OKRUHY POLYNOMŮ PRO DISKRÉTNÍ LINEÁRNÍ ŘÍZENÍ

0. Úvod

Algebraická teorie diskrétního lineárního řízení vznikla jako speciální obor teorie řízení začátkem sedmdesátých let dvacátého století. V této době totiž dochází k prudkému vývoji výpočetní techniky, která začíná pronikat do všech oblastí lidské činnosti. Také při řízení složitých procesů jsou stále větší měrou využívány ve funkci regulátorů počítače. Pro modelování na počítači však už není postačující dosavadní teorie, která byla vytvořena pro soustavy spojitě řízené jednoduchými regulátory. Vzniká potřeba vybudování nové teorie, která by byla vhodná pro řízení soustav pomocí počítačů, tedy teorie, která by svou podstatou byla diskrétní.

Touto novou teorií se stala teorie diskrétního lineárního řízení, která se nazývá algebraická, neboť pracuje s algebraickými pojmy (okruh, obor integrity, těleso) a využívá algebraických metod. Základním nástrojem jsou polynomy, které jsou chápány ne jako funkce, nýbrž jako konečné posloupnosti (svých koeficientů). Tím je možno jednotným způsobem popsat soustavy definované nad libovolnými tělesy. Podobně formální mocninné řady, které definují přenos soustav, jsou chápány jako nekonečné posloupnosti. Přenos soustavy lze pak vyjádřit jako zlomek, jehož čitatelem i jmenovatelem jsou polynomy. Základní myšlenka algebraické metody syntézy optimálního řízení využívá skutečnosti, že s polynomy je možno manipulovat zcela samostatně, čímž je algebra racionálních přenosů převedena na mnohem jednodušší algebru polynomů. Syntéza optimálního řízení se tak redukuje na řešení lineární polynomiální rovnice, při jejímž hledání lze s výhodou využít počítače.

Algebraická teorie diskrétního lineárního řízení je moderní obor teorie řízení, který nachází bohaté aplikace a je proto intenzivně studován a rozvíjen. Je založen na matematickém aparátu, který není všeobecně znám a v literatuře týkající se oboru obvykle není dostatečně vyložen.Proto jsme se pokusili v našem učebním textu monografickou formou shrnout základy matematické teorie, na níž je algebraická teorie lineárního řízení založena. Poznamenejme také, že některé z uváděných algoritmů týkající se polynomů jsou obsaženy jako procedury v běžných systémech symbolické matematiky pro PC, jako např. Mathematica, Maple, MathCad, atd.

Při psaní textu jsme vycházeli z knihy [5] Vladimíra Kučery s názvem Algebraická teorie diskrétního lineárního řízení (Academia, Praha 1978), která je základní českou publikací v oboru. Učební text lze tedy chápat jako doplněk - matematicko-teoretický základ - této knihy, s níž jsme se snažili sladit i terminologii.

Autoři

1. Okruhy a tělesa

Úvodem kapitoly připomeňme některé základní algebraické pojmy. *Operací* (přesněji *binární operací*) na dané neprázdné množině G rozumíme zobrazení množiny $G \times G$ do G. K označení operace budeme nejčastěji užívat symbol $\cdot$ (tzv. *multiplikativní značení*) nebo $+$ (tzv. *aditivní značení*). Tedy operace $\cdot$, resp. $+$ na množině G přiřazuje každé (uspořádané) dvojici prvků $a, b \in G$ prvek $a \cdot b \in G$, resp. $a + b \in G$. Při multiplikativním zápisu ovšem symbol $\cdot$ obvykle vynecháváme, tj. píšeme ab místo $a \cdot b$.

Množina, na níž je definována operace, se nazývá *grupoid*. Nechť G je grupoid a nechť příslušná operace na G je značena multiplikativně. Prvek $e \in G$ se nazývá *neutrálním prvkem* grupoidu G, jestliže pro každý prvek $a \in G$ platí $ea = ae = a$. Zřejmě každý grupoid má nejvýše jeden neutrální prvek (jsou-li totiž e, e' neutrální prvky grupoidu G, pak $e = ee' = e'$). Neutrální prvek se v případě multiplikativního značení operace často nazývá *jednotkovým prvkem* a v případě aditivního značení *nulovým prvkem*.

Grupoid G se nazývá *pologrupa*, jestliže v něm platí *asociativní zákon*, tj. $(ab)c = a(bc)$ pro všechna $a, b, c \in G$. Totožné prvky $(ab)c$ a $a(bc)$ pologrupy zapisujeme často ve tvaru abc. *Komutativním grupoidem* rozumíme grupoid G, v němž platí *komutativní zákon*, tj. $ab = ba$ pro všechna $a, b \in G$. Pologrupa s neutrálním prvkem se nazývá *monoid*. Monoid G se nazývá *grupa*, jestliže ke každému prvku $a \in G$ existuje *inverzní prvek*, tj. prvek $a^{-1} \in G$ s vlastností $aa^{-1} = a^{-1}a = e$ (kde e je neutrální prvek monoidu G). Tento inverzní prvek je pak určen jednoznačně (neboť pro libovolné dva prvky b, c inverzní k a platí $b = eb = (ca)b = c(ab) = ce = c$). Neutrální prvek je zřejmě inverzní sám k sobě, tj. $e^{-1} = e$. Je-li a^{-1} inverzní k a, pak je a inverzní k a^{-1}, tj. $(a^{-1})^{-1} = a$. V případě aditivního značení operace místo o inverzním prvku hovoříme o *opačném prvku* a místo a^{-1} užíváme označení $-a$. Připomeňme také, že místo a^{-1} často píšeme $\frac{1}{a}$ a v případě komutativního grupoidu místo ab^{-1} píšeme $\frac{a}{b}$. Místo $a + (-b)$ obvykle užíváme stručnější zápis $a - b$.

Např. množina všech celých čísel s operací $+$ je komutativní grupa (s nulovým prvkem 0), zatímco tato množina s operací $\cdot$ je jen komutativní monoid (jehož jednotkovým prvkem je 1), neboť k 0 neexistuje inverzní prvek.

