\mathbb{Z} \times \mathbb{Z}, +, .)$ ale nespĺňa podmienku (p4) a teda to nie je J-podokruh KOJ $(\mathbb{Z} \times \mathbb{Z}, +, ., (1, 1))$. Pritom ale množina B s operáciami definovanými predpismi $(a, 0) + (b, 0) = (a + b, 0)$ a $(a, 0).(b, 0) = (a.b, 0)$, ktoré na množine B sú totožné s operáciami okruhu $(\mathbb{Z} \times \mathbb{Z}, +, .)$ je komutatívny okruh s jednotkovým prvkom $(1, 0)$.*

2) Podmnožina $\mathbb{Q}[\sqrt{2}] = \{a + b.\sqrt{2} : a, b \in \mathbb{Q}\}$ poľa $(\mathbb{R}, +, .)$ je podpole poľa reálnych čísel. Skutočne, nech $r, s \in \mathbb{Q}[\sqrt{2}]$, $r = a + b.\sqrt{2}$, $s = c + d.\sqrt{2}$, $a, b, c, d \in \mathbb{Q}$. Potom $r + s = (a + c) + (b + d).\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $-r = -(a + b.\sqrt{2}) = (-a) + (-b).\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $r.s = (a + b, \sqrt{2}).(c + d.\sqrt{2}) = (a.c + 2.b.d) + (a.d + b.c).\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, $1 = 1 + 0.\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ a ak $r \neq 0$, tak $a \neq 0$ alebo $b \neq 0$ (a potom $a^2 - 2.b^2 \neq 0$) a $r^{-1} = \frac{1}{a+b.\sqrt{2}} = \frac{a}{a^2-2.b^2} + \frac{-b}{a^2-2.b^2}.\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Teda podmienky (p1) - (p5) sú splnené.

Veta 2.5. *Ak A je J-podokruh oboru integrity B, tak A je obor integrity.*

Dôkaz. Je zrejmé, že A je KOJ a ak $a, b \in A$, $a \neq 0$, $b \neq 0$, tak $a.b \neq 0$ (je to súčin dvoch nenulových prvkov v obore integrity B). □

Ako dôsledok tejto vety dostávame, že ak F je pole a A je J-podokruh poľa F ($A \leq_1 F$), tak A je obor integrity.

Nasledujúca veta je, okrem iného, dôležitá pri definovaní okruhov polynómov.

Veta 2.6. *Nech B je KOJ (s jednotkovým prvkom $\mathbf{1}$), $A \leq_1 B$ a $u \in B$. Potom množina $A[u] = \{r \in B : \exists_{n \in \mathbb{N}_0} \exists_{a_0, \ldots a_n \in A}\ r = a_0 + a_1 u + \ldots + a_n u^n\}$ je podokruh okruhu B, ktorý má nasledujúce vlastnosti:*

a) $A \cup \{u\} \subseteq A[u]$.

b) Ak $C \leq_1 B$ a $A \cup \{u\} \subseteq C$, tak $A[u] \subseteq C$.

c) $A[u]$ je KOJ a $A \leq_1 A[u]$.

Teda $A[u]$ je v zmysle množinovej inklúzie najmenší podokruh okruhu B, ktorý obsahuje podokruh A a prvok u.

Dôkaz. Zrejme $\mathbf{1} \in A[u]$ (stačí zvoliť $n = 0$ a $a_0 = \mathbf{1}$). Nech $r, s \in A[u]$. Potom existujú $n, k \in N_0$ a $a_0, a_1, ..., a_n, b_0, b_1, ..., b_k \in A$ tak, že $r = a_0 + a_1u + ... + a_nu^n$ a $s = b_0 + b_1u + ... + b_ku^k$. Nech napríklad $k \leq n$. Potom, zrejme, $r + s = (a_0 + b_0) + (a_1 + b_1)u + ... + (a_k + b_k)u^k + ... + a_nu^n \in A[u]$ $(a_i + b_i \in A)$, $-r = (-a_0) + (-a_1)u + ... + (-a_n)u^n \in A[u]$ $(-a_i \in A)$ a $r.s = (a_0 + a_1u + ... + a_nu^n).(b_0 + b_1u + ... + b_ku^k) = a_0b_0 + (a_0b_1 + a_1b_0)u + ... + a_nb_ku^{n+k} \in A[u]$ $(r.s = c_0 + c_1u + ... + c_{n+k}u^{n+k}$, kde pre všetky $l \in \{0, ..., n+k\}$ platí $c_l = \sum_{i+j=l} a_ib_j \in A)$. Ukázali sme, že $A[u] \leq_1 B$.

a) Ak $a \in A$ a zvolíme $n = 0$, $a_0 = a \in A$, tak $a = a_0 \in A[u]$ a teda $A \subseteq A[u]$. Pre $n = 1$ $a_0 = 0 \in A$ a $a_1 = \mathbf{1} \in A$ dostávame, že $u = 0 + \mathbf{1}u \in A[u]$. Teda $A \cup \{u\} \subseteq A[u]$.

b) Nech $C \leq_1 B$ a $A \cup \{u\} \subseteq C$. Ak $r \in A[u]$, tak $r = a_0 + a_1u + ... + a_nu^n$, kde $n \in \mathbb{N}_0$, a pre všetky i je $a_i \in A$. Potom pre všetky i je $a_i \in C$, $u \in C$ a preto $r = a_0 + a_1u + ... + a_nu^n \in C$. Teda $A[u] \subseteq C$.

c) vyplýva z toho, že J-podokruh KOJ je KOJ, $A \leq_1 B$, $A \subseteq A[u]$, a $\mathbf{1}$ je jednotkový prvok v $A[u]$ aj v A.

□

Príklad 2.2. *Vieme, že $\mathbb{Z} \leq_1 \mathbb{R}$ a $\sqrt{2} \in \mathbb{R}$. Podľa predchádzajúcej vety $\mathbb{Z}[\sqrt{2}] = \{r \in \mathbb{R} : \exists_{n \in \mathbb{N}_0} \exists_{a_0, ... a_n \in \mathbb{Z}}\ r = a_0 + a_1.\sqrt{2} + ... + a_n.(\sqrt{2})^n\} = \{r \in \mathbb{R} : \exists a, b \in \mathbb{Z}\ r = a + b.\sqrt{2}\}$ je najmenší podokruh okruhu $\mathbb{R}$, ktorý obsahuje $\mathbb{Z}$ a číslo $\sqrt{2}$ (pri úprave sme využili skutočnosť, že ak $k \in \mathbb{N}$, tak $(\sqrt{2})^{2k} = 2^k$ a $(\sqrt{2})^{2k+1} = 2^k.\sqrt{2}$ pričom $2^k \in \mathbb{Z}$; napríklad $2 + 3.\sqrt{2} + 1.(\sqrt{2})^2 = 4 + 3.\sqrt{2}$).*

Obor integrity celých čísel $\mathbb{Z}$ je podokruh poľa racionálnych čísel $\mathbb{Q}$, resp., čo je to isté, pole $\mathbb{Q}$ je rozšírenie oboru integrity $\mathbb{Z}$, pričom platí: Pre každé racionálne číslo $r \in \mathbb{Q}$ existujú celé čísla $a, b \in \mathbb{Z}$, $b \neq 0$ také, že $r = a.b^{-1}$. Tento známy poznatok je možné zovšeobecniť pre každý obor integrity A.

Veta 2.7. *Ak A je obor integrity tak, existuje pole $\mathbb{Q}(A)$, ktoré je rozšírením oboru integrity A (t. j. A je podokruh $\mathbb{Q}(A)$) a pre ktoré platí: Pre každé $r \in \mathbb{Q}(A)$ existujú $a, b \in A$, $b \neq 0$ tak, že $r = a.b^{-1}$.*

Príklad 2.3. *Na množine $\mathbb{Z} \times \{0\}$ definujme operácie $\oplus$, $\odot$ takto: ak $(a, 0), (b, 0) \in \mathbb{Z} \times \{0\}$, tak $(a, 0) \oplus (b, 0) = (a + b, 0)$ a $(a, 0) \odot (b, 0) = (a.b, 0)$. Je zrejmé, že $(\mathbb{Z} \times \{0\}, \oplus, \odot)$ je KOJ (jednotkový prvok v tomto okruhu je $(1, 0)$ a že tento okruh má rovnaké vlastnosti ako okruh $(\mathbb{Z}, +, .)$. Ak stotožníme každé celé číslo a s usporiadanou dvojicou $(a, 0)$, tak operácia sčitovania $+$ v $(\mathbb{Z}, +, .)$ sa sa stotožní s operáciou $\odot$ v $(\mathbb{Z} \times \{0\}, \oplus, \odot)$. Teda ide vlastne o dva modely toho istého okruhu a formálne to vyjadríme tak, že okruh $(\mathbb{Z}, +, .)$ je izomorfný s okruhom $(\mathbb{Z} \times \{0\}, \oplus, \odot)$.*

Je teda účelné, pre porovnávanie vlastností okruhov, definovať pojem homomorfizmu KOJ, ktorého špeciálnym prípadom je pojem izomorfizmu KOJ.

Definícia 2.5. *Nech* $(A, +, ., \mathbf{1})$, $(B, +, ., \mathbf{1})$ *sú KOJ.*

1) Zobrazenie $f : A \longrightarrow B$ *sa nazýva homomorfizmus KOJ* $(A, +, ., \mathbf{1})$ *do KOJ* $(B, +, ., \mathbf{1})$*, ak platí:*

(h1) Pre každé $a, b \in A$, $f(a + b) = f(a) + f(b)$.

(h2) Pre každé $a, b \in A$, $f(a.b) = f(a).f(b)$.

(h3) $f(\mathbf{1}) = \mathbf{1}$.

Označenie: $f : (A, +, ., \mathbf{1}) \longrightarrow (B, +, ., \mathbf{1})$ *(resp.* $f : A \longrightarrow B$ *ak používame skrátené označenia okruhov).*

2) Homomorfizmus KOJ $f : (A, +, ., \mathbf{1}) \longrightarrow (B, +, ., \mathbf{1})$ *sa nazýva izomorfizmus KOJ* $(A, +, ., \mathbf{1})$ *na KOJ* $(B, +, ., \mathbf{1})$*, ak* f *je bijektívne zobrazenie. Ak existuje izomorfizmus KOJ* $(A, +, ., \mathbf{1})$ *na KOJ* $(B, +, ., \mathbf{1})$*, tak hovoríme že okruh* $(A, +, ., \mathbf{1})$ *je izomorfný s okruhom* $(B, +, ., \mathbf{1})$*, označenie:* $(A, +, ., \mathbf{1}) \cong (B, +, ., \mathbf{1})$.

3) Ak $f : (A, +, ., \mathbf{1}) \longrightarrow (B, +, ., \mathbf{1})$ *je homomorfizmus KOJ, tak množina* $J(f) = \{a \in A : f(a) = 0\}$ *sa nazýva jadro homomorfizmu* $f : (A, +, ., \mathbf{1}) \longrightarrow (B, +, ., \mathbf{1})$.

Pretože inými homomorfizmami (izomorfizmami) sa nebudeme zaoberať môžeme namiesto o homomorfizmoch KOJ (izomorfizmoch KOJ) hovoriť stručne o homomorfizmoch (izomorfizmoch).

Príklady 2.3. *1. Nech* $(\mathbb{Z} \times \{0\}, \oplus, \odot, (1, 0))$ *je okruh z predchádzajúceho príkladu. Potom zobrazenie* $f : Z \longrightarrow \mathbb{Z} \times \{0\}$ *definované predpisom* $f(a) = (a, 0)$ *je izomorfizmus okruhu* $(\mathbb{Z}, +, ., 1)$ *na okruh* $(\mathbb{Z} \times \{0\}, \oplus, \odot, (1, 0))$*. Skutočne, pre každé* $a, b \in \mathbb{Z}$ *platí* $f(a + b) = (a + b, 0) = (a, 0) \oplus (b, 0) = f(a) \oplus f(b)$, $f(a.b) = (a.b, 0) = (a, 0) \odot (b, 0) = f(a) \odot f(b)$ *a platí tiež* $f(1) = (1, 0)$*. Je tiež zrejmé, že* f *je bijektívne zobrazenie.* $J(f) = \{0\}$.

2. Zobrazenie $f : (\mathbb{Z}, +, ., 1) \longrightarrow (\mathbb{Q}, +, ., 1)$ *dané predpisom* $f(a) = a$ *je homomorfizmus KOJ* $(\mathbb{Z}, +, ., 1)$ *do KOJ* $(\mathbb{Q}, +, ., 1)$. $J(f) = \{0\}$

3. Nech $(A, +, ., \mathbf{1})$ *je ľubovoľný KOJ. Potom existuje práve jeden homomorfizmus okruhu* $(\mathbb{Z}, +, ., 1)$ *do okruhu* $(A, +, ., \mathbf{1})$*. Tento homomorfizmus je daný predpisom* $f(z) = z\mathbf{1}$.

4. Zobrazenie $f : \mathbb{Z} \longrightarrow \mathbb{Z}_5$ *dané predpisom* $f(a) =$ *zvyšok po delení čísla* a *číslom 5 je homomorfizmus* $(\mathbb{Z}, +, .)$ *do* $(\mathbb{Z}_5, +, .)$. $J(f) = \{5a : a \in \mathbb{Z}\} = [0]_5$.

5) Zobrazenie $f : (\mathbb{Z} \times \{0\}, \oplus, \odot, (1, 0)) \longrightarrow (\mathbb{Z} \times \mathbb{Z}, +, ., (1, 1))$ *dané predpisom* $f(a, 0) = (a, 0)$ *nie je homomorfizmus, lebo* $f(1, 0) = (1, 0) \neq (1, 1)$.

6) Nech $\mathbb{C}$ *je pole komplexných čísel. Potom zobrazenie* $f : \mathbb{C} \longrightarrow \mathbb{C}$ *dané predpisom* $f(a + bi) = a - bi$ *je izomorfizmus (a* $f^{-1} = f$*).*

V nasledujúcej vete sformulujeme niekoľko základných vlastností homomorfizmov KOJ.

Veta 2.8. *Nech* A, B *sú KOJ a* $f : A \longrightarrow \mathcal{B}$ *je homomorfizmus. Potom platí:*

(1) $f(0) = 0$.

(2) Pre všetky $a \in A$ *platí* $f(-a) = -f(a)$.

(3) Pre všetky $a \in A$ *a všetky* $z \in \mathbb{Z}$ *platí* $f(za) = zf(a)$.

(4) Ak $a \in A$ *a* a *má inverzný prvok* a^{-1}*, tak aj* $f(a)$ *má inverzný prvok* $f(a)^{-1}$ *a platí* $f(a)^{-1} = f(a^{-1})$.

Dôkaz. (1) $f(0) = f(0) + 0 = f(0) + f(0) + (-f(0)) = f(0+0) + (-f(0)) = f(0) + (-f(0)) = 0$.

(2) Nech $a \in A$. Potom $f(-a) = f(-a) + 0 = f(-a) + f(a) + (-f(a)) = f((-a) + a) + (-f(a)) = f(0) + (-f(a)) = 0 + (-f(a)) = -f(a)$.

(3) Cvičenie (pre $z \geq 0$ to dokážeme matematickou indukciou a potom pre $z < 0$ využijeme (2).

(4) Nech $a \in A$ taký, že existuje a^{-1}. Potom $f(a^{-1}).f(a) = f(a^{-1}.a) = f(\mathbf{1}) = \mathbf{1}$. Teda $f(a^{-1})$ je inverzný prvok k $f(a)$ v okruhu B a pretože k $f(a)$ existuje najviac jeden inverzný prvok, platí $f(a^{-1}) = f(a)^{-1}$.

□

V nasledujúcej vete ukážeme, že zložené zobrazenie z dvoch homomorfizmov je tiež homomorfizmus a inverzné zobrazenie k izomorfizmu je izomorfizmus. Teda ak KOJ A je izomorfný s KOJ B tak aj B je izomorfný s A. Môžeme teda hovoriť, že A a B sú izomorfné.

Veta 2.9. *(1)Ak $f : A \longrightarrow B$ a $g : B \longrightarrow C$ sú homomorfizmy (izomorfizmy) KOJ, tak aj $g \circ f : A \longrightarrow C$ je homomorfizmus (izomorfizmus) KOJ.*

(2) Ak $f : A \longrightarrow B$ je izomorfizmus KOJ, tak aj $f^{-1} : B \longrightarrow A$ je izomorfizmus KOJ.