1.1. Definice. Neprázdná množina G, na níž jsou definovány operace $+$ a $\cdot$, se nazývá *okruh*, jestliže platí:
(1) G s operací $+$ je komutativní grupa, kterou nazýváme *aditivní grupou* okruhu G.
(2) G s operací $\cdot$ je monoid, který nazýváme *multiplikativním monoidem* okruhu G.
(3) V G platí tzv. *levý distributivní zákon*
$$a(b + c) = ab + ac \text{ pro všechna } a, b, c \in G$$
a tzv. *pravý distributivní zákon*
$$(b + c)a = ba + ca \text{ pro všechna } a, b, c \in G.$$

Symbolem 0 označujeme *nulový prvek* okruhu G, tj. nulový prvek jeho aditivní grupy, a symbolem 1 *jednotkový prvek* okruhu G, tj. jednotkový prvek jeho multiplikativního monoidu. Je-li $a \in G$, pak *opačným*, resp. *inverzním prvkem* k prvku a v okruhu G rozumíme opačný prvek $-a$ k a v aditivní grupě okruhu G, resp. inverzní prvek a^{-1} k a v multiplikativním monoidu okruhu G.

1.2. Tvrzení. *V libovolném okruhu G platí:*

(1) $a0 = 0a = 0$ *pro každé* $a \in G$.
(2) $(-a)b = -(ab) = a(-b)$ *pro všechna* $a, b \in G$.
(3) $(-a)(-b) = ab$ *pro všechna* $a, b \in G$.
(4) $a(b-c) = ab - ac$, $(b-c)a = ba - ca$ *pro všechna* $a, b, c \in G$.
(5) $(\sum_{i=1}^{m} a_i)(\sum_{j=1}^{n} b_j) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j$ *pro všechna* $a_1, ..., a_m, b_1, ..., b_n \in G$ *(tzv. zobecněný distributivní zákon).*

Důkaz. (1) Pro libovolné $a \in G$ máme $a0 = a(0+0)$, takže užitím levého distributivního zákona dostáváme $a0 = a0 + a0$. Přičtením prvku $-(a0)$ k oběma stranám této rovnosti obdržíme $a0 = 0$. Analogicky se dokáže rovnost $0a = 0$.
(2) Pro $a, b \in G$ máme $(-a)b + ab = (-a+a)b = 0b = 0$, čili $(-a)b = -(ab)$. Analogicky lze ukázat, že $a(-b) = -(ab)$.
(3) Z (2) plyne $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$ pro všechna $a, b \in G$.
(4) Pro libovolné prvky $a, b, c \in G$ v důsledku levého distributivního zákona a rovnosti (2) máme $a(b-c) = a(b+(-c)) = ab + a(-c) = ab + (-(ac)) = ab - ac$. Podobně se dokáže druhá rovnost.
(5) Nejprve se ukáže, že rovnost platí pro $m = 1$, a to matematickou indukcí podle n s využitím levého distributivního zákona. Matematickou indukcí podle m a využitím pravého distributivního zákona se pak dokáže uvedené pravidlo.

Okruh G se nazývá *triviální*, jestliže $G = \{0\}$. Zřejmě je G triviální, právě když $0 = 1$ (neboť z rovnosti $0 = 1$ a z 1.2(1) plyne $a = 1a = 0a = 0$ pro všechna $a \in G$). Jestliže multiplikativní monoid okruhu G je komutativní, pak se G nazývá *komutativní* (a jelikož levý a pravý distributivní zákon jsou v tomto případě ekvivalentní, nerozlišujeme je a hovoříme o *distributivním zákonu*).

1.3. Příklady. a) Množiny $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ všech celých, racionálních, reálných a komplexních čísel s obvyklým sčítáním a násobením jsou zřejmě komutativní okruhy. Množina $\mathbb{N}$ všech přirozených (tj. celých nezáporných) čísel s těmito operacemi ovšem okruh není, neboť $\mathbb{N}$ s operací $+$ je jen monoid, nikoliv grupa.

b) Buď $\mathcal{F}[0,1]$ množina všech spojitých (reálných) funkcí definovaných na intervalu [0,1]. Pro libovolné prvky $f, g \in \mathcal{F}[0,1]$ položme $(f+g)(t) = f(t) + g(t)$ a $(fg)(t) = f(t)g(t)$ pro všechna $t \in [0,1]$. Pak $\mathcal{F}[0,1]$ je komutativní okruh.

c) Množina $\mathcal{M}_n$ všech čtvercových matic n-tého řádu ($n > 1$ přirozené číslo) nad $\mathbb{R}$ s obvyklými operacemi sčítání a násobení matic je okruh, který není komutativní.

1.4. Definice. Okruhy G_1 a G_2 se nazývají *izomorfní*, jestliže existuje bijekce $f : G_1 \to G_2$ taková, že pro libovolné prvky $a, b \in G_1$ platí $f(a+b) = f(a) + f(b)$ a $f(ab) = f(a)f(b)$. Tato bijekce se pak nazývá *izomorfismus*.

Zřejmě bijekce $f : G_1 \to G_2$ z 1.4 má také tu vlastnost, že $f(0)$ je nulovým a $f(1)$ jednotkovým prvkem okruhu G_2. Izomorfní okruhy lze tedy z algebraického hlediska považovat za totožné (neboť se liší jen charakterem svých prvků).

1.5. Definice. Buď G okruh. Prvek $a \in G - \{0\}$ se nazývá *dělitel nuly*, jestliže existuje prvek $b \in G - \{0\}$ tak, že platí $ab = 0$ nebo $ba = 0$. Netriviální komutativní okruh, který nemá dělitele nuly, se nazývá *obor integrity*.

1.6. Tvrzení. *Netriviální komutativní okruh* G *je obor integrity, právě když v něm platí tzv. zákon o krácení:*

Jestliže $a, b, c \in G$ *jsou libovolné prvky s vlastností* $ab = ac$ *a* $a \neq 0$, *pak* $b = c$.

Důkaz. Nechť v G platí zákon o krácení a nechť $a, b \in G$ jsou libovolné prvky s vlastností $ab = 0$. Pak $ab = a0$, tedy $a = 0$ nebo $b = 0$. Tedy G nemá dělitele nuly. Naopak, nechť G nemá dělitele nuly a nechť $a, b, c \in G$ jsou libovolné prvky s vlastností $ab = ac$ a $a \neq 0$. Pak $ab - ac = 0$, tedy $a(b - c) = 0$. Odtud $b - c = 0$, takže $b = c$.

Samozřejmě, zákon o krácení v předchozí větě lze ekvivalentně vyjádřit tak, že v něm rovnost $ab = ac$ nahradíme rovností $ba = ca$ (jelikož je G komutativní).

1.7. Příklady. Okruhy $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ jsou obory integrity. Naproti tomu komutativní okruh $\mathcal{F}[0, 1]$ není obor integrity.

V okruhu obecně neexistuje ke každému nenulovému prvku prvek inverzní. Protože však inverzní prvky hrají významnou roli při řešení rovnic, budeme se zajímat o ty prvky okruhu, k nimž inverzní prvky existují.

1.8. Definice. Buď G okruh a $e \in G$ libovolný prvek. Jestliže existuje k prvku e prvek inverzní, pak se e nazývá *jednotka.*

1.9. Tvrzení. *Množina všech jednotek v okruhu tvoří (multiplikativní) grupu.*

Důkaz. Zřejmě jednotkový prvek okruhu je jednotkou a pro libovolné dvě jednotky a, b platí $(ab)^{-1} = b^{-1}a^{-1}$.

1.10. Definice. Buď G okruh a $a, b \in G$.

Prvky a, b se nazývají *zleva (zprava) asociované* a píšeme $a \sim_l b$ ($a \sim_r b$), jestliže existuje jednotka e v G s vlastností $a = eb$ ($a = be$).

Říkáme, že prvek b je *levým (pravým) dělitelem* prvku a a píšeme $b|_l a$ ($b|_r a$), jestliže existuje prvek $c \in G$ s vlastností $a = bc$ ($a = cb$). V opačném případě píšeme $b \nmid_l a$ ($b \nmid_r a$).

Prvek $d \in G$ se nazývá *společný levý (pravý) dělitel* prvků a, b, je-li levým (pravým) dělitelem každého z nich.

Společný levý (pravý) dělitel d prvků a, b se nazývá jejich *největším společným levým (pravým) dělitelem*, jestliže každý společný levý (pravý) dělitel prvků a, b je levým (pravým) dělitelem prvku d. Množinu všech největších společných levých, resp. pravých dělitelů prvků a, b označíme symbolem $(a, b)_l$, resp. $(a, b)_r$.

Říkáme, že prvky a, b jsou *zleva (zprava) nesoudělné*, jsou-li jejich společnými levými (pravými) děliteli jen jednotky v G.

Je snadno vidět, že relace $\sim_l$ a $\sim_r$ jsou ekvivalence na G.

1.11. Tvrzení. *Buď G okruh a $a, b \in G$. Pak platí:*
(1) Jestliže $a \sim_r b$, pak $a|_l b$ a $b|_l a$. Pokud je G obor integrity, pak platí i opačná implikace.
(2) Nechť $d_1 \in (a, b)_l$ a $d_2 \in G$ jsou libovolné prvky. Jestliže $d_1 \sim_r d_2$, pak $d_2 \in (a, b)_l$. Pokud je G obor integrity, platí také opačná implikace.
(3) Jsou-li prvky a, b zleva nesoudělné, pak $1 \in (a, b)_l$. Je-li G komutativní, pak platí i opačná implikace.

Důkaz. (1) Nechť $a \sim_r b$. Pak existuje jednotka $e \in G$ tak, že $a = be$, tj. $b = ae^{-1}$. Tedy $b|_l a$ a $a|_l b$. Nechť G je obor integrity a nechť naopak $a|_l b$ a $b|_l a$. Pak existují prvky $c_1, c_2 \in G$ tak, že $b = ac_1$ a $a = bc_2$. Jestliže $a = 0$, pak $b = 0$, tudíž $a \sim_r b$. Nechť $a \neq 0$. Potom $a1 = a = bc_2 = (ac_1)c_2 = a(c_1c_2)$, takže podle 1.6 máme $1 = c_1c_2$. Proto je c_2 jednotka, tedy $a \sim_r b$.

(2) Nechť $d_1 \sim_r d_2$. Pak existuje jednotka $e \in G$ tak, že $d_1 = d_2 e$. Jelikož $d_1|_l a$ a $d_1|_l b$, existují prvky $c_1, c_2 \in G$ tak, že $a = d_1 c_1$ a $b = d_1 c_2$. Odtud $a = d_2 e c_1$ a $b = d_2 e c_2$, tedy $d_2|_l a$ a $d_2|_l b$. Je-li nyní $d_3 \in G$ libovolný společný levý dělitel prvků a, b, pak $d_3|_l d_1$, proto existuje $c_3 \in G$ s vlastností $d_1 = d_3 c_3$. Odtud $d_2 e = d_3 c_3$, čili $d_2 = d_3 c_3 e^{-1}$. Tedy $d_3|_l d_2$, což znamená, že $d_2 \in (a, b)_l$. Jestliže naopak platí $d_2 \in (a, b)_l$ a G je obor integrity, pak $d_1|_l d_2$ a $d_2|_l d_1$, takže $d_1 \sim_r d_2$ podle (1).
(3) Nechť a, b jsou zleva nesoudělné. Zřejmě $1|_l a$ i $1|_l b$. Nechť $c \in G$ je libovolný prvek s vlastností $c|_l a$, $c|_l b$. Pak c je jednotka v G, tedy $c|_l 1$. Proto $1 \in (a, b)_l$. Naopak, nechť G je komutativní, nechť $1 \in (a, b)_l$ a nechť $c \in G$ je libovolný prvek s vlastností $c|_l a$ a $c|_l b$. Pak $c|_l 1$, tedy c je jednotka v G. To znamená, že a, b jsou zleva nesoudělné.