Dôkaz. (1) Nech $a, b \in A$. Potom $g \circ f(a+b) = g(f(a+b)) = g(f(a) + f(b)) = g(f(a)) + g(f(b)) = g \circ f(a) + g \circ f(b)$. Podobne sa ukáže, že $g \circ f(a.b) = g \circ f(a).g \circ f(b)$. Nakoniec, $g \circ f(\mathbf{1}) = g(f(\mathbf{1})) = g(\mathbf{1}) = \mathbf{1}$. Teda $g \circ f$ je homomorfizmus. Je známe, že zloženie dvoch bijektívnych zobrazení je bijektívne zobrazenie.

(2) Pretože f je bijektívne zobrazenie, existuje inverzné zobrazenie $f^{-1} : B \longrightarrow A$, ktoré je tiež bijektívne. Stačí ukázať, že f^{-1} je homomorfizmus. Nech $c, d \in B$. Potom $f(f^{-1}(c+d)) = c + d = f(f^{-1}(c)) + f(f^{-1}(d)) = f(f^{-1}(c) + f^{-1}(d))$. Pretože f je prosté zobrazenie a $f(f^{-1}(c+d) = f(f^{-1}(c) + f^{-1}(d))$, platí $f^{-1}(c+d) = f^{-1}(c) + f^{-1}(d)$. Podobne sa ukáže, že $f^{-1}(c.d) = f^{-1}(c).f^{-1}(d)$. Platí tiež $f(f^{-1}(\mathbf{1})) = \mathbf{1} = f(\mathbf{1})$ a pretože f je prosté zobrazenie, dostávame, že $f^{-1}(\mathbf{1}) = \mathbf{1}$. Teda f^{-1} je izomorfizmus. □

3 Pojem polynómu a okruhu polynómov

Všade v nasledujúcom texte budeme pod okruhom rozumieť vždy komutatívny okruh s jednotkovým prvkom (KOJ). Jednotkový prvok okruhu budeme označovať spravidla $\mathbf{1}$. Pripomeňme, že vždy platí $\mathbf{1} \neq 0$.

K definovaniu pojmu polynóm využijeme vetu 2.6.

Príklad 3.1. *Pole $\mathbb{R}$ je KOJ, $\mathbb{Z}$ je podokruh okruhu $\mathbb{R}$, ($\mathbb{Z} \leq_1 \mathbb{R}$) a $\sqrt{2} \in \mathbb{R}$. Potom (pozri príklad 2.2) $\mathbb{Z}[\sqrt{2}] = \{a_0 + a_1\sqrt{2} + ... + a_n(\sqrt{2})^n : n \in \mathbb{N}_0,\ a_0, a_1, ..., a_n \in \mathbb{Z}\} = \{c_0 + c_1\sqrt{2} : c_0, c_1 \in \mathbb{Z}\}$ ($(\sqrt{2})^{2k} = 2^k \in \mathbb{Z}$, $(\sqrt{2})^{2k+1} = 2^k\sqrt{2}$). Vyjadrenie prvkov $\mathbb{Z}[u]$ v tvare $a_0 + a_1\sqrt{2} + ... + a_n(\sqrt{2})^n$, $n \in \mathbb{N}_0,\ a_0, a_1, ..., a_n \in \mathbb{Z}$ nie je jednoznačné, napríklad $2 + 1\sqrt{2} + 2(\sqrt{2})^2 = 6 + 1\sqrt{2}$, $2 + 0\sqrt{2} + (-1)(\sqrt{2})^2 = 0$.*

Vyjadrenie prvkov okruhu $\mathbb{Z}[\sqrt{2}]$ v tvare $a_0 + a_1\sqrt{2} + ... + a_n(\sqrt{2})^n,\ n \in \mathbb{N}_0,\ a_0, a_1, ..., a_n \in \mathbb{Z}$ pripomína polynómy s koeficientami v okruhu $\mathbb{Z}$ ale toto vyjadrenie nie je jednoznačné. Je prirodzené žiadať, aby každý prvok okruhu polynómov s koeficientami v KOJ A mal jednoznačné vyjadrenie v tvare $a_0 + a_1u + ... + a_nu^n,\ n \in \mathbb{N}_0,\ a_0, a_1, ..., a_n \in A$, špeciálne aj nulový prvok 0. To znamená, že ak $0 = a_0 + a_1u + ... + a_nu^n,\ \ n \in \mathbb{N}_0,\ a_0, a_1, ..., a_n \in A$, tak $a_0 = a_1 = ... = a_n = 0$. Touto vlastnosťou sú charakterizované tie prvky u, ktoré sú vhodné na definovanie okruhu polynómov.

Definícia 3.1. *Nech B je KOJ, $A \leq_{\mathbf{1}} B$ a $u \in B$.*

a) Prvok u sa nazýva algebraický nad A, ak existujú $n \in \mathbb{N}_0$, $a_0, a_1, ..., a_n \in A$, tak, že $a_0 + a_1u + ... + a_nu^n = 0$, pričom pre aspoň jedno $i \in \{0, ..., n\}$ platí $a_i \neq 0$.

b) Prvok u sa nazýva neurčitá nad A alebo tiež transcendentný nad A, ak nie je algebraický nad A, t. j. pre každé $n \in \mathbb{N}_0$ a $a_0, a_1, ..., a_n \in A$ z rovnosti $a_0 + a_1u + ... + a_nu^n = 0$ vyplýva, že $a_0 = a_1 = ... = a_n = 0$.

Príklad 3.2. *1) Prvok $\sqrt{2} \in \mathbb{R}$ je algebraický prvok nad $\mathbb{Z}$, lebo existuje $2 \in \mathbb{N}_0$, $2, 0, -1 \in \mathbb{Z}$ tak. že $2 + 0\sqrt{2} + (-1)(\sqrt{2})^2 = 0$, pričom $2 \neq 0$, $-1 \neq 0$.*

2) Ak $A \leq_{\mathbf{1}} B$, tak každý prvok $a \in A$ je algebraický nad A, pretože $(-a) + \mathbf{1}a = 0$, $-a, \mathbf{1} \in A$ a $\mathbf{1} \neq 0$.

3) Uvažujme o okruhu $(\mathbb{R}^{\mathbb{R}}, +, .)$, kde $\mathbb{R}^{\mathbb{R}}$ je množina všetkých zobrazení $\mathbb{R} \longrightarrow \mathbb{R}$, $+$, $.$ sú binárne operácie na množine $\mathbb{R}^{\mathbb{R}}$ definované nasledovne (obvyklý súčet a súčin reálnych funkcií): Ak $f, g \in \mathbb{R}^{\mathbb{R}}$, tak $f + g : \mathbb{R} \longrightarrow \mathbb{R}$ je zobrazenie také, že pre každé $t \in \mathbb{R}$ platí $(f + g)(t) = f(t) + g(t)$ a $f.g : \mathbb{R} \longrightarrow \mathbb{R}$ je zobrazenie také, že pre každé $t \in \mathbb{R}$ platí $(f.g)(t) = f(t).g(t)$. Ľahko sa overí, že $(\mathbb{R}^{\mathbb{R}}, +, .)$ je KOJ, nulový prvok (jednotkový prvok) v tomto okruhu je zobrazenie $\overline{0} : \mathbb{R} \longrightarrow \mathbb{R}$ ($\overline{1} : \mathbb{R} \longrightarrow \mathbb{R}$) také že pre každé $t \in \mathbb{R}$ platí $\overline{0}(t) = 0$ ($\overline{1}(t) = 1$).

Pre každé $a \in \mathbb{R}$ označme $\overline{a}$ konštantné zobrazenie $\mathbb{R} \longrightarrow \mathbb{R}$, pre ktoré $\overline{a}(t) = a$ pre všetky $t \in \mathbb{R}$. Nech $\overline{\mathbb{R}} = \{\overline{a} :\ a \in \mathbb{R}\}$. Potom $\overline{\mathbb{R}}$ je neprázdna podmnožina okruhu $(\mathbb{R}^{\mathbb{R}}, +, .)$ a pretože pre každé $\overline{a}, \overline{b} \in \overline{\mathbb{R}}$ platí $\overline{a} + \overline{b} = \overline{a + b} \in \overline{\mathbb{R}}$, $-(\overline{a}) = \overline{(-a)} \in \overline{\mathbb{R}}$, $\overline{a}.\overline{b} = \overline{a.b} \in \overline{\mathbb{R}}$ a $\overline{1} \in \overline{\mathbb{R}}$ dostávame, že $\overline{\mathbb{R}}$ je podokruh okruhu $(\mathbb{R}^{\mathbb{R}}, +, .)$ obsahujúci jednotku okruhu $(\mathbb{R}^{\mathbb{R}}, +, .)$ (teda J-podokruh), t.j. $\overline{\mathbb{R}} \leq_1 (\mathbb{R}^{\mathbb{R}}, +, .)$.

Označme id identické zobrazenie $\mathbb{R} \longrightarrow \mathbb{R}$. Je to zobrazenie definované predpisom $id(t) = t$. Zrejme $id \in \mathbb{R}^{\mathbb{R}}$. Ukážeme, že id je neurčitá nad $\overline{\mathbb{R}}$. Sporom: Nech id je algebraický prvok nad $\overline{\mathbb{R}}$. Potom existujú $n \in \mathbb{N}_0$ a $\overline{a_0}, \overline{a_1}, ..., \overline{a_n} \in \overline{\mathbb{R}}$ tak, že $\overline{a_0} + \overline{a_1}id + ... + \overline{a_n}(id)^n = \overline{0}$ a pre aspoň jedno $i \in \{0, ..., n\}$ je $\overline{a_i} \neq \overline{0}$. Nech $k \in \{0, ..., n\}$ je najväčšie číslo, pre ktoré $\overline{a_k} \neq \overline{0}$. Potom $\overline{a_{k+1}} = ... = \overline{a_n} = \overline{0}$ a platí $\overline{a_0} + \overline{a_1}id + ... + \overline{a_k}id^k = \overline{0}$. Nech $f = \overline{a_0} + \overline{a_1}id + ... + \overline{a_k}(id)^k$. Potom $f = \overline{0}$ a súčasne pre každé $t \in \mathbb{R}$ $f(t) = (\overline{a_0} + \overline{a_1}id + ... + \overline{a_k})(t) = \overline{a_0}(t) + \overline{a_1}(t)id(t) + ... + \overline{a_k}(t)id(t)^k = a_0 + a_1t + ... + a_kt^k$. Pretože $f = \overline{0}$ pre jej $k-tu$ deriváciu $f^{(k)}$ platí $f^{(k)} = \overline{0}$. Na druhej strane z matematickej analýzy vieme, že pre každé $t \in \mathbb{R}$ platí $f^{(k)}(t) = (k!)a_k$, pričom $(k!)a_k \neq 0$. Dostali sme spor a preto je id neurčitá nad $\overline{\mathbb{R}}$.

Veta 3.1. *Nech B je KOJ, $A \leq_{\mathbf{1}} B$, $x \in B$ je neurčitá nad A a $f(x) =$*

$a_0 + a_1x + ... + a_nx^n, g(x) = b_0 + b_1x + ... + b_kx^k \in A[x]$ *(*$a_i, b_j \in A$*). Potom platí:*

1) $f(x) = 0$ *vtedy a len vtedy keď* $a_0 = a_1 = ... = a_n = 0$.

2) Ak $a_n \neq 0$, $b_k \neq 0$, *tak* $f(x) = g(x)$ *vtedy a len vtedy, keď* $n = k$ *a pre všetky* $i \in \{0, ..., n\}$ *platí* $a_i = b_i$.

Dôkaz. 1) Ak $f(x) = a_0 + a_1x + ... + a_nx^n = 0$, tak, podľa definície neurčitej platí $a_0 = a_1 = ... = a_n = 0$. Obrátene, ak $a_0 = a_1 = ... = a_n = 0$, tak, zrejme, $f(x) = 0$.

2) Nech $f(x) = g(x)$, Potom $h(x) = f(x) - g(x) = 0$. Nech $n \neq k$. Potom, ak $n > k$ tak $h(x) = (a_0 - b_0) + ... + (a_k - b_k)x^k + ... + a_nx^n$. Podľa 1) je potom $a_n = 0$ a to je spor. Ak $n < k$, tak $h(x) = (a_0 - b_0) + ... + (a_n - b_n)x^n + ... + (-b_k)x^k$ a podľa 1) potom $-b_k = 0 = b_k$, čo je opäť spor. Teda platí $n = k$. Potom máme $h(x) = (a_0 - b_0) + ... + (a_n - b_n)x^n$ a podľa 1) pre všetky $i \in \{0, ..., n\}$ platí $a_i - b_i = 0$ a teda $a_i = b_i$. Dôkaz obráteného tvrdenia je zrejmý. □

Z predchádzajúcej vety vyplýva, že ak x je neurčitá nad KOJ A, tak v okruhu $A[x]$ je vyjadrenie každého nenulového prvku v tvare $a_0 + ... + a_nx^n$, kde $n \in \mathbb{N}_0$, $a_0, ...a_n \in A$ a $a_n \neq 0$, jednoznačné a teda okruh $A[x]$ je vhodný model na štúdium polynómov s koeficientami z okruhu A.

Definícia 3.2. *a) Nech* B *je KOJ,* $A \leq_1 B$ *a* $x \in B$ *je neurčitá (transcendentný prvok) nad* A. *Potom okruh* $A[x]$ *(podokruh okruhu* B*) sa nazýva okruh polynómov v neurčitej* x *nad okruhom* A *a prvky okruhu* $A[x]$ *sa nazývajú polynómy nad okruhom* A *(v neurčitej* x*). Nulový prvok okruhu* $A[x]$ *sa nazýva nulový polynóm. Polynómy v neurčitej* x *budeme označovať* $f(x)$, $g(x)$, $h(x)$, ..., $p(x)$, ... *a podobne. Ak* $f(x) = a_0 + a_1x + ... + a_nx^n \in A[x]$, *tak prvky* $a_0, a_1, ..., a_n \in A$ *sa nazývajú koeficienty polynómu* $f(x)$, *prvky* $a_0, a_1x, ..., a_nx^n$ *sa nazývajú členy* $f(x)$. *Ak* $f(x) = a_0 + a_1x + ... + a_nx^n \in A[x]$ *je nenulový polynóm a* $a_n \neq 0$, *tak toto vyjadrenie sa nazýva základný tvar polynómu* $f(x)$, *prvok* a_n *sa nazýva vedúci koeficient a prvok* a_nx^n *vdúci člen polynómu* $f(x)$. *Základný tvar nulového polynómu je* 0.

b) Ak $f(x) \in A[x]$, *tak stupeň polynómu* $f(x)$, *ktorý označujeme* $stf(x)$ *je definovaný nasledovne: Ak* $f(x) = a_0 + a_1x + ... + a_nx^n$ *a* $a_n \neq 0$, *tak* $stf(x) = n$. *Ak* $f(x) = 0$, *tak* $stf(x) = -\infty$.

Ak $f(x)$ je nenulový polynóm, tak $stf(x) \in \mathbb{N}_0$.

Pri vyjadrení polynómu $f(x) \in A[x]$ v tvare $f(x) = a_0 + a_1x + ... + a_nx^n$ budeme vždy predpokladať, že $a_0, a_1, ..., a_n \in A$.

Nech $f(x) = a_0 + a_1x + ... + a_nx^n$, $g(x) = b_0 + b_1x + ...b_kx^k$ sú polynómy z $A[x]$. Pre počítanie s polynómami je užitočné vedieť, že $f(x).g(x) = (a_0 + a_1x + ... + a_nx^n).(b_0 + b_1x + ...b_kx^k) = a_0b_0 + (a_0b_1 + a_1b_0)x + ... + a_nb_kx^{n+k} = c_0 + c_1x + ... + c_lx^l + ... + c_{n+k}x^{n+k}$, kde pre všetky $l \in \{0, 1, ..., n + k\}$ platí $c_l = \sum_{i+j=l} a_ib_j$ (ak $l \leq n$ a $l \leq k$, tak $c_l = a_0b_l + a_1b_{l-1} + a_2b_{l-2} + ... + a_lb_0$). Ak $n \geq k$, tak $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_k + b_k)x^k + ... + a_nx^n$.