Pro "pravé" pojmy samozřejmě platí analogie tvrzení 1.11.

1.12. Definice. Buď G okruh. Prvek $a \in G - \{0\}$, který není jednotkou, se nazývá *zleva (zprava) ireducibilní*, jestliže pro libovolný prvek $b \in G$ z podmínky $b|_l a$ ($b|_r a$) vyplývá, že b je jednotka nebo $b \sim_r a$ ($b \sim_l a$).

Jestliže G je komutativní okruh, pak v definicích 1.10 a 1.12 všechny "levé" a "pravé" pojmy splývají, proto adverbia "zleva", "zprava" a adjektiva "levý", "pravý" vynecháváme. Místo $\sim_l$ a $\sim_r$ pak píšeme $\sim$, místo $|_l$ a $|_r$, resp. $\nmid_l$ a $\nmid_r$ píšeme $|$, resp. $\nmid$ a místo $(a, b)_l$ a $(a, b)_r$ píšeme (a, b).

1.13. Příklady. a) V oboru integrity $\mathbb{Z}$ jsou jednotky právě čísla 1 a -1, takže dva prvky jsou asociované, právě když se rovnají nebo liší o znaménko. Proto ireducibilní prvky v $\mathbb{Z}$ jsou právě všechna prvočísla větší než 1 a všechna čísla k nim opačná.

b) V okruhu $\mathcal{M}_n$ čtvercových matic n-tého řádu nad nějakým tělesem T je nenulová matice $A \in \mathcal{M}_n$ dělitelem nuly, resp. jednotkou, právě když A je singulární, resp. regulární.

c) Buď $n \geq 1$ přirozené číslo a pro libovolná čísla $a, b \in \mathbb{Z}$ položme $a \equiv b (\mathrm{mod}\ n)$, právě když $n|(a-b)$ v $\mathbb{Z}$. Pak relace $\equiv (\mathrm{mod}\ n)$ je ekvivalence, která vytváří rozklad množiny $\mathbb{Z}$ na právě n tříd $C_0, C_1, ..., C_{n-1}$, kde $i \in C_i$ pro každé $i \in \{0, 1, ..., n-1\}$. Nechť $\mathbb{Z}_n = \{C_0, C_1, ..., C_{n-1}\}$ a pro libovolná $i, j, k \in \{0, 1, ..., n-1\}$ položme $C_i + C_j = C_k \Leftrightarrow i + j \equiv k (\mathrm{mod}\ n)$ a $C_i C_j = C_k \Leftrightarrow ij \equiv k (\mathrm{mod}\ n)$. Pak $\mathbb{Z}_n$ je komutativní okruh, který se nazývá *okruh zbytkových tříd modulo n.* Jednotky v $\mathbb{Z}_n$ jsou ty třídy C_i, pro něž je i nesoudělné s n v $\mathbb{Z}$, zatímco dělitelé nuly jsou ty třídy C_i, pro něž je i soudělné s n v $\mathbb{Z}$.

1.14. Definice. Okruh G takový, že množina $G - \{0\}$ s operací $\cdot$ je grupa, se nazývá *těleso.*

Zřejmě komutativní tělesa (tj. komutativní okruhy, které jsou tělesa) jsou obory integrity. Pro komutativní tělesa se v literatuře někdy používá termínu *pole.* Nadále budeme v textu tělesem vždy rozumět komutativní těleso.

1.15. Příklady. Obory integrity $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ jsou tělesa. Jestliže n je prvočíslo, pak $\mathbb{Z}_n$ je těleso.

1.16. Definice. *Hodnota* v tělese T je zobrazení $H : T \to \mathbb{R}$, které splňuje následující čtyři axiomy:
(i) $\forall a \in$T: $H(a) \geq 0$,
(ii) $\forall a \in$T: $H(a) = 0 \Leftrightarrow a = 0$,

(iii) $\forall a, b \in T : H(ab) = H(a)H(b)$,
(iv) $\forall a, b \in T : H(a + b) \leq H(a) + H(b)$.

1.17. Tvrzení. *Je-li H hodnota v tělese T, pak pro libovolný prvek $a \in T$ platí:*
(1) $H(1) = 1$,
(2) $H(-a) = H(a)$,
(3) $H(a^{-1}) = \frac{1}{H(a)}$, *jestliže* $a \neq 0$.

Důkaz. (1) Nechť $a \in T - \{0\}$ je libovolný prvek. Potom $H(a) = H(1)H(a)$, takže $H(1) = 1$, neboť $H(a) \neq 0$.
(2) Užitím dokázaného vztahu (1) dostáváme $(H(-1))^2 = H(-1)H(-1) = H(1) = 1$, takže $H(-1) = 1$. Odtud $H(-a) = H(-1)H(a) = H(a)$.
(3) Máme $H(a)H(a^{-1}) = H(1) = 1$, tedy $H(a^{-1}) = \frac{1}{H(a)}$.

1.18. Příklady. (1) V tělesech $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ je hodnotou absolutní hodnota.
(2) V každém tělese T existuje tzv. *triviální hodnota* H, pro niž platí $H(a) = 1$ pro všechna $a \in T - \{0\}$. Např. v tělese $\mathbb{Z}_n$, kde n je prvočíslo, jiná hodnota než triviální neexistuje.

1.19. Definice. Říkáme, že posloupnost $\{a_0, a_1, a_2, ...\}$ prvků tělesa T *konverguje k nule* vzhledem k hodnotě H v T, jestliže k libovolnému $\varepsilon \in \mathbb{R}$, $\varepsilon > 0$ existuje přirozené číslo n_0 takové, že pro všechna $n > n_0$ platí $H(a_n) < \varepsilon$.

1.20. Příklady. V $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$ konverguje daná posloupnost k nule vzhledem k hodnotě dané absolutní hodnotou, právě když konverguje k nule v obvyklém pojetí. Zřejmě posloupnost v libovolném tělese T konverguje k nule vzhledem k triviální hodnotě, právě když od jistého indexu jsou všechny prvky této posloupnosti rovny nulovému prvku tělesa T.

Buď G okruh a $G' \subseteq G$ podmnožina. Jestliže $0 \in G'$, $1 \in G'$ a $+, \cdot$ jsou operace na G' (tj. $a + b, ab \in G'$ pro všechna $a, b \in G'$), pak G' je okruh, který se nazývá *podokruh* okruhu G. Je-li G' dokonce obor integrity, resp. těleso, pak se nazývá *podoborem integrity*, resp. *podtělesem* okruhu G. Tak například $\mathbb{Z}$ je podoborem integrity tělesa $\mathbb{Q}$, $\mathbb{Q}$ je podtělesem tělesa $\mathbb{R}$ a $\mathbb{R}$ je podtělesem tělesa $\mathbb{C}$.

2. Formální mocninné řady

2.1. Definice. Buď T těleso. *Formální mocninnou řadou* nad tělesem T rozumíme výraz

$$\mathbf{a} = a_0 + a_1 z + a_2 z^2 + ...,$$

kde $a_0, a_1, a_2, ...$ jsou prvky tělesa T, tzv. *koeficienty* řady $\mathbf{a}$, a z je tzv. *neurčitá* řady $\mathbf{a}$. Nejmenší přirozené číslo n takové, že $a_n \neq 0$, nazýváme *řádem* formální mocninné řady $\mathbf{a}$ a značíme symbolem $\mathcal{O}\mathbf{a}$. Pokud jsou všechny koeficienty řady $\mathbf{a}$ rovny nule, pak klademe $\mathcal{O}\mathbf{a} = \infty$.

Množinu všech formálních mocninných řad s neurčitou z nad tělesem T označíme symbolem $T(z)$.

Formální mocninnou řadu s neurčitou z chápeme jako algebraický objekt, nikoliv jako obvyklou mocninnou řadu, tj. funkci proměnné z. V teorii diskrétního lineárního řízení se z aplikačních důvodů za neurčitou ve formálních mocninných řadách často volí z^{-1} místo z (takže se v těchto řadách na místech exponentů u z vyskytují jen záporná celá čísla). Jedná se jen o jiný způsob zápisu, v našem

textu se přidržíme jednoduššího a z matematického hlediska přirozenějšího zápisu s kladnými (celými) exponenty u z.

Formální mocninná řada $\mathbf{a} = a_0 + a_1 z + a_2 z^2 + ...$ s neurčitou z (nad daným tělesem) je zřejmě jednoznačně určena posloupností $\{a_0, a_1, a_2, ...\}$ svých koeficientů. Buďte nyní $\mathbf{a}, \mathbf{b} \in T(z)$ formální mocninné řady a nechť $\{a_0, a_1, ...\}$ a $\{b_0, b_1, ...\}$ jsou posloupnosti jejich koeficientů. Nechť $\mathbf{a} + \mathbf{b}$, resp. $\mathbf{ab}$ je formální mocninná řada s neurčitou z nad tělesem T, jejíž posloupnost koeficientů $\{c_0, c_1, ...\}$, resp. $\{d_0, d_1, ...\}$ je dána vztahem

$$c_k = a_k + b_k, \text{ resp. } d_k = \sum_{i,j \in \mathbb{N}, i+j=k} a_i b_j \text{ pro všechna } k \in \mathbb{N}.$$

2.2. Tvrzení. *Množina $T(z)$ s výše definovanými operacemi sčítání a násobení tvoří obor integrity. Nulovým, resp. jednotkovým prvkem tohoto oboru integrity je řada, jejíž posloupností koeficientů je posloupnost $\{0, 0, 0, ...\}$, resp. $\{1, 0, 0, ...\}$. Opačným prvkem k řadě $\mathbf{a} \in T(z)$, $\mathbf{a} = a_0 + a_1 z + a_2 z^2 + ...$, je řada, jejíž posloupnost koeficientů je $\{-a_0, -a_1, -a_2, ...\}$.*

Důkaz. Je snadno vidět, že $T(z)$ je vzhledem k definovanému sčítání komutativní grupa, v níž nulový prvek a opačný prvek k danému prvku mají uvedený tvar. Zřejmě $T(z)$ s definovaným násobením je komutativní grupoid, jehož jednotkový prvek má uvedený tvar. Ukážeme, že toto násobení je asociativní. Nechť $\mathbf{a}, \mathbf{b}, \mathbf{c} \in T(z)$ jsou formální mocninné řady s posloupnostmi koeficientů $\{a_0, a_1, ...\}$, $\{b_0, b_1, ...\}$ a $\{c_0, c_1, ...\}$. Nechť $\{d_0, d_1, ...\}$ je posloupnost koeficientů řady $\mathbf{ab}$ a $\{e_0, e_1, ...\}$ je posloupnost koeficientů řady $(\mathbf{ab})\mathbf{c}$. Pak pro libovolné $k \in \mathbb{N}$ platí $e_k = \sum_{i+j=k} d_i c_j = \sum_{i+j=k} (\sum_{m+n=i} a_m b_n) c_j = \sum_{m+n+j=k} a_m b_n c_j$ (poslední rovnost plyne ze zobecněného distributivního zákona 1.2(5)). Stejný výsledek zřejmě dostaneme, jestliže $\{e_0, e_1, ...\}$ bude posloupnost koeficientů řady $\mathbf{a}(\mathbf{bc})$. Tedy násobení v $T(z)$ je asociativní. Podobně jako asociativita násobení v $T(z)$ se dokáže platnost distributivního zákona v $T(z)$. Tedy je $T(z)$ komutativní okruh. Buďte nyní $\mathbf{a}, \mathbf{b} \in T(z)$ nenulové prvky, $\mathbf{a} = a_0 + a_1 z + a_2 z^2 + ...$, $\mathbf{b} = b_0 + b_1 z + b_2 z^2 + ...$ Nechť k je řád řady $\mathbf{a}$ a l je řád řady $\mathbf{b}$. Pak $a_k \neq 0 \neq b_l$. Jestliže $\mathbf{c} = \mathbf{ab} = c_0 + c_1 z + c_2^{-2} + ...$, pak $c_{k+l} = a_k b_l \neq 0$ (jelikož T je obor integrity). Tedy $\mathbf{c}$ není nulovým prvkem okruhu $T(z)$, takže $T(z)$ nemá dělitele nuly. Proto je $T(z)$ obor integrity.