Príklad 3.3. *Nech $f(x) = 1 + x^2$, $g(x) = 2$ sú polynómy z okruhu polynómov $\mathbb{Z}[x]$. Vedúci koeficient $f(x)$ je 1, vedúci člen $f(x)$ je x^2, vedúci koeficient aj vedúci člen $g(x)$ je 2, $stf(x) = 2$, $stg(x) = 0$.*

4 Základné vlastnosti okruhov polynómov

Z definície okruhu polynómov a vety 2.6.c) vyplýva, že každý okruh polynómov je KOJ.

Veta 4.1. *Okruh polynómov $A[x]$ je obor integrity vtedy a len vtedy, keď A je obor integrity.*

Dôkaz. "$\Rightarrow$" Nech $A[x]$ je obor integrity. Pretože $A \leq_1 A[x]$, podľa vety 2.5 A je obor integrity.

"$\Leftarrow$" Nech A je obor integrity, $f(x)$, $g(x)$ sú nenulové polynómy z $A[x]$. Potom $f(x) = a_0 + a_1x + ... + a_nx^n$, $a_n \neq 0$, $g(x) = b_0 + b_1x + ...b_kx^k$, $b_k \neq 0$ a $f(x).g(x) = c_0 + c_1x + ... + c_{n+k}x^{n+k}$, kde $c_{n+k} = a_nb_k$. Pretože $a_n, b_k \in A$, A je obor integrity a $a_n \neq 0$, $b_k \neq 0$, platí $c_{n+k} \neq 0$ a preto $f(x).g(x) \neq 0$. Teda $A[x]$ je obor integrity. □

V súvislosti so stupňami polynómov je účelné prijať nasledujúcu dohodu:

Dohoda. Pre každé $n \in \mathbb{N}_0$ platí $-\infty < n$, $n + (-\infty) = (-\infty) + n = -\infty = (-\infty) + (-\infty)$.

Veta 4.2. *Nech $A[x]$ je okruh polynómov, $f(x), g(x) \in A[x]$. Potom platí:*

1) $st(f(x) + g(x)) \leq max\{stf(x), stg(x)\}$,

2) $st(f(x).g(x)) \leq stf(x) + stg(x)$ a v prípade, že A je obor integrity, tak $st(f(x).g(x)) = stf(x) + stg(x)$.

Dôkaz. 1) - na cvičení

2) Ak $f(x) = 0$, tak $f(x).g(x) = 0$ a $st(f(x).g(x)) = -\infty = -\infty + stg(x) = stf(x) + stg$. Podobne v prípade, ak $g(x) = 0$.

Nech $f(x) \neq 0$, $g(x) \neq 0$. Potom $f(x) = a_0 + a_1x + ... + a_nx^n$, $a_n \neq 0$, $stf(x) = n$, $g(x) = b_0 + b_1x + ...b_kx^k$, $b_k \neq 0$, $stg(x) = k$ a $f(x).g(x) = c_0 + c_1x + ... + c_{n+k}x^{n+k}$, kde $c_{n+k} = a_nb_k$. Zrejme $st(f(x).g(x)) \leq n + k = stf(x) + stg(x)$. Ak A je obor integrity, tak $c_{n+k} = a_nb_k \neq 0$ a preto $st(f(x).g(x)) = n + k = stf(x) + stg(x)$. □

Príklad 4.1. *1) Nech $f(x) = 1 + x^2, g(x) = 1 - x^2 \in \mathbb{Z}(x)$. Potom $f(x) + g(x) = 2$ a $st(f(x) + g(x)) = 0 < 2 = max\{stf(x), stg(x)\}$.*

2) Nech $f(x) = 2x, g(x) = 1 + 3x \in \mathbb{Z}_6[x]$, ($\mathbb{Z}_6$ nie je obor integrity). Potom $f(x).g(x) = 2x$ a $st(f(x).g(x)) = 1 < 2 = stf(x) + stg(x)$.

Definícia 4.1. *Nech $A[x]$ je okruh polynómov nad KOJ A v neurčitej x, $f(x) = a_0 + a_1x + ... + a_nx^n \in A[x]$, B je KOJ, $A \leq_1 B$ a $c \in B$. Potom prvok $f(c) = a_0 + a_1c + ... + a_nc^n$ okruhu B sa nazýva hodnota polynómu $f(x)$ v prvku c. Ak $f(c) = 0$, tak c sa nazýva koreň polynómu $f(x)$.*

Príklad 4.2. *1) Číslo $\sqrt{2} \in \mathbb{R}$ je koreň polynómu $f(x) = 2 - x^2 \in \mathbb{Z}[x]$.*

2) Ak $g(x) = 2 + x + x^2 \in \mathbb{Z}[x]$, tak $g(\sqrt{2}) = 4 + \sqrt{2}$ je hodnota $g(x)$ v čísle $\sqrt{2} \in \mathbb{R}$.

3) Ak $h(x) = a_0 \in \mathbb{Z}[x]$, $a_0 \in \mathbb{Z}$, tak $h(\sqrt{2}) = a_0$.

4) Ak $f(x) = a_0 \in A[x]$ a $a_0 \neq 0$ (t. j. $stf(x) = 0$), tak $f(x)$ nemá žiadny koreň. Ak $f(x) = 0$, tak každý prvok okruhu A je koreň $f(x)$.

Veta 4.3. *(Dosadzovacie pravidlo) Nech $A[x]$ je okruh polynómov nad KOJ A v neurčitej x, B je KOJ, $A \leq_1 B$ a $u \in B$. Potom existuje práve jeden homomorfizmus $\sigma : A[x] \longrightarrow A[u]$ taký, že pre každé $a \in A$ platí $\sigma(a) = a$ a $\sigma(x) = u$. Tento homomorfizmus je daný predpisom $\sigma(f(x)) = f(u)$ a je surjektívny. Ak u je neurčitá nad A, tak σ je izomorfizmus.*

Dôkaz. Nech $\sigma : A[x] \longrightarrow A[u]$ je zobrazenie dané predpisom $\sigma(f(x)) = f(u)$. Ukážeme, že je to homomorfizmus okruhov.

Nech $f(x), g(x) \in A[x]$, $f(x) = a_0 + a_1x + ... + a_nx^n$, $g(x) = b_0 + b_1x + ...b_kx^k$. Potom $f(u) = a_0 + a_1u + ... + a_nu^n$, $g(u) = a_0 + a_1u + ... + a_ku^k$.

Nech $h(x) = f(x) + g(x)$. Potom, ak $n \geq k$, $h(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_k + b_k)x^k + ... + a_nx^n$ a $h(u) = (a_0 + b_0) + (a_1 + b_1)u + ... + (a_k + b_k)u^k + ... + a_nu^n = a_0 + a_1u + ... + a_ku^k + ... + a_nu^n + b_0 + b_1 + ...b_ku^k = f(u) + g(u)$. Podobne aj pre $n \leq k$ dostaneme, že platí $h(u) = f(u) + g(u)$.

Nech teraz $r(x) = f(x).g(x)$. Potom $r(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + ... + a_nb_kx^{n+k}$ a $f(u).g(u) = (a_0 + a_1u + ... + a_nu^n).(b_0 + b_1 + ...b_ku^k) = a_0b_0 + (a_0b_1 + a_1b_0)u + ... + a_nb_ku^{n+k} = r(u)$.

Teda pre ľubovoľné polynómy $f(x), g(x) \in A[x]$ platí $\sigma(f(x) + g(x)) = \sigma(h(x)) = h(u) = f(u) + g(u) = \sigma(f(x)) + \sigma(g(x))$ aj $\sigma(f(x).g(x)) = \sigma(r(x)) = r(u) = f(u).g(u) = \sigma(f(x)).\sigma(g(x))$ a preto je σ homomorfizmus okruhu $A[x]$ do $A[u]$.

Nech $r \in A[u]$. Potom $r = a_0 + a_1u + ... + a_nu^n$, $a_0, a_1, ..., a_n \in A$. Pre polynóm $f(x) = a_0 + a_1x + ... + a_nx^n \in A[x]$ platí $\sigma(f(x)) = f(u) = r$ a teda σ je surjektívne zobrazenie.

Jednoznačnosť σ: Nech $\tau : A[x] \longrightarrow A[u]$ je homomorfizmus pre ktorý platí, že $\tau(a) = a$ pre každé $a \in A$ a $\tau(x) = u$. Nech $f(x) \in A[x]$, $f(x) = a_0 + a_1x + ... + a_nx^n$. Potom $\tau(f(x)) = \tau(a_0 + a_1x + ... + a_nx^n) = \tau(a_0) + \tau(a_1x) + ... + \tau(a_nx^n) = \tau(a_0) + \tau(a_1).\tau(x) + ... + \tau(a_n).\tau(x^n) = a_0 + a_1u + ... + a_nu^n = f(u) = \sigma(f(x))$. Teda $\tau = \sigma$.

Nech u je neurčitá nad A a $f(x) \in A[x]$, $f(x) = a_0 + a_1x + ... + a_nx^n$, $(a_i \in A)$. Nech $\sigma(f(x)) = f(u) = 0$. Potom $a_0 + a_1u + ... + a_nu^n = 0$ a pretože u je neurčitá nad A, dostávame, že $a_0 = a_1 = ... = a_n = 0$. Z toho vyplýva, že $f(x) = 0$. Nech teraz $g(x), h(x) \in A[x]$, pre ktoré $\sigma(g(x)) = \sigma(h(x))$. Potom $\sigma(g(x)) - \sigma(h(x)) = 0$ a $\sigma(g(x) - h(x)) = \sigma(g(x)) - \sigma(h(x)) = 0$ Preto $g(x) - h(x) = 0$ a teda $g(x) = h(x)$. Ukázali sme, že v tomto prípade je σ aj injektívne a preto je σ izomorfizmus $A[x] \longrightarrow A[u]$. □

Príklad 4.3. *Nech $f(x), g(x), h(x), r(x)$ sú polynómy z okruhu polynómov $A[x]$, $f(x) = g(x).h(x) + r(x)$ a $c \in A$. Potom platí $f(c) = g(c).h(c) + r(c)$. Skutočne, nech $\sigma : A[x] \longrightarrow A[c] = A$ je homomorfizmus z predchádzajúcej vety.*

Potom $f(c) = \sigma(f(x)) = \sigma(g(x).h(x) + r(x)) = \sigma(g(x).h(x)) + \sigma(r(x)) = \sigma(g(x)).\sigma(h(x)) + \sigma(r(x)) = g(c).h(c) + r(c)$.

Konkrétne, ak $f(x) = (1 + x^2 - x^3)(2 - x^2) + (1 + x)$ *je polynóm v* $\mathbb{Z}[x]$, *tak* $f(2) = (1 + 2^2 - 2^3)(2 - 2^2) + (1 + 2) = 9$.

Z predchádzajúcej vety vyplýva, že ak A je KOJ a x, y sú neurčité nad A, tak okruhy polynómov $A[x]$, $A[y]$ sú izomorfné a zobrazenie, ktoré každému polynómu $f(x) = a_0 + a_1x + ... + a_nx^n$ z $A[x]$ priradí polynóm $f(y) = a_0 + a_1y + ... + a_ny^n$ je izomorfizmus $A[x] \longrightarrow A[y]$. Pretože izomorfné okruhy majú rovnaké vlastnosti, nezáleží na tom , ktorú neurčitú si vyberieme.

Zostáva ešte otázka, či pre každý KOJ A existuje neurčitá nad A a teda či existuje okruh polynómov nad A. Odpoveď dáva nasledujúca veta, ktorú nebudeme zatiaľ dokazovať.

Veta 4.4. *Pre každý KOJ (obor integrity)* A *existuje KOJ (obor integrity)* B *a prvok* $x \in B$, *tak, že* $A \leq_{\mathbf{1}} B$ *a* x *je neurčitá nad* A.

5 Deliteľnosť v okruhoch polynómov

Podobne, ako v okruhu celých čísel aj pri štúdiu okruhov polynómov má významnú úlohu pojem deliteľnosti. V okruhoch polynómov nad poľami je problematika deliteľnosti v mnohom podobná ako v okruhu celých čísel.

Definícia 5.1. *Nech* $A[x]$ *je okruh polynómov nad KOJ* A, $f(x), g(x) \in A[x]$. *Hovoríme, že* $g(x)$ *delí* $f(x)$ *v* $A[x]$ *(alebo tiež* $f(x)$ *je deliteľný polynómom* $g(x)$ *v* $A[x]$*), ak existuje* $h(x) \in A[x]$ *taký, že* $f(x) = g(x).h(x)$. *Označenie:* $g(x) \mid f(x)$. *Označenie* $g(x) \nmid f(x)$ *znamená, že* $g(x)$ *nedelí* $f(x)$.

Príklad 5.1. *1)* $2 + 2x \mid 1 - x^2$ *v* $\mathbb{Q}[x]$, *lebo existuje polynóm* $\frac{1}{2} - \frac{1}{2}x \in \mathbb{Q}[x]$ *tak, že* $1 - x^2 = (2 + 2x).(\frac{1}{2} - \frac{1}{2}x)$. *Súčasne platí, že* $2 + 2x \nmid 1 - x^2$ *v* $\mathbb{Z}[x]$.

2) $1 + 2x^2 \mid 2x$ *v* $\mathbb{Z}_4[x]$, *lebo existuje polynóm* $2x \in \mathbb{Z}_4[x]$ *tak, že* $2x = (1 + 2x^2).2x$.

3) Pre každý polynóm $f(x) \in A[x]$ *platí* $f(x) \mid 0$ *a* $\mathbf{1} \mid f(x)$ *v* $A[x]$, *platí tiež* $0 \mid 0$ *v* $A[x]$.

4) Nech $A[x]$ *je okruh polynómov,* B *je KOJ,* $A \leq_{\mathbf{1}} B$, $f(x), g(x), h(x) \in A[x]$, $f(x) = g(x).h(x)$ *a* $c \in B$. *Potom platí: Ak* c *je koreň* $g(x)$, *tak* c *je aj koreň* $f(x)$. *Teda ak* $g(x) \mid f(x)$ *a* c *je koreň* $g(x)$, *tak* c *je koreňom* $f(x)$. *Ak* B *je obor integrity a* c *je koreň* $f(x)$, *tak* c *je koreňom* $g(x)$ *alebo* $h(x)$.

Veta 5.1. *Nech* $A[x]$ *je okruh polynómov nad KOJ* A, $f(x), g(x), h(x) \in A[x]$. *Potom v* $A[x]$ *platí:*

1) $f(x) \mid f(x)$.

2) Ak $f(x) \mid g(x)$ *a* $g(x) \mid h(x)$, *tak* $f(x) \mid h(x)$.

3) Ak $f(x) \mid g(x)$ *a* $f(x) \mid h(x)$, *tak pre každé* $u(x), v(x) \in A[x]$ *platí, že* $f(x) \mid u(x).g(x) + v(x).h(x)$.

4) Ak A *je obor integrity,* $g(x) \mid f(x)$ *a* $f(x) \neq 0$, *tak* $stg(x) \leq stf(x)$.

Dôkaz. 2) Ak $f(x) \mid g(x)$ a $g(x) \mid h(x)$, tak existujú $r(x), s(x) \in A[x]$ tak, že $g(x) = f(x).r(x)$ a $h(x) = g(x).s(x)$ Potom $h(x) = f(x).r(x).s(x)$, pričom $r(x).s(x) \in A[x]$. Teda $f(x) \mid h(x)$.

3) Podobne ako 2).

4) Existuje $h(x) \in A[x]$ tak, že $f(x) = g(x).h(x)$. Pretože $f(x) \neq 0$, platí $g(x) \neq 0$ aj $h(x) \neq 0$ a preto $stg(x) \geq 0$, $sth(x) \geq 0$. Pretože A je obor integrity, podľa vety 3.2 časť 2) platí $stf(x) = stg(x) + sth(x)$ a pretože $sth(x) \geq 0$, dostávame, že $stf(x) \geq stg(x)$. □

Pri štúdiu problematiky deliteľnosti v okruhoch polynómov hrá, podobne ako v prípade deliteľnosti v okruhu celých čísel, nasledujúca veta o delení so zvyškom.