2.3. Tvrzení. *Jednotky v $T(z)$ jsou právě řady nulového řádu.*

Důkaz. Nechť $\mathbf{a} \in T(z)$, $\mathbf{a} = a_0 + a_1 z + a_2 z^2 + ...$, a předpokládejme, že $\mathbf{a}$ je jednotkou oboru integrity $T(z)$. Pak existuje $\mathbf{b} \in T(z)$, $\mathbf{b} = b_0 + b_1 z + b_2 z^2 + ...$, tak, že $\mathbf{ab}$ má posloupnost koeficientů $\{1, 0, 0, ...\}$. Tedy $a_0 b_0 = 1$, a proto $a_0 \neq 0$. Takže $\mathcal{O}\mathbf{a} = 0$.
Naopak, předpokládejme, že $\mathcal{O}\mathbf{a} = 0$. Pak $a_0 \neq 0$, tedy následující (nekonečná) soustava lineárních rovnic s neznámými $b_0, b_1, b_2, ...$ má jediné řešení:

$$a_0 b_0 = 1$$

$$a_1 b_0 + a_0 b_1 = 0$$

$$a_2 b_0 + a_1 b_1 + a_0 b_2 = 0$$

.....

$$a_0b_n + a_1b_{n-1} + ... + a_nb_0 = 0$$

.....

Po vyčíslení těchto neznámých má ovšem řada $\mathbf{b} = b_0 + b_1z + b_2z^2 + ...$ tu vlastnost, že posloupnost koeficientů řady $\mathbf{ab}$ je $\{1, 0, 0, ...\}$, takže je inverzním prvkem k $\mathbf{a}$ v $T(z)$. Proto je $\mathbf{a}$ jednotkou v $T(z)$.

2.4. Důsledek. *V $T(z)$ jsou asociovanými prvky právě řady stejného řádu.*

Důkaz. Buďte $\mathbf{a}, \mathbf{b} \in T(z)$, $\mathbf{a} = a_0 + a_1z + a_2z^2 + ...$, a nechť $\mathcal{O}\mathbf{b} = n$. Jestliže $\mathbf{a}$ a $\mathbf{b}$ jsou asociované, pak existuje jednotka $\mathbf{c}$ v $T(z)$ tak, že $\mathbf{a} = \mathbf{bc}$. Podle 2.3 platí $\mathcal{O}\mathbf{c} = 0$, tedy z definice násobení řad ihned vyplývá, že $\mathcal{O}\mathbf{a} = n$.
Naopak, nechť $\mathcal{O}\mathbf{a} = n$. Pak následující (nekonečná) soustava lineárních rovnic s neznámými $c_0, c_1, ...$ má (jediné) řešení:

$$a_n = b_nc_0$$

$$a_{n+1} = b_{n+1}c_0 + b_nc_1$$

$$a_{n+2} = b_{n+2}c_0 + b_{n+1}c_1 + b_nc_2$$

.....

$$a_{n+m} = b_{n+m}c_0 + b_{n+m-1}c_1 + ... + b_nc_m$$

.....

Po vyčíslení těchto neznámých má zřejmě řada $\mathbf{c} = c_0 + c_1z + c_2z^2 + ...$ vlastnost $\mathbf{a} = \mathbf{bc}$. Protože $c_0 \neq 0$, je podle 2.3 řada $\mathbf{c}$ jednotkou v $T(z)$. Takže $\mathbf{a}$ a $\mathbf{b}$ jsou asociované.

2.5. Důsledek. *Ireducibilní prvky v $T(z)$ jsou právě řady prvního řádu.*

Důkaz. Buď $\mathbf{a} \in T(z)$, $\mathbf{a} = a_0 + a_1z + a_2z^2 + ...$, a nechť $\mathcal{O}\mathbf{a} = n$. Předpokládejme, že $\mathbf{a}$ je ireducibilní prvek v $T(z)$ a připusťme, že $n \neq 1$. Protože $\mathbf{a}$ není jednotkou v $T(z)$, podle 2.3 platí $n > 1$. Položme $\mathbf{b} = z$ a $\mathbf{c} = a_nz^{(n-1)} + a_{n+1}z^n + ...$ Pak $\mathbf{a} = \mathbf{bc}$, takže $\mathbf{b}|\mathbf{a}$. Protože $\mathcal{O}\mathbf{b} = 1$, podle 2.3 $\mathbf{b}$ není jednotkou v $T(z)$ a podle 2.4 $\mathbf{b}$ není ani asociovaná s $\mathbf{a}$. To je ovšem spor s předpokladem, že $\mathbf{a}$ je ireducibilní. Proto $n = 1$.
Předpokládejme naopak, že $n = 1$. Nechť $\mathbf{b} \in T(z)$, $\mathbf{b} = b_0 + b_1z + b_2z^2 + ...$, je libovolná řada s vlastností $\mathbf{b}|\mathbf{a}$. Pak existuje řada $\mathbf{c} = c_0 + c_1z + c_2z^2 + ...$ tak, že $\mathbf{a} = \mathbf{bc}$. Je-li $b_0 \neq 0$, pak je $\mathbf{b}$ podle 2.3 jednotkou v $T(z)$. Předpokládejme tedy, že $b_0 = 0$. Protože $b_0c_1 + b_1c_0 = a_1 \neq 0$, musí platit $b_1 \neq 0$. Pak ovšem $\mathcal{O}\mathbf{b} = 1$, takže podle 2.4 jsou $\mathbf{a}$ a $\mathbf{b}$ asociované. Proto je $\mathbf{a}$ ireducibilní prvek v $T(z)$.