Veta 5.2. *Nech A je obor integrity, $A[x]$ je okruh polynómov nad A, $f(x), g(x) \in A[x]$, $g(x) \neq 0$, $g(x) = b_0 + ... + b_k x^k$, $b_k \neq 0$ a existuje inverzný prvok b_k^{-1} k prvku b_k v obore integrity A. Potom existujú jednoznačne určené polynómy $h(x), r(x) \in A[x]$ také, že $f(x) = h(x).g(x) + r(x)$ a $str(x) < stg(x)$.*

Dôkaz. 1) Existencia:

a) Ak $stf(x) < stg(x)$, tak $f(x) = 0.g(x) + f(x)$, $stf(x) < stg(x)$. Ak teda zvolíme $h(x) = 0$ a $r(x) = f(x)$, tak výrok o existencii platí. Pretože $g(x) \neq 0$, $stg(x) \geq 0$, pre $f(x) = 0$ platí $stf(x) < stg(x)$ a preto ak $f(x)$ je nulový polynóm, tak dokazovaný výrok o existencii platí.

b) Nech $f(x) \neq 0$, $f(x) = a_0 + ... + a_n x^n$, $a_n \neq 0$ ($n \in \mathbb{N}_0$). Dôkaz urobíme matematickou indukciou 2. typu vzhľadom na $n = stf(x)$.

1. Nech $n = 0$. Potom $f(x) = a_0 \neq 0$. Ak $stf(x) = 0 < stg(x)$, tak podľa a) výrok platí. Nech $stf(x) = 0 \geq stg(x)$. Potom $stg(x) = 0$ a $g(x) = b_0 \neq 0$. Podľa predpokladu vety prvok b_0 má inverzný prvok b_0^{-1} v A. Potom $a_0 = (a_0 b_0^{-1})b_0 + 0$, $st0 < stb_0$. Ak teraz zvolíme $h(x) = a_0 b_0^{-1}$ a $r(x) = 0$, tak platí $f(x) = h(x).g(x) + r(x)$ a $str(x) < stg(x)$.

2. Nech teraz $n \in \mathbb{N}_0$, $n > 0$ a pre všetky $m \in \mathbb{N}_0$ také, že $m < n$ výrok platí. Ak $stf(x) < stg(x)$, tak podľa a) výrok platí. Nech $stf(x) = n \geq stg(x) = k$. Nech $f(x) = a_0 + ... + a_n x^n$, $a_n \neq 0$. Pretože $n - k \geq 0$, $a_n b_k^{-1} x^{n-k} \in A[x]$. Potom polynóm $f_1(x) = f(x) - a_n b_k^{-1} x^{n-k}.g(x) = a_0 + ... + a_n x^n - (a_n b_k^{-1} b_0 x^{n-k} + ... + a_n b_k^{-1} b_{k-1} x^{n-1} + a_n (b_k^{-1} b_k) x^n) = a_0 + ... + (a_{n-1} - a_n b_k^{-1} b_{k-1}) x^{n-1}$ má stupeň najviac $n - 1$ a teda $stf_1(x) < n$.

Ak $f_1(x) = 0$, tak $f(x) = (a_n b_k^{-1} x^{n-k}).g(x) + 0$, $st0 < stg(x)$ a teda výrok platí.

Nech $f_1(x) \neq 0$. Potom $0 \leq stf_1(x) < n$ a podľa indukčného predpokladu existujú polynómy $h_1(x), r(x) \in A[x]$ také, že $f_1(x) = h_1(x).g(x) + r(x)$ a $str(x) < stg(x)$. Potom ale (z definície $f_1(x)$) dostávame, že $f(x) = f_1(x) + a_n b_k^{-1} x^{n-k}.g(x) = h_1(x).g(x) + r(x) + a_n b_k^{-1} x^{n-k}.g(x) = (h_1(x) + a_n b_k^{-1} x^{n-k}).g(x) + r(x)$, kde $h(x) = h_1(x) + a_n b_k^{-1} x^{n-k}, r(x) \in A[x]$ a $str(x) < stg(x)$.

Teda výrok o existencii platí pre ľubovoľné polynómy $f(x), g(x) \in A[x]$ spĺňajúce predpoklady vety.

Jednoznačnosť:

Nech $f(x) = h_1(x).g(x) + r_1(x) = h_2(x).g(x) + r_2(x)$, $str_1(x) < stg(x)$, $str_2(x) < stg(x)$. Potom $(h_1(x)-h_2(x)).g(x) = r_2(x)-r_1(x)$. Ak $h_1(x)-h_2(x) \neq 0$, tak $st(h_1(x) - h_2(x)) \geq 0$ a $st(r_2(x) - r_1(x)) \leq max\{str_2(x), st(-r_1(x))\} < stg(x) \leq stg(x) + st(h_1(x) - h_2(x)) = st(g(x).(h_1(x) - h_2(x))$. Teda $st(r_2(x) - r_1(x)) < st(g(x).(h_1(x) - h_2(x))$ - dostali sme spor. Preto $h_1(x) - h_2(x)) = 0$ a potom aj $r_2(x) - r_1(x) = 0$. Z toho vyplýva, že $h_1(x) = h_2(x)$ a $r_1(x) = r_2(x)$. □

Pretože v každom poli existuje pre každý nenulový prvok inverzný prvok, dostávame:

Dôsledok 5.1. *Nech F je pole, $F[x]$ je okruh polynómov nad F, $f(x), g(x) \in F[x]$, $g(x) \neq 0$. Potom existujú jednoznačne určené polynómy $h(x), r(x) \in F[x]$ také, že $f(x) = h(x).g(x) + r(x)$ a $str(x) < stg(x)$.*

Príklad 5.2. *V okruhu polynómov $\mathbb{Z}_5[x]$ vydeľte so zvyškom polynóm $f(x) = 2x^4 + x^3 + 3x + 2$ polynómom $g(x) = 3x^2 + x + 1$. Všimnime si, že $3^{-1} = 2$ v $\mathbb{Z}_5$ a $2.3^{-1}x^{4-2} = 4x^2$.*

$$
\begin{array}{rl}
2x^4 + x^3 \qquad\quad + 3x + 2 : 3x^2 + x + 1 = 4x^2 + 4x + 4 & \\
-(\underline{2x^4 + 4x^3 + 4x^2}) & \\
\qquad 2x^3 + x^2 + 3x + 2 & \\
\quad -(\underline{2x^3 + 4x^2 + 4x}) & \\
\qquad\qquad 2x^2 + 4x + 2 & \\
\qquad\quad -(\underline{2x^2 + 4x + 4}) & \\
\qquad\qquad\qquad 3 &
\end{array}
$$

Teda $f(x) = (4x^2 + 4x + 4).g(x) + 3$, $st3 = 0 < 2 = stg(x)$.

Nasledujúci dôsledok vety 4.2 vyplýva z toho, že k jednotkovému prvku v každom KOJ existuje inverzný prvok a je na ňom založený výpočet hodnoty polynómu pomocou Hornerovej schémy.

Dôsledok 5.2. *Nech A je obor integrity, $A[x]$ je okruh polynómov nad A, $f(x) \in A[x]$ a $c \in A$. Potom existuje jednoznačne určený polynóm $h(x) \in A[x]$ taký, že $f(x) = h(x)(x - c) + f(c)$. Ak $stf(x) = n \geq 1$, tak $sth(x) = n - 1$.*

Dôkaz. $f(x), x - c \in A[x]$, $x - c \neq 0$ a k $\mathbf{1}$, ktorý je vedúcim koeficientom polynómu $x - c$ existuje inverzný prvok ($\mathbf{1}^{-1} = \mathbf{1}$). Podľa predchádzajúcej vety existujú jednoznačne určené polynómy $h(x), r(x) \in A[x]$, také, že $f(x) = h(x)(x - c) + r(x)$ a $str(x) < st(x - c) = 1$. Preto $r(x) = d \in A$. Teda máme $f(x) = h(x)(x-c)+d$. Podľa vety 3.3 platí $f(c) = h(c).(c-c)+d = h(c).0+d = d$. Teda $d = f(c)$ a $f(x) = h(x).(x - c) + f(c)$. Nech $stf(x) = n \geq 1$. Potom $n = stf(x) = st(h(x).(x - c) + f(c)) = st(h(x).(x - c)) = sth(x) + st(x - c) = sth(x) + 1$. Teda $sth(x) = n - 1$. □

Z predchádzajúceho dôsledku bezprostredne vyplýva:

Dôsledok 5.3. *Nech A je obor integrity, $A[x]$ je okruh polynómov nad A, $f(x) \in A[x]$ a $c \in A$. Potom c je koreň polynómu $f(x)$ vtedy a len vtedy, keď $x - c \mid f(x)$.*

Hornerova schéma.

Nech A je obor integrity, $f(x) \in A[x]$, $stf(x) = n \geq 1$, $c \in A$. Potom $f(x) = a_0 + a_1x + ... + a_nx^n$, $a_n \neq 0$ a podľa dôsledku 4.2 existuje polynóm $g(x) \in A[x]$, $stg(x) = n - 1$ tak, že $f(x) = g(x).(x - c) + f(c)$. Nech $g(x) = b_0 + b_1x + ... + b_{n-1}x^{n-1}$, $b_{n-1} \neq 0$. Potom platí

$a_0 + a_1x + ... + a_nx^n = (b_0 + b_1x + ... + b_{n-1}x^{n-1})(x - c) + f(c) = f(c) + (-c)b_0 + ((-c)b_1 + b_0)x + ((-c)b_2 + b_1)x^2 + ... + ((-c)b_{n-1} + b_{n-2})x^{n-1} + b_{n-1}x^n$. Z tejto rovnosti dostávame nasledujúce rovnosti:

$b_{n-1} = a_n$, $(-c)b_{n-1} + b_{n-2} = a_{n-1}$, $(-c)b_{n-2} + b_{n-3} = a_{n-2}$, ... , $(-c)b_2 + b_1 = a_2$, $(-c)b_1 + b_0 = a_1$, $(-c)b_0 + f(c) = a_0$.

Po úprave dostávame rovnosti pomocou ktorých z koeficientov polynómu $f(x)$ vypočítame koeficienty polynómu g(x) a hodnotu $f(c)$:

$b_{n-1} = a_n$

$b_{n-2} = a_{n-1} + cb_{n-1}$

$b_{n-3} = a_{n-2} + cb_{n-2}$

.....

$b_1 = a_2 + cb_2$

$f(c) = a_0 + cb_0$

Tieto rovnosti môžeme zapísať pomocou tabuľky, ktorá sa nazýva Hornerova schéma:

	a_n	a_{n-1}	a_{n-2}	. . . . .	a_2	a_1	a_0
c		cb_{n-1}	cb_{n-2}	. . . . .	cb_2	cb_1	cb_0
	b_{n-1}	b_{n-2}	b_{n-3}	. . . . .	b_1	b_0	$f(c)$

kde každý prvok tretieho riadku je súčet prvkov, ktoré sú nad ním.

Príklad 5.3. *Vypočítajte $f(3)$, ak $f(x) = 2 + x + 2x^2 - x^4 \in \mathbb{Z}[x]$.*

Použijeme Hornerovu schému:

	-1	0	2	1	2
3		-3	-9	-21	-60
	-1	-3	-7	-20	$\underline{-58}$

Teda $f(3) = -58$. Súčasne platí $f(x) = (-x^3 - 3x^2 - 7x - 20).(x - 3) + (-58)$.

Definícia 5.2. *Nech $A[x]$ je okruh polynómov nad KOJ A.*

a) Polynóm $f(x) = a_0 + ... + a_nx^n \in A[x]$, $a_n \neq 0$ sa nazýva normovaný, ak $a_n = \mathbf{1}$ (t. j. $f(x) = a_0 + ... + x^n$).

b) Nech $f(x), g(x) \in A[x]$. Hovoríme, že polynóm $f(x)$ je asociovaný s polynómom $g(x)$ v $A[x]$, ak $f(x) \mid g(x)$ a súčasne $g(x) \mid f(x)$ v $A[x]$. Označenie: $f(x) \sim g(x)$.

Príklad 5.4. *1) Polynóm* $f(x) = 2 + 3x + x^4$ *je normovaný polynóm.*

2) Nech $f(x) = x + 1$, $g(x) = 2x + 2$. *Potom* $f(x) \sim g(x)$ *v* $\mathbb{Q}[x]$ *ale* $f(x) \nsim g(x)$ *v* $\mathbb{Z}[x]$.

3) Nech $f(x), g(x), h(x), r(x) \in A[x]$ *a* $f(x) \sim g(x)$ *v* $A[x]$. *Potom v* $A[x]$ *platí:* $h(x) \mid f(x) \Leftrightarrow h(x) \mid g(x)$ *a tiež* $f(x) \mid r(x) \Leftrightarrow g(x) \mid r(x)$. *Teda z hľadiska deliteľnosti majú* $f(x)$ *a* $g(x)$ *rovnaké vlastnosti.*

Veta 5.3. *Nech* $A[x]$ *je okruh polynómov nad KOJ* A, $f(x), g(x), h(x) \in A[x]$. *Potom v* $A[x]$ *platí:*

1) $f(x) \sim f(x)$.

2) Ak $f(x) \sim g(x)$, *tak* $g(x) \sim f(x)$.

3) Ak $f(x) \sim g(x)$ *a* $g(x) \sim h(x)$, *tak* $f(x) \sim h(x)$.

4) $f(x) \sim 0$ *práve vtedy, keď* $f(x) = 0$.

5) Ak A *je obor integrity a* $f(x) \sim g(x)$, *tak* $stf(x) = stg(x)$.

Dôkaz. 3) Nech $f(x) \sim g(x)$ a $g(x) \sim h(x)$. Potom $f(x) \mid g(x)$ a $g(x) \mid h(x)$ a preto $f(x) \mid h(x)$. Súčasne platí $h(x) \mid g(x)$ a $g(x) \mid f(x)$ a preto $h(x) \mid f(x)$. Teda $f(x) \sim h(x)$.

4) Ak $f(x) \sim 0$, tak $0 \mid f(x)$ a preto $f(x) = 0$. Obrátene, ak $f(x) = 0$, tak podľa 1) $0 \sim 0$.

5) Ak $f(x) = 0$, tak podľa 4) aj $g(x) = 0$ a $stf(x) = -\infty = stg(x)$.

Nech $f(x) \neq 0$. Potom aj $g(x) \neq 0$ Pretože A je obor integrity, $f(x) \mid g(x)$ a $g(x) \neq 0$, platí $stf(x) \leq stg(x)$. Podobne, $g(x) \mid f(x)$ a $f(x) \neq 0$ a preto $stg(x) \leq stf(x)$. Teda platí $stf(x) = stg(x)$. □

Príklad 5.5. *V* $\mathbb{Z}_4[x]$ *platí, že* $1+2x \sim 1+2x^2$ *pričom* $st(1+2x) \neq st(1+2x^2)$. *Skutočne,* $1 + 2x^2 = (1 + 2x).(1 + 2x + 2x^2)$ *a preto* $1 + 2x \mid 1 + 2x^2$ *a súčasne* $1 + 2x = (1 + 2x^2).(1 + 2x + 2x^2)$ *a preto* $1 + 2x^2 \mid 1 + 2x$. *Je to možné preto, že* $\mathbb{Z}_4$ *nie je obor integrity (*$2.2 = 0$ *v* $\mathbb{Z}_4$*).*

V okruhoch polynómov nad poľami, platia pre reláciu asociovanosti polynómov aj ďalšie vlastnosti:

Veta 5.4. *Nech* F *je pole,* $F[x]$ *je okruh polynómov nad* F *a* $f(x), g(x) \in F[x]$. *Potom v* $F[x]$ *platí:*

1) $f(x) \sim g(x)$ *vtedy a len vtedy, keď existuje* $c \in F\backslash\{0\}$ *tak, že* $f(x) = c.g(x)$.

2) $f(x) \sim \mathbf{1}$ *vtedy a len vtedy, keď* $stf(x) = 0$ *(t. j.* $f(x) = a_0 \in F\backslash\{0\}$*).*

3) Ak $f(x)$, $g(x)$ *sú normované polynómy a* $f(x) \sim g(x)$, *tak* $f(x) = g(x)$.

4) Ak $f(x) \neq 0$, *tak existuje práve jeden normovaný polynóm* $h(x) \in f(x)$ *taký, že* $f(x) \sim h(x)$.