2.6. Definice. Buď T těleso a $\{a_0, a_1, a_2, ...\}$ posloupnost prvků tělesa T. Tato posloupnost se nazývá *rekurentní*, jestliže existují čísla $r, s \in \mathbb{N}$, $r \neq 0$ a prvky $c_0, c_1, ..., c_{r-1} \in T$ tak, že pro každé $j = s, s + 1, ...$ platí

$$a_{j+r} = c_0a_j + c_1a_{j+1} + ... + c_{r-1}a_{j+r-1}.$$

Jinými slovy, posloupnost $\{a_0, a_1, ...\}$ je rekurentní, jestliže existují čísla $n_0, r \in \mathbb{N}$, $r > 0$ a $n_0 \geq r - 1$ tak, že pro každé $n > n_0$ ($n \in \mathbb{N}$) je prvek a_n roven jisté lineární kombinaci (dané neměnnými koeficienty) předcházejících r členů této posloupnosti.

2.7. Definice. Formální mocninná řada se nazývá *kauzální*, jestliže posloupnost jejích koeficientů je rekurentní.

Množinu všech kauzálních formálních mocninných řad s neurčitou z nad tělesem T označíme symbolem $T\{z\}$.

Důkazy následujících dvou tvrzení jsou poněkud náročnější, proto je neuvádíme:

2.8. Tvrzení. *$T\{z\}$ je podoborem integrity oboru integrity $T(z)$.*

2.9. Tvrzení. *Jednotkami, resp. ireducibilními prvky v $T\{z\}$ jsou právě kauzální formální mocninné řady nulového, resp. prvního řádu. Asociovanými prvky v $T\{z\}$ jsou právě kauzální formální mocninné řady stejného řádu.*

2.10. Příklad. Nechť $\mathbf{a} = a_0 + a_1 z + a_2 z^2 + ...$ je řada s posloupností koeficientů $\{0, 1, 2, 3, 1, 5, -3, 13, -19, 45, -83, 173, ...\}$. Pak $\mathbf{a} \in \mathbb{R}\{z\}$, neboť platí $a_{j+2} = 2a_j - a_{j+1}$ pro všechna $j = 2, 3, ...$

2.11. Definice. Buď T těleso, v němž je definována hodnota H. Kauzální formální mocninná řada $a_0 + a_1 z + a_2 z^2 + ...$ nad T se nazývá *stabilní* formální mocninná řada (vzhledem k H), jestliže posloupnost jejích koeficientů konverguje k nule vzhledem k H.

Množinu všech stabilních (vzhledem k H) formálních mocninných řad nad tělesem T s hodnotou H označíme symbolem $T^+\{z\}$.

Také následující tvrzení uvádíme bez důkazu:

2.12. Tvrzení. *$T^+\{z\}$ je podoborem integrity oboru integrity $T\{z\}$.*

2.13. Příklad. Nechť $\mathbf{a} = z + \frac{1}{2}z^2 + \frac{1}{4}z^3 + ...$ Pak $\mathbf{a} \in \mathbb{R}^+\{z\}$ vzhledem k hodnotě dané absolutní hodnotou, ale $\mathbf{a} \notin \mathbb{R}^+\{z\}$ vzhledem k triviální hodnotě.

3. Polynomy

I nadále označujeme symbolem T libovolné pevně dané (komutativní) těleso.

3.1. Definice. Formální mocninná řada $\mathbf{a} = a_0 + a_1 z + a_2 z^2 + ...$ nad tělesem T, jejíž posloupnost koeficientů má pouze konečný počet členů různých od nuly, se nazývá *polynom s neurčitou z nad tělesem T*. Největší číslo $n \in \mathbb{N}$ s vlastností $a_n \neq 0$ se nazývá *stupeň* polynomu $\mathbf{a}$ a značí se symbolem $\mathfrak{d}\mathbf{a}$. Polynom, jehož všechny koeficienty jsou rovny nule, se nazývá nulový a ztotožňuje se s 0 (tj. nulovým prvkem tělesa T). Pro nulový polynom klademe $\mathfrak{d}0 = -\infty$. Podobně libovolný polynom nulového stupně $\mathbf{a} = a_0$ se ztotožňuje s prvkem $a_0 \in T$.

Množinu všech polynomů s neurčitou z nad tělesem T označujeme symbolem $T[z]$.

3.2. Poznámka. *a) Polynomy zapisujeme ve tvaru*

$$\mathbf{a} = a_0 + a_1 z + ... + a_n z^n,$$

kde $n = \mathfrak{d}\mathbf{a}$ (pokud $\mathbf{a} \neq 0$).

b) Zřejmě každý polynom je stabilní formální mocninnou řadou pro libovolnou hodnotu v tělese T, tj. platí inkluze $T[z] \subseteq T^+\{z\}$ (přičemž rovnost nastane pouze pro triviální hodnotu v T).

3.3. Tvrzení. *$T[z]$ je podoborem integrity oboru integrity $T(z)$.*

Důkaz. Zřejmě nulový i jednotkový prvek oboru integrity $T(z)$ jsou polynomy. Dále je také zřejmé, že opačný prvek k polynomu je polynom a že součet i součin dvou polynomů jsou opět polynomy. Odtud plyne tvrzení.

3.4. Poznámka. a) Podle 2.8, 2.12, 3.2b) a 3.3 je tedy $T[z]$ podoborem integrity oboru integrity $T^+\{z\}$.

b) Jsou-li $\mathbf{a}$, $\mathbf{b}$ polynomy, pak zřejmě platí $\mathfrak{d}(\mathbf{a}+\mathbf{b}) \leq \max\{\mathfrak{d}\mathbf{a}, \mathfrak{d}\mathbf{b}\}$ a $\mathfrak{d}(\mathbf{ab}) = \mathfrak{d}\mathbf{a} + \mathfrak{d}\mathbf{b}$.