Dôkaz. 1) "⇒": Ak $f(x) = 0$, tak aj $g(x) = 0$ a existuje $\mathbf{1} \in F\backslash\{0\}$ tak, že $0 = \mathbf{1}.0$. Ak $f(x) \neq 0$, tak aj $g(x) \neq 0$ a pretože $g(x) \mid f(x)$ existuje $h(x) \in F[x]$, pre ktoré $f(x) = h(x).g(x)$. Potom (pretože F je obor integrity) platí $stf(x) = sth(x) + stg(x)$. Okrem toho, pretože $f(x) \sim g(x)$, platí $stf(x) = stg(x)$ a teda $sth(x) = 0$. To znamená, že $h(x) = c \in F\backslash\{0\}$ a $f(x) = c.g(x)$.

"$\Leftarrow$": Nech existuje $c \in F\backslash\{0\}$, pre ktoré $f(x) = c.g(x)$. Potom $g(x) \mid f(x)$ v $F[x]$. Súčasne existuje $c^{-1} \in F \subseteq F[x]$ a platí $g(x) = c^{-1}.f(x)$. Potom $f(x) \mid g(x)$ v $F[x]$ a teda $f(x) \sim g(x)$.

2) $f(x) \sim \mathbf{1} \Leftrightarrow$ existuje $c \in F\backslash\{0\}$ tak, že $f(x) = c.\mathbf{1} = c \Leftrightarrow stf(x) = 0$.

3) Nech $f(x) = a_0 + ... + x^n$, $g(x) = b_0 + ... + x^k$, $n, k \in \mathbb{N}_0$ a $f(x) \sim g(x)$. Potom $stf(x) = n = k = stg(x)$ a existuje $c \in F\backslash\{0\}$ tak, že $f(x) = c.g(x)$. To znamená, že $a_0 + ... + x^n = cb_0 + ... + cx^n$ a preto $c = \mathbf{1}$. Teda $f(x) = \mathbf{1}.g(x) = g(x)$.

4) Nech $f(x) \neq 0$. Potom $f(x) = a_0 + ... + a_n x^n$, $a_n \in F$, $a_n \neq 0$. Potom existuje $a_n^{-1} \in F$ a polynóm $h(x) = a_n^{-1}.f(x) = a_n^{-1}a_0 + ... + \mathbf{1}x^n$ je normovaný polynóm, ktorý je podľa 1) asociovaný s $f(x)$, t. j. $f(x) \sim h(x)$. Nech $h_1(x) \in F[x]$ je tiež normovaný polynóm a $f(x) \sim h_1(x)$. Potom $h_1(x) \sim h(x)$ a podľa 3) platí $h_1(x) = h(x)$. □

Príklad 5.6. *1) Nech* $f(x) = 2 + 3x + 3x^3 \in \mathbb{R}[x]$. *Potom* $f(x) \sim \frac{2}{3} + x + x^3 = h(x)$ *v* $\mathbb{R}[x]$, *kde* $h(x)$ *je normovaný polynóm.*

2) $2 + 3x + 4x^5 \sim 3 + 2x + x^5$ *v* $\mathbb{Z}_5[x]$.

Podobne ako v teórii deliteľnosti v okruhu celých čísel aj v teórii deliteľnosti v okruhoch polynómov nad poľami hrá významnú úlohu pojem najväčšieho spoločného deliteľa.

Definícia 5.3. *Nech* F *je pole,* $f(x), g(x) \in F[x]$.

a) Polynóm $d(x) \in F[x]$ *sa nazýva najväčší spoločný deliteľ (n. s. d.) polynómov* $f(x)$, $g(x)$ *v* $F[x]$, *ak platí:*
(1) $d(x) \mid f(x)$, $d(x) \mid g(x)$.
(2) Ak $h(x) \in F[x]$ *a* $h(x) \mid f(x)$, $h(x) \mid g(x)$, *tak* $h(x) \mid d(x)$ *v* $F[x]$.

Označenie: n.s.d.$\{f(x), g(x)\}$.

b) Ak $d(x)$ *je n. s. d. polynómov* $f(x)$, $g(x)$ *v* $F[x]$ *a* $d(x)$ *je normovaný alebo* $d(x) = 0$, *tak* $d(x)$ *budeme označovať* $(f(x), g(x))$.

c) Polynómy $f(x)$, $g(x)$ *sa nazývajú nesúdeliteľné (súdeliteľné) v* $F[x]$, *ak* $(f(x), g(x)) = \mathbf{1}$ *(ak nie sú nesúdeliteľné, t. j. ak* $(f(x), g(x)) \neq \mathbf{1}$*).*

Príklad 5.7. *1) V každom okruhu polynómov* $F[x]$ *nad poľom* F *je* 0 *n. s. d. polynómov* 0, 0 *a teda platí* $0 = (0, 0)$.

2) Nech $f(x) = x^2 + 2x + 1$, $g(x) = x^2 - 1$ *sú polynómy v* $\mathbb{R}[x]$. *Ukážeme, že* $d(x) = x + 1$ *je n.s.d.*$\{f(x), g(x)\}$ *v* $\mathbb{R}[x]$. *Pretože* $f(x) = (x + 1).(x + 1)$ *a* $g(x) = (x + 1).(x - 1)$, *platí* $d(x) \mid f(x)$ *aj* $d(x) \mid g(x)$. *Nech* $h(x) \in \mathbb{R}[x]$ *a* $h(x) \mid f(x)$ *a* $h(x) \mid g(x)$. *Potom* $h(x) \mid f(x) - g(x) = 2x + 2$ *a pretože* $2x + 2 \mid x + 1 = d(x)$ *v* $\mathbb{R}[x]$, *platí* $h(x) \mid d(x)$ *v* $\mathbb{R}[x]$. *Teda* $d(x)$ *je n.s.d.*$\{f(x), g(x)\}$ *v* $\mathbb{R}[x]$ *a pretože* $d(x)$ *je normovaný polynóm,* $d(x) = (f(x), g(x))$.

3) Nech F *je pole,* $f(x) \mid g(x)$ *v* $F[x]$. *Potom* $f(x)$ *je n.s.d.*$\{f(x), g(x)\}$ *v* $F[x]$.

4) Ak $d(x)$ *je n.s.d.*$\{f(x), g(x)\}$ *v* $F[x]$, *tak* $d(x)$ *je n.s.d.*$\{g(x), f(x)\}$ *v* $F[x]$. *Špeciálne,* $(f(x), g(x)) = (g(x), f(x))$.

5) Ak $d(x)$ *je n.s.d.*$\{f(x), g(x)\}$ *v* $F[x]$, $f(x) \sim f_1(x)$ *a* $g(x) \sim g_1(x)$ *v* $F[x]$, *tak* $d(x)$ *je aj n.s.d.*$\{f(x)_1, g(x)_1\}$ *v* $F[x]$. *Vyplýva to z toho, že asociované polynómy majú tých istých deliteľov.*

Veta 5.5. *Nech F je pole, $f(x), g(x) \in F[x]$. Potom v $F[x]$ platí:*
1) Ak $d(x)$ je $n.s.d.\{f(x), g(x)\}$ a $h(x) \sim d(x)$, tak $h(x)$ je $n.s.d.\{f(x), g(x)\}$.
2) Ak $d(x)$ aj $h(x)$ je $n.s.d.\{f(x), g(x)\}$, tak $d(x) \sim h(x)$.

Dôkaz. 1) Z predpokladov vyplýva, že v $F[x]$ platí $h(x) \mid d(x)$, $d(x) \mid f(x)$, $d(x) \mid g(x)$. Potom, zrejme, $h(x) \mid f(x)$, $h(x) \mid g(x)$. Nech $r(x) \mid f(x)$ a $r(x) \mid g(x)$ v $F[x]$. Potom $r(x) \mid d(x)$ a pretože platí aj $d(x) \mid h(x)$, dostávame, že platí $r(x) \mid h(x)$. Teda $h(x)$ je $n.s.d.\{f(x), g(x)\}$.

2) Polynóm $d(x)$ je $n.s.d.\{f(x), g(x)\}$ a preto $d(x) \mid f(x)$, $d(x) \mid g(x)$. Pretože $h(x)$ je $n.s.d.\{f(x), g(x)\}$ platí $d(x) \mid h(x)$. Analogicky sa ukáže, že $h(x) \mid d(x)$. Teda $d(x) \sim h(x)$. □

Dôsledok 5.4. *Nech F je pole, $f(x), g(x), d(x) \in F[x]$. Potom v $F[x]$ platí:*
Ak existuje $d(x) \in F[x]$ tak, že $d(x)$ je $n.s.d.\{f(x), g(x)\}$ tak existuje práve jeden polynóm $h(x) \in F[x]$ taký, že $h(x) = (f(x), g(x))$, pričom $d(x) \sim h(x)$.

Na základe predchádzajúceho dôsledku budeme skutočnosť, že $d(x)$ je $n.s.d.\{f(x), g(x)\}$ zapisovať $d(x) \sim (f(x), g(x))$.

Zatiaľ ešte nevieme, či pre ľubovoľnú dvojicu polynómov nad poľom existuje n. s. d.. K tomu, aby sme to dokázali využijeme nasledujúce pomocné tvrdenie (a vetu a delení so zvyškom).

Lema 5.1. *Nech F je pole, $f(x), g(x), h(x), r(x), d(x) \in F[x]$ a $f(x) = h(x).g(x) + r(x)$. Potom $d(x)$ je $n.s.d.\{f(x), g(x)\}$ práve vtedy, keď $d(x)$ je $n.s.d.\{g(x), r(x)\}$.*

Dôkaz. "⇒": Nech $d(x)$ je $n.s.d.\{f(x), g(x)\}$. Potom $d(x) \mid f(x)$, $d(x) \mid g(x)$ a preto $d(x) \mid r(x) = f(x) - h(x).g(x)$. Teda platí $d(x) \mid g(x)$ a $d(x) \mid r(x)$. Nech $s(x) \in F[x]$ a $s(x) \mid g(x)$, $s(x) \mid r(x)$. Potom $s(x) \mid h(x).g(x) + r(x) = f(x)$, $s(x) \mid g(x)$ a pretože $d(x)$ je $n.s.d.\{f(x), g(x)\}$ dostávame, že $s(x) \mid d(x)$. Teda $d(x)$ je $n.s.d.\{g(x), r(x)\}$.

"⇐": Nech $d(x)$ je $n.s.d.\{g(x), r(x)\}$. Potom $d(x) \mid g(x)$, $d(x) \mid r(x)$ a preto $d(x) \mid f(x) = h(x).g(x) + r(x)$. Teda platí $d(x) \mid f(x)$ a $d(x) \mid g(x)$. Nech $s(x) \in F[x]$ a $s(x) \mid f(x)$, $s(x) \mid g(x)$. Potom $s(x) \mid h(x).g(x) - r(x) = r(x)$, $s(x) \mid g(x)$ a pretože $d(x)$ je $n.s.d.\{g(x), r(x)\}$ dostávame, že $s(x) \mid d(x)$. Teda $d(x)$ je $n.s.d.\{f(x), g(x)\}$. □

Teraz ukážeme na príklade, ako pomocou vety a delení so zvyškom a predchádzajúcej lemy vypočítame n. s. d. dvoch polynómov. Takýto výpočet sa nazýva Euklidov algoritmus.

Príklad 5.8. *Vypočítajte $d(x) = (f(x), g(x))$ v $\mathbb{Z}_5[x]$, ak $f(x) = x^4 + x^3 + 2x^2 + x + 4$ a $g(x) = x^3 + x^2 + 4x + 4$. Ďalej nájdite polynómy $u(x), v(x) \in \mathbb{Z}_5[x]$, tak aby platilo $d(x) = u(x).f(x) + v(x).g(x)$.*

Najprv vydelíme so zvyškom polynóm $f(x)$ polynómom $g(x)$:

$$\begin{array}{l} x^4 + x^3 + 2x^2 + x + 4 : x^3 + x^2 + 4x + 4 = x \\ \underline{-(x^4 + x^3 + 4x^2 + 4x)} \\ \qquad\qquad 3x^2 + 2x + 4 = r_2(x) \end{array}$$

Dostávame, že $f(x) = x.g(x) + r_2(x)$, $str_2(x) < stg(x)$. *Podľa predchádzajúcej lemy platí, že* $n.s.d.\{f(x), g(x)\} = n.s.d.\{g(x), r_2(x)\}$.

Teraz vydelíme polynóm $g(x)$ *polynómom* $r_2(x)$*:*

$$\begin{array}{l} x^3 + x^2 + 4x + 4 : x^2 + 2x + 4 = 2x + 4 \\ -(\underline{x^3 + 4x^2 + 3x}) \\ \qquad 2x^2 + x + 4 \\ \quad -(\underline{2x^2 + 3x + 1} \\ \qquad\qquad 3x + 3 = r_3(x) \end{array}$$

Teraz dostávame $g(x) = (2x + 4).r_2(x) + r_3(x)$, $str_3(x) < str_2(x)$ *a podľa predchádzajúcej lemy platí, že* $n.s.d.\{g(x), r_2(x)\} = n.s.d.\{r_2(x), r_3(x)\}$.

Ďalej vydelíme polynóm $r_2(x)$ *polynómom* $r_3(x)$*:*

$$\begin{array}{l} 3x^2 + 2x + 4 : 3x + 3 = x + 3 \\ -(\underline{3x^2 + 3x}) \\ \qquad 4x + 4 \\ \quad -(\underline{4x + 4}) \\ \qquad\qquad 0 \end{array}$$

Teda platí $r_2(x) = (x+3).r_3(x)+0$ *a tiež* $n.s.d.\{r_2(x), r_3(x)\} = n.s.d\{r_3(x), 0) = r_3(x)\}$.

Teda $3x+3 = r_3(x) = n.s.d.\{r_2(x), r_3(x)\} = n.s.d.\{g(x), r_2(x)\} = n.s.d.\{f(x), g(x)\}$. *Je to posledný nenulový zvyšok v uvedenom postupe, ktorý sa nazýva Euklidov algoritmus. Potom, pretože* $3x + 3 \sim x + 1$, *dostávame, že* $x + 1 = (f(x), g(x))$, *t. j.* $d(x) = x + 1$.

Na výpočet polynómov $u(x)$, $v(x)$ *využijeme horeuvedený Euklidov algoritmus.*

Zrejme $3x+3 = r_3(x) = g(x)+(-(2x+4)).r_2(x) = g(x)+(-(2x+4).(f(x)+(-x).g(x)) = (-(2x+4)).f(x)+(1+(2x^2+4x)).g(x) = (3x+1).f(x)+(2x^2+4x+1).g(x)$.

Teda $3x+3 = (3x+1).f(x)+(2x^2+4x+1).g(x)$ *a ak túto rovnosť vynásobíme prvkom* $3^{-1} = 2$, *dostaneme*

$d(x) = x + 1 = (x + 2).f(x) + (4x^2 + 3x + 2).g(x)$. *Teda* $u(x) = x + 2$ *a* $v(x) = 4x^2 + 3x + 2$.

Veta 5.6. *Nech* F *je pole,* $f(x), g(x) \in F[x]$. *Potom v* $F[x]$ *platí:*

a) Existuje $d(x) \in F[x]$ *taký, že* $d(x)$ *je* $n.s.d.\{f(x), g(x)\}$.

b) Ak $d(x)$ *je* $n.s.d.\{f(x), g(x)\}$, *tak existujú* $u(x), v(x) \in F[x]$, *pre ktoré platí* $d(x) = u(x).f(x) + v(x).g(x)$.

Dôkaz. a) 1. Ak $g(x) = 0$, tak $f(x)$ je $n.s.d.\{f(x), g(x)\}$.

2. Nech $g(x) \neq 0$. Označme $f(x) = r_0(x)$, $g(x) = r_1(x)$. Pretože $r_1(x) \neq 0$, podľa vety o delení so zvyškom existujú jednoznačne určené polynómy $h_1(x), r_2(x) \in F[x]$ také, že

$r_0(x) = h_1(x).r_1(x) + r_2(x)$ a $str_2(x) < str_1(x)$.

Ak $k \geq 1$ a sú definované polynómy $r_{k-1}(x), r_k(x) \in F[x]$, $r_k(x) \neq 0$, tak definujeme $r_{k+1}(x)$ takto: Existujú jednoznačne určené polynómy $h_k(x), r_{k+1}(x) \in F[x]$ také, že

$r_{k-1}(x) = h_k(x).r_k(x) + r_{k+1}(x)$ a $str_{k+1}(x) < str_k(x)$.

Pretože $str_1(x) > str_2(x) > ... > str_k(x)$ a pre $r_k(x) \neq 0$ je $str_k(x) \geq 0$ existuje $l \geq 1$ ($l \leq 1 + g(x)$) tak, že $r_l(x) \neq 0$ a $r_{l+1}(x) = 0$. Takýmto postupom dostaneme nasledujúci systém rovností:

$r_0(x) = h_1(x).r_1(x) + r_2(x)$

$r_1(x) = h_2(x).r_2(x) + r_3(x)$

.....

$r_{l-2}(x) = h_{l-1}(x).r_{l-1}(x) + r_l(x)$

$r_{l-1}(x) = h_l(x).r_l(x) + 0$

Ukážeme, že $r_l(x)$ je $n.s.d.\{f(x), g(x)\}$. Z poslednej rovnosti vidíme, že $r_l(x) \mid r_{l-1}(x)$ a preto $r_l(x)$ je $n.s.d.\{r_{l-1}(x), r_l(x)\}$. Z predposlednej rovnosti a lemy 4.1 vyplýva, že $n.s.d.\{r_{l-1}(x), r_l(x)\} = n.s.d.\{r_{l-2}(x), r_{l-1}(x)\}$, z ďalšej predchádzajúcej rovnosti a lemy 4.1 dostaneme, že $n.s.d.\{r_{l-2}(x), r_{l-1}(x)\} = n.s.d.\{r_{l-3}(x), r_{l-2}(x)\}$, a. t. ď. Teda $r_l(x) = n.s.d.\{r_{l-1}(x), r_l(x)\} = n.s.d.\{r_{l-2}(x), r_{l-1}(x)\} = n.s.d.\{r_{l-3}(x), r_{l-2}(x))\} = ... = n.s.d.\{r_2(x), r_3(x)\} = n.s.d.\{r_1(x), r_2(x)\} = n.s.d.\{r_0(x), r_1(x)\} = n.s.d.\{f(x), g(x)\}$.

Uvedený postup sa nazýva Euklidov algoritmus a $n.s.d.(f(x), g(x))$ je posledný nenulový zvyšok v Euklidovom algoritme.

b) 1. Ak $f(x) \mid g(x)$, tak $f(x)$ je $n.s.d.\{f(x), g(x)\}$ a $f(x) = \mathbf{1}.f(x) + 0.g(x)$, teda $u(x) = \mathbf{1}$, $v(x) = 0$. Podobne je to v prípade, že $g(x) \mid f(x)$.

2. Nech $f(x) \nmid g(x)$ a $g(x) \nmid f(x)$. Potom $g(x) \neq 0$ a použitím vyššie uvedeného Euklidovho algoritmu vypočítame $r_l(x) = n.s.d.\{r_0(x), r_1(x)\}$. Potom, použitím rovností z Euklidovho algoritmu (začneme s predposlednou) dostaneme: $r_l(x) = r_{l-2}(x) + (-h_{l-1}(x)).r_{l-1}(x) = r_{l-2}(x) + (-h_{l-1}(x)).(r_{l-3}(x) + (-h_{l-2}(x)).r_{l-2}(x)) = (-h_{l-1}(x)).r_{l-3}(x) + (\mathbf{1} + h_{l-1}(x).h_{l-2}(x)).r_{l-2}(x) = ... = u(x).r_0(x) + v(x).r_1(x) = u(x).f(x) + v(x).g(x)$, $u(x), v(x) \in F[x]$. Ak $d(x)$ je ľubovoľný $n.s.d.\{f(x), g(x)\}$, tak $d(x) \sim r_l(x)$ a existuje $c \in F \setminus \{0\}$ tak, že $d(x) = c.r_l(x)$. Potom $d(x) = (c.u(x).f(x) + (c.v(x).g(x)$, $c.u(x), c.v(x) \in F[x]$. □

Príklad 4.7 je ukážkou, použitia Euklidovho algoritmu na výpočet n. s. d. a polynómov $u(x)$ a $v(x)$.

Veta 5.7. *Nech F je pole, $f(x), g(x), h(x) \in F[x]$. Potom v $F[x]$ platí:*

1) Ak $(f(x), g(x)) = \mathbf{1}$, $f_1(x), g_1(x) \in F[x]$, $f_1(x) \mid f(x)$, $g_1(x) \mid g(x)$, tak $(f_1(x), g_1(x)) = \mathbf{1}$.

2) Ak $f(x) \mid g(x).h(x)$ a $(f(x), g(x)) = \mathbf{1}$, tak $f(x) \mid h(x)$.

3) Ak $f(x) \mid h(x)$, $g(x) \mid h(x)$ a $(f(x), g(x)) = \mathbf{1}$, tak $f(x).g(x) \mid h(x)$.

4) Ak $(f(x), g(x)) = \mathbf{1}$, $(f(x), h(x)) = \mathbf{1}$, tak $(f(x), g(x).h(x)) = \mathbf{1}$.

5) Ak $(f(x), g(x)) = \mathbf{1}$, $k, l \in \mathbb{N}$, tak $(f(x)^k, g(x)^l) = \mathbf{1}$.

6) Ak $(f(x), g(x)) = d(x) \neq 0$, $f(x) = f_1(x).d(x)$, $g(x) = g_1(x).d(x)$, tak $(f_1(x), g_1(x)) = \mathbf{1}$.

Dôkaz. 1) Nech $d(x) = (f_1(x), g_1(x))$. Potom $d(x) \mid f_1(x)$, $d(x) \mid g_1(x)$ a preto $d(x) \mid f(x)$, $d(x) \mid g(x)$. Potom, pretože $(f(x), g(x)) = \mathbf{1}$ platí $d(x) \mid \mathbf{1}$ a preto $std(x) = 0$. Teda $d(x) = c \in F\backslash\{0\}$ a pretože $d(x)$ je normovaný polynóm, platí $d(x) = \mathbf{1}$.

2) Existujú polynómy $u(x), v(x), r(x) \in F[x]$také, že $\mathbf{1} = u(x).f(x)+v(x).g(x)$ a $g(x).h(x) = r(x).f(x)$. Potom $h(x) = \mathbf{1}.h(x) = (u(x).f(x)+v(x).g(x)).h(x) = u(x).f(x).h(x)+v(x).g(x).h(x) = u(x).f(x).h(x)+v(x).r(x).f(x) = (u(x).h(x)+v(x).r(x)).f(x)$. Teda $f(x) \mid h(x)$.

3) Existujú polynómy $u(x), v(x), r(x), s(x) \in F[x]$také, že $\mathbf{1} = u(x).f(x) + v(x).g(x)$, $h(x) = r(x).f(x)$, $h(x) = s(x).g(x)$. Potom $h(x) = \mathbf{1}.h(x) = (u(x).f(x)+v(x).g(x)).h(x) = u(x).f(x).h(x)+v(x).g(x).h(x) = u(x).f(x).s(x).g(x)+v(x).g(x).r(x).f(x) = (u(x).s(x) + v(x).r(x)).f(x).g(x)$. Preto $f(x).g(x) \mid h(x)$.

4) Nech $d(x) = (f(x), g(x).h(x))$. Potom, pretože $d(x) \mid f(x)$ a $g(x) \mid g(x)$, podľa 1) platí $(d(x), g(x)) = \mathbf{1}$. Pretože $d(x) \mid g(x).h(x)$ a $(d(x), g(x)) = \mathbf{1}$, podľa 2) platí $d(x) \mid h(x)$. Teda $d(x) \mid f(x)$, $d(x) \mid h(x)$ a pretože $(f(x), h(x)) = \mathbf{1}$, platí $d(x) \mid \mathbf{1}$. Potom $d(x) = c \in F\backslash\{0\}$ a pretože $d(x)$ je normovaný polynóm, platí $d(x) = \mathbf{1}$.

5) Dokáže sa zo 4) pomocou matematickej indukcie.

6) Existujú $u(x), v(x) \in F[x]$ také, že $d(x) = u(x).f(x) + v(x).g(x) = u(x).f_1(x).d(x)+v(x).g_1(x).d(x) = (u(x).f_1(x)+v(x).g_1(x)).d(x)$. Pretože $d(x) \neq 0$, z predchádzajúcej rovnosti dostaneme rovnosť $\mathbf{1} = u(x).f_1(x) + v(x).g_1(x)$. Zrejme $\mathbf{1} \mid f_1(x)$, $\mathbf{1} \mid g_1(x)$. Nech $r(x) \in F[x]$ a $r(x) \mid f_1(x)$, $r(x) \mid g_1(x)$. Potom, podľa vety 4.1.3) platí, že $r(x) \mid u(x).f_1(x) + v(x).g_1(x) = \mathbf{1}$. Teda $\mathbf{1} = (f_1(x), g_1(x))$. □

S pojmom najväčšieho spoločného deliteľa úzko súvisí pojem najmenšieho spoločného násobku polynómov.

Definícia 5.4. *Nech F je pole, $f(x), g(x) \in F[x]$. Polynóm $n(x) \in F[x]$ sa nazýva najmenší spoločný násobok (n. s. n.) polynómov $f(x)$, $g(x)$ v $F[x]$, ak v $F[x]$ platí:*

1) $f(x) \mid n(x)$, $g(x) \mid n(x)$,

2) Ak $h(x) \in F[x]$ a $f(x) \mid h(x)$ aj $g(x) \mid h(x)$, tak $n(x) \mid h(x)$.

Označenie: n.s.n.$\{f(x), g(x)\}$.

Ak $n(x)$ je n.s.n.$\{f(x), g(x)\}$ v $F[x]$ a $n(x) = 0$ alebo $n(x)$ je normovaný, tak $n(x)$ označujeme $[f(x), g(x)]$.

Príklad 5.9. *1) Ak $f(x), g(x) \in F[x]$, $f(x) = 0$ alebo $g(x) = 0$, tak 0 je n.s.n.$\{f(x), g(x)\}$. Teda $[f(x), 0] = [0, g(x)] = 0$.*

2) Nech $f(x) = x^2 + 2x + 1$, $g(x) = x^2 - 1$ sú polynómy v $\mathbb{R}[x]$. Potom $f(x) = (x + 1)^2$, $g(x) = (x + 1).(x - 1)$. Ukážeme, že $n(x) = (x + 1)^2.(x - 1) = (x + 1).(x^2 - 1)$ je n. s. n. polynómov $f(x)$, $g(x)$ v $\mathbb{R}[x]$. Je zrejmé, že $f(x) \mid n(x)$ aj $g(x) \mid n(x)$. Nech $h(x) \in \mathbb{R}[x]$ a $f(x) \mid h(x)$ aj $g(x) \mid h(x)$. Potom $(x+1)^2 \mid h(x)$ aj $x - 1 \mid h(x)$. Ale $(x + 1, x - 1) = 1$ a podľa vety 4.7.5) potom aj $((x+1)^2, x - 1) = 1$. Podľa vety 4.7.3) potom $(x + 1)^2.(x - 1) = n(x) \mid h(x)$.

V príklade 4.6.2) sme ukázali, že $(f(x), g(x)) = x + 1$. Teda vidíme, že v tomto prípade platí: $(f(x), g(x)).n(x) = f(x).g(x)$.

Veta 5.8. *Nech F je pole, $f(x), g(x) \in F[x]$, $d(x) = (f(x), g(x))$ v $F[x]$. Potom v $F[x]$ platí:*

1) Ak $f(x) = 0$ alebo $g(x) = 0$, tak $0 = [f(x), g(x)]$.

2) Ak $f(x) \neq 0$ aj $g(x) \neq 0$ a $n(x) \in F[x]$ je taký polynóm, že $f(x).g(x) = n(x).d(x)$ (taký polynóm existuje lebo $d(x) \mid f(x)$ a preto $d(x) \mid f(x).g(x)$), tak $n(x)$ je $n.s.n.\{f(x), g(x)\}$.

3) Ak $n(x)$ je $n.s.n.\{f(x), g(x)\}$, $s(x) \in F[x]$, tak $s(x)$ je $n.s.n.\{f(x), g(x)\}$ vtedy a len vtedy, keď $s(x) \sim n(x)$.

Dôkaz. 1) Zrejmé.

2) $d(x) \mid f(x)$, $d(x) \mid g(x)$ a preto existujú $f_1(x), g_1(x) \in F[x]$ tak, že $f(x) = f_1(x).d(x)$ a $g(x) = g_1(x).d(x)$. Podľa vety 4.7.6) platí $(f_1(x), g_1(x)) = \mathbf{1}$. Ďalej platí $f(x).g(x) = f_1(x).g_1(x).d(x).d(x) = n(x).d(x)$ a pretože $d(x) \neq 0$, z toho dostávame, že $n(x) = f_1(x).g_1(x).d(x)$. Ukážeme, že $n(x)$ je $n.s.n.\{f(x), g(x)\}$.

$n(x) = f_1(x).g_1(x).d(x) = f(x).g_1(x) = f_1(x).g(x)$, preto $f(x) \mid n(x)$ aj $g(x) \mid n(x)$. Nech $h(x) \in F[x]$ a $f(x) \mid h(x)$, $g(x) \mid h(x)$. Pretože $d(x) \mid f(x)$ a $f(x) \mid h(x)$, platí aj $d(x) \mid h(x)$ a teda existuje $h_1(x) \in F[x]$ také, že $h(x) = h_1(x).d(x)$. Pretože $f(x) = f_1(x).d(x) \mid h(x) = h_1(x).d(x)$ a $d(x) \neq 0$, platí aj $f_1(x) \mid h_1(x)$. Podobne sa ukáže, že $g_1(x) \mid h_1(x)$. Súčasne platí $(f_1(x), g_1(x)) = \mathbf{1}$, preto $f_1(x).g_1(x) \mid h_1(x)$. Potom ale platí aj $n(x) = f_1(x).g_1(x).d(x) \mid h(x) = h_1(x).d(x)$. Dokázali sme, že $n(x)$ je $n.s.n.\{f(x), g(x)\}$.

3) "$\Rightarrow$": Nech $s(x)$ je $n.s.n.\{f(x), g(x)\}$. Podľa predpokladov platí $f(x) \mid n(x)$, $g(x) \mid n(x)$ a preto $s(x) \mid n(x)$. Súčasne platí, že $f(x) \mid s(x)$, $g(x) \mid s(x)$ a pretože $n(x)$ je $n.s.n.(f(x), g(x))$, dostávame, že $n(x) \mid s(x)$. Dokázali sme, že $s(x) \sim n(x)$.

"$\Leftarrow$": Ak $s(x) \sim n(x)$, tak $s(x) \mid n(x)$ a $n(x) \mid s(x)$. Pretože $f(x) \mid n(x)$, $g(x) \mid n(x)$ a $n(x) \mid s(x)$, platí aj $f(x) \mid s(x)$, $g(x) \mid s(x)$. Nech $h(x) \in F[x]$ a $f(x) \mid h(x)$, $g(x) \mid h(x)$. Potom $n(x) \mid h(x)$ a pretože súčasne platí $s(x) \mid n(x)$, dostávame, že $s(x) \mid h(x)$. Teda $s(x)$ je $n.s.n.\{f(x), g(x)\}$. □

Z tejto vety vyplýva, že pre každé dva polynómy $f(x)$, $g(x)$ v okruhu polynómov $F[x]$ nad poľom F existuje n. s. n. a špeciálne aj $[f(x), g(x)]$. Podľa časti 3) tejto vety sú výroky "$n(x)$ je n. s. n. $f(x)$, $g(x)$" a "$n(x) \sim [f(x), g(x)]$" ekvivalentné a preto namiesto "$n(x)$ je n. s. n. $f(x)$, $g(x)$" môžeme písať "$n(x) \sim [f(x), g(x)]$".

Pojem najväčšieho spoločného deliteľa (najmenšieho spoločného násobku), ktorý sme definovali pre dvojicu polynómov je možné rozšíriť na ľubovoľný konečný počet polynómov.

6 Korene polynómov

Príklad 6.1. *Polynóm $f(x) = (x-1)^2, (x+1) \in \mathbb{R}[x]$ má v $\mathbb{R}$ korene 1 a -1. Koreň 1 je príklad dvojnásobného koreňa a koreň -1 jednoduchého koreňa polynómu $f(x)$.*

Definícia 6.1. *Nech F je podpole poľa F_1 (t. j. F_1 je rozšírenie F), x je neurčitá nad F_1 (a teda aj nad F), $f(x) \in F[x]$, $c \in F_1$ a $k \in \mathbb{N}$.*

a) Prvok c sa nazýva koreň polynómu $f(x)$, ak $f(c) = 0$ (podľa dôsledku 4.3 je to ekvivalentné s tým, že $x - c \mid f(x)$ v $F_1[x]$).

b)Prvok c sa nazýva k-násobný koreň polynómu $f(x)$, ak $(x-c)^k \mid f(x)$ a $(x-c)^{k+1} \nmid f(x)$ v $F_1[x]$.

c) 1-násobný koreň polynómu $f(x)$ sa nazýva jednoduchý koreň polynómu $f(x)$.

d) Ak $k \geq 2$, tak k-násobný koreň polynómu $f(x)$ sa nazýva viacnásobný koreň polynómu $f(x)$.

Príklad 6.2. *1. Polynóm $f(x) = (x-1)^3.(x^2-1) \in Q[x]$ má štvornásobný koreň 1 a jednoduchý koreň -1 ($f(x) = (x-1)^4.(x+1)$).*

2. Ak F je podpole poľa F_1 a $F[x]$ je okruh polynómov nad F, tak každý prvok $c \in F_1$ je koreňom nulového polynómu $0 \in F[x]$. Polynómy nultého stupňa nemajú žiadny koreň.

Veta 6.1. *Nech F je pole, $f(x) \in F[x]$, $stf(x) = n \geq 0$. Potom platí:*

1) Ak $c_1, ..., c_k \in F$ sú navzájom rôzne korene polynómu $f(x)$, pre každé i je c_i m_i-násobný koreň $f(x)$ a $g(x) = (x-c_1)^{m_1}. \ ... \ .(x-c_k)^{m_k}$, tak $g(x) \mid f(x)$.

2) Polynóm $f(x)$ má v poli F najviac n koreňov, pričom l-násobný koreň sa počíta l-krát.

Dôkaz. 1) Nech $c_1, ..., c_k \in F$ sú navzájom rôzne korene polynómu $f(x)$ v F a pre každé $i \in \{1, ..., k\}$ je c_i m_i-násobný koreň $f(x)$. Potom pre každé i platí $(x-c_i)^{m_i} \mid f(x)$, pre $i \neq j$ platí $(x-c_i, x-c_j) = 1$ a preto aj $((x-c_i)^{m_i}, (x-c_j)^{m_j}) = 1$. Pretože $((x-c_1)^{m_1}, (x-c_2)^{m_2}) = 1$, podľa vety 4.7.3) platí $(x-c_1)^{m_1}.(x-c_2)^{m_2} \mid f(x)$. Platí aj $((x-c_1)^{m_1}.(x-c_2)^{m_2}), (x-c_3)^{m_3}) = 1$ a preto $(x-c_1)^{m_1}.(x-c_2)^{m_2}).(x-c_3)^{m_3} \mid f(x)$... Takýmto postupom nakoniec dostaneme, že $g(x) = (x-c_1)^{m_1}.(x-c_2)^{m_2}). \ ... \ .(x-c_k)^{m_k} \mid f(x)$.

2) Ak $stf(x) = 0$, tak $f(x)$ nemá v F koreň a teda výrok platí. Nech $stf(x) = n \geq 1$. Ak $f(x)$ nemá v F žiadny koreň, tak výrok platí. Predpokladajme že $f(x)$ má v F m koreňov, $m \in \mathbb{N}$. Nech $c_1, ..., c_k \in F$ sú všetky navzájom rôzne korene polynómu $f(x)$ v F a pre každé $i \in \{1, ..., k\}$ je c_i m_i-násobný koreň $f(x)$. Potom $m_1 + ... + m_k = m$. Podľa 1), polynóm $g(x) = (x-c_1)^{m_1}. \ ... \ .(x-c_k)^{m_k}$ delí polynóm $f(x)$ a preto $stg(x) \leq stf(x) = n$. Ale $stg(x) = st(x-c_1)^{m_1} + ... + st(x-c_k)^{m_k} = m_1 + ... + m_k = m$ a teda $m \leq n$.

□

Dôsledok 6.1. *Nech pole F_1 je rozšírenie poľa F, $f(x) \in F[x]$, $stf(x) = n \geq 0$. Potom $f(x)$ má v F_1 najviac n koreňov, pričom k-násobný koreň sa počíta k-krát.*

Dôkaz. Bez ujmy na všeobecnosti môžeme predpokladať, že x je neurčitá aj nad F_1 a teda $F[x]$ je podokruh okruhu $F_1[x]$. Potom $f(x) \in F_1[x]$, $stf(x) = n \geq 0$ a podľa predchádzajúcej vety má $f(x)$ v poli F_1 najviac n koreňov, pričom k-násobný koreň sa počíta k-krát. □

Dôsledok 6.2. *Nech* $f(x) = a_0x^n + a_1x^{n-1} + ... + a_n \in F[x]$, $stf(x) = n \geq 1$ *(a teda* $a_0 \neq 0$*),* F_1 *je rozšírenie poľa* F *a* $c_1, \ ... \ , c_n \in F_1$ *sú (všetky) korene polynómu* $f(x)$ *(k-násobný koreň je napísaný k-krát). Potom platí:*

1) $f(x) = a_0(x - c_1).(x - c_2). \ ... \ .(x - c_n)$.

2) (Newtonove vzorce pre vzťahy medzi koreňmi a koeficientami polynómu)

$-a_1a_0^{-1} = c_1 + c_2 + ... + c_n$

$a_2a_0^{-1} = c_1c_2 + c_1c_3 + ... + c_1.c_n + c_2c_3 + c_2c_4 + ... + c_2c_n + ... + c_{n-1}c_n$

$-a_3a_0^{-1} = c_1c_2c_3 + c_1c_2c_4 + ... + c_1c_2c_n + ... + c_{n-2}c_{n-1}c_n$

. . . . . .

$(-\mathbf{1})^{n-1}a_{n-1}a_0^{-1} = c_1c_2...c_{n-1} + c_1c_2...c_n + ...c_2c_3...c_n$

$(-\mathbf{1})^n a_n a_0^{-1} = c_1c_2...c_n$

Dôkaz. 1) Zrejme $f(x) \in F_1[x]$ a pre polynóm $g(x)$ z vety 6.1.1) platí $g(x) = (x - c_1).(x - c_2). \ ... \ .(x - c_n)$. Pretože $g(x) \mid f(x)$ a $stg(x) = n = stf(x)$ platí $f(x) = cg(x)$, kde $c \in F\backslash\{0\}$. Porovnaním vedúcich koeficientov polynómov $f(x)$ a $cg(x)$ dostaneme, že $c = a_0$. Teda $f(x) = a_0(x - c_1).(x - c_2). \ ... \ .(x - c_n)$.

2) Pretože, podľa 1) platí $a_0^{-1}f(x) = (x - c_1).(x - c_2). \ ... \ .(x - c_n)$, Newtonove vzorce dostaneme ako rovnosti zodpovedajúcich koeficientov polynómov $a_0^{-1}f(x)$ a $(x - c_1).(x - c_2). \ ... \ .(x - c_n)$. □

Dôsledok 6.3. *Nech* $f(x), g(x) \in F[x]$, $n \in \mathbb{N}$, $1 \leq stf(x) \leq n$, $1 \leq stg(x) \leq n$, $c_0, \ ..., \ c_n$ *sú navzájom rôzne prvky poľa* F *a pre všetky* $i \in \{0, ..., n\}$ *platí* $f(c_i) = g(c_i)$. *Potom* $f(x) = g(x)$.

Dôkaz. Nech $h(x) = f(x) - g(x)$. Potom $sth(x) \leq max\{stf(x), stg(x)\} \leq n$. Nech $h(x) \neq 0$. Potom $sth(x) \geq 0$ a pre každé $i \in \{0, ..., n\}$ platí $h(c_i) = f(c_i) - g(c_i) = 0$, t. j. $f(x)$ má v F aspoň $n+1$ koreňov. Dostali sme spor. Preto $h(x) = f(x) - g(x) = 0$ a teda $f(x) = g(x)$. □

Veta 6.2. *(Lagrangeov interpolačný vzorec)*

Nech $n \in \mathbb{N}$, $c_0, \ ... \ , c_n$ *sú navzájom rôzne prvky poľa* F *a* $d_0, \ ... \ , d_n$ *sú ľubovoľné prvky poľa* F. *Potom existuje práve jeden polynóm* $f(x) \in F[x]$ *taký, že* $stf(x) \leq n$ *a pre všetky* $i \in \{0, ..., n\}$ *platí* $f(c_i) = d_i$. *Polynóm* $f(x)$ *je daný predpisom*

$f(x) = \sum_{i=0}^{n} d_i . \frac{(x-c_0).(x-c_1). \ ... \ .(x-c_{i-1}).(x-c_{i+1}). \ ... \ .(x-c_n)}{(c_i-c_0).(c_i-c_1). \ ... \ .(c_i-c_{i-1}).(c_i-c_{i+1}). \ ... \ .(c_i-c_n)}$.

Dôkaz. Je zrejmé, že $stf(x) \leq n$ a ľahko sa overí, že pre všetky i platí $f(c_i) = d_i$. Jednoznačnosť vyplýva z dôsledku 6.3. □

Príklad 6.3. *Nájdite polynóm* $f(x)$ *najviac* 2. *stupňa v* $\mathbb{R}[x]$, *pre ktorý platí* $f(1) = 2$, $f(2) = -1$ *a* $f(3) = 2$. *Použijeme Lagrangeov vzorec:*

$f(x) = 2.\frac{(x-2).(x-3)}{(1-2).(1-3)} - 1.\frac{(x-1).(x-3)}{(2-1).(2-3)} + 2.\frac{(x-1).(x-2)}{(3-1).(3-2)} = 3x^2 - 12x + 11.$

Definícia 6.2. *Pole* F *sa nazýva algebraicky uzavreté, ak každý polynóm* $f(x) \in F[x]$, $stf(x) \geq 1$ *má v poli* F *koreň.*

Príklad 6.4. *1. Pole $\mathbb{R}$ nie je algebraicky uzavreté. Polynóm $f(x) = x^2 + 1 \in \mathbb{R}[x]$ nemá v $\mathbb{R}$ koreň (pre každé $t \in \mathbb{R}$ je $f(t) \geq 1$).*

2. Pole $\mathbb{Z}_3$ nie je algebraicky uzavreté. Polynóm $f(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ nemá v $\mathbb{Z}_3$ koreň ($f(0) = 1$, $f(1) = 2$, $f(2) = 2$).

Veta 6.3. *(Gauss)*
Pole komplexných čísel je algebraicky uzavreté.

Dôsledok 6.4. *Každý polynóm $f(x) \in \mathbb{R}[x]$, $stf(x) \geq 1$ má v poli komplexných čísel koreň.*

Veta 6.4. *(Steinitz) Pre každé pole F existuje algebraicky uzavreté pole K, ktoré je rozšírením poľa F.*

Dôsledok 6.5. *Nech F je pole $f(x) \in F[x]$, $stf(x) \geq 1$. Potom existuje pole K, ktoré je rozšírením poľa F také, že polynóm $f(x)$ má v poli K aspoň jeden koreň.*

Teraz sa budeme zaoberať otázkou, ako je možné zistiť, či daný polynóm má viacnásobný koreň bez toho, aby sme tento koreň poznali. K tomu bude užitočné poznať pojem formálnej derivácie polynómu a niektoré jej vlastnosti.

Definícia 6.3. *Nech $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in F[x]$. Potom polynóm $Df(x) = a_1 + 2a_2x + ... + na_nx^{n-1} \in F[x]$ sa nazýva formálna derivácia polynómu $f(x)$.*

Príklad 6.5. *1) Nech $f(x) = 2 + x^2 + 2x^3 \in \mathbb{R}[x]$. Potom $Df(x) = 2x + 6x^2$.*
2) Nech $f(x) = x^5 + x + 1 \in \mathbb{Z}_5[x]$. Potom $Df(x) = 5x^4 + 1 = 1$.
3) Ak $f(x) = a_0 \in F[x]$, tak $Df(x) = 0$.

Veta 6.5. *Nech $f(x), g(x) \in F[x]$. Potom v $F[x]$ platí:*
1) $D(f(x) + g(x)) = Df(x) + Dg(x)$.
2) $D(f(x).g(x)) = (Df(x)).g(x) + f(x).Dg(x)$.

Dôkaz. 1) Nech $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$, $g(x) = b_0 + b_1x + b_2x^2 + ... + b_kx^k$. Nech napríklad $n \geq k$. Potom $f(x) + g(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... + (a_k + b_k)x^k + ... + a_nx^n$ a $D(f(x) + g(x) = (a_1 + b_1) + 2(a_2 + b_2)x + ...k(a_k + b_k)x^{k-1} + ... + na_nx^{n-1} = (a_1 + a_2x + ... + ka_kx^{k-1} + ... + a_nx^{n-1}) + (b_1 + 2b_2x + ... + kb_kx^{k-1}) = Df(x) + Dg(x)$.

2) Nech $g(x) = b_0 + b_1x + ... + b_kx^k \in F[x]$ je ľubovoľný polynóm.

a) Nech $f(x) = a \in F$. Potom $D(a.g(x)) = D(ab_0 + ab_1x + ab_2x^2 + ... + ab_kx^k) = ab_1 + 2ab_2x + ... + kab_kx^{k-1} = a.Dg(x) = D(a).g(x) + a.Dg(x)$.

b) Nech $f(x) = ax^n \in F[x]$, $n \geq 1$. Potom $D((ax^n).g(x)) = D(ab_0x^n + ab_1x^{n+1} + ab_2x^{n+2} + ... + ab_kx^{n+k}) = nab_0x^{n-1} + (n+1)ab_1x^n + (n+2)ab_2x^{n+1} + ... + (n+k)ab_kx^{n+k-1} = nab_0x^{n-1} + nab_1x^{n-1}.x + nab_2x^{n-1}.x^2 + ... + nab_kx^{n-1}.x^k + ab_1x^n + 2ab_2x^n.x + ... + kab_kx^n.x^{k-1} = nax^{n-1}.(b_0 + b_1x + b_2x^2 + ... + b_kx^k) + ax^n.(b_1 + 2b_2x + ... + kb_kx^{k-1}) = D(ax^n).g(x) + ax^n.Dg(x)$.

c) Nech teraz $f(x) \in F[x]$ je ľubovoľný polynóm, $f(x) = a_0 + a_1x + ... + a_nx^n$. Použitím 1), 2a), 2b) dostaneme: $D(f(x).g(x)) = D(a_0.g(x) + a_1x.g(x) + ... +$

$a_n x^n.g(x)) = D(a_0.g(x)) + D(a_1 x.g(x)) + ... + D(a_n x^n.g(x)) = D(a_0).g(x) + a_0.Dg(x) + D(a_1 x).g(x) + a_1 x.Dg(x) + ... + D(a_n x^n).g(x) + a_n x^n.Dg(x) = (D(a_0) + D(a_1 x) + ... + D(a_n x^n)).g(x) + (a_0 + a_1 x + ... + a_n x^n).Dg(x) = D(a_0 + a_1 x + ... + a_n x^n).g(x) + f(x).Dg(x) = (Df(x)).g(x) + f(x).Dg(x).$

□

Príklad 6.6. *1) Nech $x-c \in F[x]$. Dokážte, že pre každé $k \in \mathbb{N}$ platí $D(x-c)^k = k(x-c)^{k-1}$.*

Dokážeme to matematickou indukciou. Ak $k = 1$, tak $D(x-c)^1 = 1 = 1(x-c)^0$.

Nech platí $D(x-c)^k = k(x-c)^{k-1}$. Potom $D(x-c)^{k+1} = D((x-c)^k.(x-c)) = k(x-c)^{k-1}.(x-c) + (x-c)^k.\mathbf{1} = k(x-c)^k + (x-c)^k = (k+1)(x-c)^k$.

Všimnime si, že pre polynóm $x - 1 \in \mathbb{Z}_3[x]$ platí $D(x-1)^3 = 3(x-1) = 0$.

Nasledujúca veta dáva návod ako zistiť, či daný polynóm má viacnásobný koreň.

Veta 6.6. *Nech $f(x) \in F[x]$, $stf(x) \geq 1$. Potom $f(x)$ má v nejakom rozšírení poľa F viacnásobný koreň práve vtedy, keď $st(f(x), Df(x)) \geq 1$.*

Dôkaz. "⇒": Nech $f(x)$ má viacnásobný koreň $c \in F_1$, kde pole F_1 je rozšírenie F. Potom $(x-c)^2 \mid f(x)$ v $F_1[x]$ a teda existuje $g(x) \in F_1[x]$ tak, že $f(x) = (x-c)^2.g(x)$. Potom $Df(x) = 2(x-c).g(x) + (x-c)^2.Dg(x) = (x-c).(2g(x) + (x-c).Dg(x))$ a teda $x - c \mid Df(x)$ v $F_1[x]$. Nech $d(x) = (f(x), Df(x))$ v $F[x]$. Potom existujú $u(x), v(x) \in F[x]$ tak, že $d(x) = u(x).f(x) + v(x).Df(x)$. Pretože $x-c$ delí $f(x)$ aj $Df(x)$, $x - c \mid u(x).f(x) + v(x).Df(x) = d(x)$ v $F_1[x]$. Pretože $d(x) \neq 0$, platí $1 = st(x-c) \leq std(x)$.

"⇐": Nech $d(x) = (f(x), Df(x))$ v $F[x]$ a $std(x) \geq 1$. Potom, podľa dôsledku 6.4 existuje rozšírenie K poľa F, v ktorom má $d(x)$ koreň c. Potom $x - c \mid d(x)$ v $K[x]$ a pretože $d(x) \mid f(x)$ a $d(x) \mid Df(x)$ v $F[x]$ a $F[x] \subseteq K[x]$, platí tiež, že $x - c \mid f(x)$ a $x - c \mid Df(x)$ v $K[x]$. Teda existujú $h(x), r(x) \in K[x]$ také, že $f(x) = (x-c).h(x)$ a $Df(x) = (x-c).r(x)$. Potom (z prvej rovnosti) $Df(x) = h(x) + (x-c).Dh(x)$ a teda $(x-c).r(x) = h(x) + (x-c).Dh(x)$. Preto $h(x) = (x-c).(r(x) - Dh(x))$ a teda $f(x) = (x-c).h(x) = (x-c)^2.(r(x) - Dh(x))$. Z toho vyplýva, že c je viacnásobný koreň $f(x)$. □

Príklad 6.7. *Zistite, či polynóm $f(x) = x^3 + 4x^2 + 4x + 1 \in \mathbb{Z}_5[x]$ má viacnásobný koreň.*

Podľa predchádzajúcej vety k tomu použijeme polynóm $d(x) = (f(x), Df(x))$. $Df(x) = 3x^2 + 3x + 4$.

$$
\begin{array}{l}
x^3+4x^2+4x+1 : 3x^2+3x+4 = 2x+1 \\
-\underline{(x^3+x^2+3x)} \\
\qquad 3x^2+x+1 \\
\quad -\underline{(3x^2+3x+4)} \\
\qquad\quad 3x+2
\end{array}
$$

$$
\begin{array}{l}
3x^2+3x+4 : 3x+2 = x+2 \\
-\underline{(3x^2+2x)} \\
\qquad x+4 \\
\quad -\underline{(x+4)} \\
\qquad\quad 0
\end{array}
$$

Teda $d(x) \sim 3x+2$, $std(x) = 1$ *a preto* $f(x)$ *má viacnásobný koreň.*

Hovoríme, že pole F má charakteristiku $charF$ rovnú ∞, ak pre každé $a \in F$, $a \neq 0$ a pre každé $n \in \mathbb{N}$ platí $na \neq 0$. Toto je ekvivalentné s tým, že pre každé $n \in \mathbb{N}$ $n\mathbf{1} \neq 0$, kde $\mathbf{1}$ je jednotkový prvok poľa F. Skutočne ak pre každé $n \in \mathbb{N}$ platí $n\mathbf{1} \neq 0$ a $a \in F$, $a \neq 0$, tak $na = n(\mathbf{1}.a) = (n\mathbf{1}).a \neq 0$. Platnosť obrátenej implikácie je zrejmá. Napríklad, $char\mathbb{Q} = char\mathbb{R} = char\mathbb{C} = \infty$. Ak pole F_1 je rozšírením poľa F a $charF = \infty$, tak aj $charF_1 = \infty$ (lebo jednotkový prvok F_1 je ten istý ako jednotkový prvok F a jeho n-násobky v F_1 sú tie isté ako v n-násobky v F). Ak $charF = \infty$, $f(x) = a_0 + a_1x + ... + a_nx^n \in F[x]$, $stf(x) = n \geq 1$ (t. j. $a_n \neq 0$), tak pre jeho deriváciu $Df = a_1 + ... + na_nx^{n-1}$ platí, že $stDf(x) = n-1$ (lebo $na_n \neq 0$).

Napríklad v $\mathbb{Z}_5[x]$ má polynóm $f(x) = 1+2x+x^5$ stupeň 5 a jeho derivácia $Df(x) = 2$ má stupeň 0 ($\mathbb{Z}_5$ nemá charakteristiku rovnú ∞).

Veta 6.7. *Nech* F *je pole,* $charF = \infty$, $f(x) \in F[x]$, $f(x) \neq 0$, F_1 *je rozšírenie poľa* F *a* $c \in F_1$. *Potom platí:*

1) Ak c *je* k*-násobný koreň polynómu* $f(x)$, $k \geq 2$, *tak* c *je* $k-1$*-násobný koreň polynómu* $Df(x)$.

2) Ak c *je koreň* $f(x)$, $k \in \mathbb{N}$ *a* c *je* k*-násobný koreň* $Df(x)$, *tak* c *je* $k+1$*-násobný koreň* $f(x)$.

3) Ak c *je jednoduchý koreň* $f(x)$, *tak* c *nie je koreň* $Df(x)$.

Dôkaz. 1) Nech $k \geq 2$. Platí $(x-c)^k \mid f(x)$ a $(x-c)^{k+1} \nmid f(x)$ v $F_1[x]$. Potom existuje $g(x) \in F_1[x]$ tak, že $f(x) = (x-c)^k.g(x)$. Potom $Df(x) = k(x-c)^{k-1}g(x) + (x-c)^k.Dg(x) = (x-c)^{k-1}(kg(x) + (x-c).Dg(x))$ a teda $(x-c)^{k-1} \mid Df(x)$. Nech $(x-c)^k \mid Df(x)$. Potom existuje $h(x) \in F_1[x]$, pre ktorý platí $Df(x) = (x-c)^k.h(x)$. Potom $(x-c)^k.h(x) = (x-c)^{k-1}(kg(x)+(x-c).Dg(x))$ a pretože $(x-c)^{k-1} \neq 0$ a $F_1[x]$ je obor integrity, platí $(x-c)h(x) = kg(x)+(x-c).Dg(x)$. Potom $kg(x) = (k\mathbf{1}).g(x) = (x-c)(h(x)-Dg(x))$ a teda $x-c \mid g(x)$ $((k\mathbf{1}, x-c) = 1)$. Potom $g(x) = (x-c).r(x)$, kde $r(x) \in F_1[x]$ a $f(x) = (x-c)^k.g(x) = (x-c)^{k+1}.r(x)$ a preto $(x-c)^{k+1} \mid f(x)$. Dostali sme spor a teda $(x-c)^k \nmid Df(x)$. Ukázali sme, že c je $k-1$-násobný koreň $Df(x)$.

2) Nech c je koreň $f(x)$ a c je k-násobný koreň $Df(x)$ Potom $f(x) = (x-c).g(x)$, $Df(x) = (x-c)^k.h(x)$, kde $g(x), h(x) \in F_1[x]$ a $(x-c)^{k+1} \nmid Df(x)$. Platí tiež $Df(x) = g(x) + (x-c).Dg(x)$. Potom $g(x) + (x-c).Dg(x) = (x-c)^k.h(x)$ a z toho dostaneme, že $g(x) = (x-c).((x-c)^{k-1}.h(x) - Dg(x))$. Potom $f(x) =$

$(x-c).g(x) = (x-c)^2.((x-c)^{k-1}.h(x) - Dg(x))$ a teda c je aspoň dvojnásobný koreň $f(x)$. Nech c je l-násobný koreň $f(x)$. Potom $l \geq 2$ a podľa 1) je c $l-1$-násobný koreň $Df(x)$. Teda $l-1 = k$ a $l = k+1$.

3) Ak by c bol koreň $Df(x)$, tak podľa 2) by bol aspoň dvojnásobným koreňom $f(x)$, čo je spor s predpokladom.

□

Podobne, ako v matematickej analýze aj pre polynómy je užitočné definovať formálnu deriváciu n-tého rádu.

Definícia 6.4. *Nech F je pole, $f(x) \in F[x]$. Potom pre každé $n \in \mathbb{N}_0$ je definovaná n-tá formálna derivácia $D^{(n)}f(x)$ polynómu $f(x)$ nasledovne:*

1) $D^{(0)}f(x) = f(x)$.

2) Ak $n \in \mathbb{N}_0$, tak $D^{(n+1)}f(x) = D(D^{(n)}f(x))$.

Teda $D^{(1)}f(x) = Df(x)$, $D^{(2)}f(x) = D(Df(x))$, a. t. ď.

Z predchádzajúcej vety potom dostaneme nasledujúci dôsledok.

Dôsledok 6.6. *Nech F je pole, $charF = \infty$, $f(x) \in F[x]$, $f(x) \neq 0$, F_1 je rozšírenie poľa F, $c \in F_1$ a $k \in \mathbb{N}$. Potom c je k-násobný koreň polynómu $f(x)$ práve vtedy, keď $f(c) = Df(c) = ... = D^{(k-1)}f(c) = 0$ a $D^{(k)}f(c) \neq 0$.*

Ďalší dôsledok predchádzajúcej vety využijeme v dôkaze po ňom nasledujúcej vety.

Dôsledok 6.7. *Nech F je pole, $charF = \infty$, $f(x) \in F[x]$, $f(x) \neq 0$, $d(x) = (f(x), Df(x))$, F_1 je rozšírenie poľa F a $c \in F_1$. Potom ak $k \in \mathbb{N}$ a c je k-násobný koreň $f(x)$, tak $(x-c)^{k-1} \mid d(x)$ a $(x-c)^k \nmid d(x)$.*

Dôkaz. Existujú $u(x), v(x) \in F[x]$ také, že $d(x) = u(x).f(x) + v(x).Df(x)$. Ak $k \geq 2$, tak podľa predchádzajúcej vety $(x-c)^{k-1} \mid Df(x)$ v $F_1[x]$. Zrejme platí tiež $(x-c)^{k-1} \mid f(x)$ v $F_1[x]$ a preto $(x-c)^{k-1} \mid u(x).f(x)+v(x).Df(x) = d(x)$ v $F_1[x]$. Ak $(x-c)^k \mid d(x)$, tak (pretože $d(x) \mid Df(x)$) $(x-c)^k \mid Df(x)$ a to je spor s tým, že c je $k-1$- násobný koreň $Df(x)$. Teda $(x-c)^k \nmid d(x)$.

Ak $k = 1$, tak, zrejme $(x-c)^0 = \mathbf{1} \mid d(x)$. Ak $x-c \mid d(x)$, tak $x-c \mid Df(x)$ a to je spor s tým, že c nie je koreň $Df(x)$ podľa predchádzajúcej vety časť 3). □

.

Príklad 6.8. *Nech $F[x]$ je okruh polynómov nad poľom F, $x-c, r(x) \in F[x]$. Potom platí: Ak $x-c \nmid r(x)$ v $F[x]$, tak $(x-c, r(x)) = \mathbf{1}$ v $F[x]$. Skutočne, ak $x-c \nmid r(x)$, tak $r(x) \neq 0$. Nech $(x-c, r(x)) = d(x) \neq \mathbf{1}$. Potom $std(x) \geq 1$ a pretože $d(x) \mid x-c$ platí $std(x) = 1$. Potom $d(x) \sim x-c$ a preto $x-c \mid r(x)$. Dostali sme spor.*

Nasledujúca veta dáva návod ako k polynómu, ktorý má viacnásobné korene je možné nájsť polynóm, ktorý má tie isté korene a všetky jeho korene sú jednoduché.

Veta 6.8. *Nech F je pole, $charF = \infty$, $f(x) \in F[x]$, $d(x) = (f(x), Df(x))$ a $g(x) \in F[x]$ je taký polynóm, pre ktorý platí $f(x) = d(x).g(x)$ (taký polynóm existuje, lebo $d(x) \mid f(x)$ v $F[x]$). Potom platí:*

1) Ak F_1 je rozšírenie poľa F a $c \in F_1$, tak c je koreň $f(x)$ práve vtedy, keď c je koreň $g(x)$.

2) Všetky korene polynómu $g(x)$ sú jednoduché.

Dôkaz. 1) Nech c je k-násobný koreň $f(x)$, $k \in \mathbb{N}$. Potom $(x-c)^k \mid f(x)$ a podľa predchádzajúceho dôsledku $(x-c)^{k-1} \mid d(x)$, $(x-c)^k \nmid d(x)$. Potom existujú $h(x), r(x) \in F_1[x]$ tak, že $f(x) = (x-c)^k.h(x)$ a $d(x) = (x-c)^{k-1}.r(x)$. Zrejme $x - c \nmid r(x)$ (lebo v opačnom prípade by platilo, že $(x-c)^k \mid d(x)$). Potom $(x-c)^k.h(x) = f(x) = d(x).g(x) = (x-c)^{k-1}.r(x).g(x)$ a pretože $(x-c)^{k-1} \neq 0$, dostávame $(x-c).h(x) = r(x).g(x)$. Teda $x - c \mid r(x).g(x)$ v $F_1[x]$. Ak $x-c \nmid g(x)$ v $F_1[x]$, tak $(x-c, g(x)) = \mathbf{1}$ v $F_1[x]$ a pretože $x-c \nmid r(x)$, platí tiež $(x-c, r(x)) = \mathbf{1}$ v $F_1[x]$. Potom ale platí $(x-c, r(x).g(x)) = \mathbf{1}$ v $F_1[x]$ a preto $x-c \nmid r(x).g(x)$ v $F_1[x]$, čo dáva spor. Teda $x-c \mid g(x)$ v $F_1[x]$ a preto c je koreň $g(x)$.

Obrátene, nech c je koreň $g(x)$. Potom $g(c) = 0$ a preto aj $f(c) = d(c).g(c) = 0$. Teda c je koreň $f(x)$.

2) Nech c je viacnásobný koreň $g(x)$. Potom $(x-c)^2 \mid g(x)$ a pretože $g(x) \mid f(x)$ platí aj $(x-c)^2 \mid f(x)$. Nech c je k-násobný koreň $f(x)$. Potom $k \geq 2$ a podľa predchádzajúceho dôsledku $(x-c)^{k-1} \mid d(x)$. Potom $(x-c)^{k+1} = (x-c)^{k-1}.(x-c)^2 \mid d(x).g(x) = f(x)$ a to je spor s tým, že c je k-násobný koreň $f(x)$. Teda c je jednoduchý koreň $g(x)$. □

Príklad 6.9. *Zistite, či polynóm $f(x) = x^6 - 6x^4 - 4x^3 + 9x^2 + 12x + 4 \in \mathbb{R}[x]$ má viacnásobné korene. Ak áno, tak nájdite polynóm $g(x) \in \mathbb{R}[x]$, ktorý má tie isté korene ako $f(x)$ a všetky jeho korene sú jednoduché.*

Najprv určíme $Df(x) = 6x^5 - 24x^3 - 12x^2 + 18x + 12$.

Potom určíme $d(x) = (f(x), Df(x)) = x^4 + x^3 - 3x^2 - 5x - 2$. Pretože $std(x) = 4 \geq 1$ polynóm $f(x)$ má aspoň jeden viacnásobný koreň.

Nakoniec vydelíme polynóm $f(x)$ polynómom $d(x)$ a dostaneme $f(x) : d(x) = x^2 - x - 2$. Teda $g(x) = x^2 - x - 2$.

Môžeme si ešte všimnúť, že -1 a 2 sú všetky korene $g(x)$ a preto sú to aj všetky korene $f(x)$.

Literatúra

[1] G. Birkhoff, S. Mac Lane: Prehľad modernej algebry, ALFA, Bratislava 1979

[2] T. Katriňák, M. Gavalec, E. Gedeonová, J. Smítal: Algebra a teoretická aritmetika 1, UK Bratislava, 2002

[3] F. Šik: Algebra I., UJEP Brno, 1962 (skriptá)