3.5. Tvrzení. *Jednotky v $T[z]$ jsou právě polynomy nulového stupně.*

Důkaz. Nechť $\mathbf{a} = a_0$ je polynom nulového stupně. Pak $\mathcal{O}\mathbf{a} = 0$, tedy $\mathbf{a}$ je jednotka v $T[z]$ podle 2.3 a 3.3 (zřejmě $\mathbf{a}^{-1} = a_0^{-1}$).
Naopak, nechť polynom $\mathbf{a}$ je jednotka v $T[z]$. Pak $\mathbf{a}$ je nenulový polynom, tedy $\mathfrak{d}\mathbf{a} \geq 0$. Připusťme, že $\mathfrak{d}\mathbf{a} > 0$. Protože $\mathfrak{d}\mathbf{a}^{-1} \geq 0$ (jelikož $\mathbf{a}^{-1}$ je nenulový polynom), dostáváme $\mathfrak{d}(\mathbf{a}\mathbf{a}^{-1}) = \mathfrak{d}\mathbf{a} + \mathfrak{d}\mathbf{a}^{-1} > 0$. To je ale spor, neboť $\mathbf{a}\mathbf{a}^{-1} = 1$ je polynom nulového stupně. Proto $\mathfrak{d}\mathbf{a} = 0$.

3.6. Důsledek. *Polynomy $\mathbf{a}, \mathbf{b} \in T[z]$ jsou asociované, právě když existuje polynom $\mathbf{c}$ nulového stupně takový, že platí $\mathbf{a} = \mathbf{bc}$.*

3.7. Tvrzení. *Buďte $\mathbf{a}, \mathbf{b} \in T[z]$, $\mathbf{b} \neq 0$. Pak existují jednoznačně určené polynomy $\mathbf{g}, \mathbf{h} \in T[z]$ takové, že platí*

$$\mathbf{a} = \mathbf{bg} + \mathbf{h},$$

$$\mathfrak{d}\mathbf{h} < \mathfrak{d}\mathbf{b}.$$

Důkaz. Nejprve dokážeme existenci polynomů $\mathbf{g}, \mathbf{h} \in T[z]$ splňujících tvrzení. Je-li $\mathfrak{d}\mathbf{a} < \mathfrak{d}\mathbf{b}$, pak $\mathbf{a} = \mathbf{b}0 + \mathbf{a}$, takže $\mathbf{g} = 0$ a $\mathbf{h} = \mathbf{a}$ jsou hledané polynomy. Předpokládejme nyní, že $\mathfrak{d}\mathbf{b} \leq \mathfrak{d}\mathbf{a}$, a užijme matematickou indukci vzhledem ke stupni polynomu $\mathbf{a}$. Nechť tedy $\mathbf{a} = a_0 + a_1 z + ... + a_n z^n$ a $\mathbf{b} = b_0 + b_1 z + ... + b_m z^m$, tj. $\mathfrak{d}\mathbf{a} = n$ a $\mathfrak{d}\mathbf{b} = m$. Jestliže $n = 0$, pak také $m = 0$, a proto $\mathbf{a} = a_0 \neq 0 \neq b_0 = \mathbf{b}$. Položíme-li $\mathbf{g} = a_0 b_0^{-1}$ a $\mathbf{h} = 0$, pak zřejmě $\mathbf{a} = \mathbf{bg} + \mathbf{h}$ a $-\infty = \mathfrak{d}\mathbf{h} < \mathfrak{d}\mathbf{b} = 0$, tedy pro polynomy $\mathbf{g}$ a $\mathbf{h}$ tvrzení platí. Buď $n > 0$ libovolné přirozené číslo a předpokládejme, že tvrzení platí, pokud místo $\mathbf{a}$ vezmeme libovolný polynom z $T[z]$ stupně menšího než n. Jelikož stupeň polynomu $\mathbf{a}_1 = \mathbf{a} - a_n b_m^{-1} z^{(n-m)}\mathbf{b}$ je menší než n, existují polynomy $\mathbf{g}_1$,$\mathbf{h} \in T[z]$ s vlastností

$$\mathbf{a}_1 = \mathbf{bg}_1 + \mathbf{h},$$

$$\mathfrak{d}\mathbf{h} < \mathfrak{d}\mathbf{b}.$$

Odtud po úpravě dostaneme

$$\mathbf{a} = \mathbf{bg} + \mathbf{h},$$

kde $\mathbf{g} = \mathbf{g}_1 + a_n b_m^{-1} z^{(n-m)}$. Takže pro polynom $\mathbf{a}$ stupně n splňují $\mathbf{g}$ a $\mathbf{h}$ tvrzení. Tím je dokázána existence polynomů $\mathbf{g}, \mathbf{h}$ splňujících tvrzení pro libovolný polynom $\mathbf{a}$. Zbývá dokázat jejich jednoznačnost. Nechť tedy

$$\mathbf{a} = \mathbf{bg} + \mathbf{h} = \mathbf{bg}_1 + \mathbf{h}_1,$$

$$\mathfrak{d}\mathbf{h} < \mathfrak{d}\mathbf{b},\ \mathfrak{d}\mathbf{h}_1 < \mathfrak{d}\mathbf{b}.$$

Po úpravě dostáváme

$$\mathbf{b}(\mathbf{g} - \mathbf{g}_1) = \mathbf{h}_1 - \mathbf{h}.$$

Kdybychom připustili, že $\mathbf{g}-\mathbf{g}_1 \neq 0$, pak by platilo $\mathfrak{d}(\mathbf{b}(\mathbf{g}-\mathbf{g}_1)) = \mathfrak{d}\mathbf{b}+\mathfrak{d}(\mathbf{g}-\mathbf{g}_1) \geq \mathfrak{d}\mathbf{b}$. Protože však $\mathfrak{d}(\mathbf{h}_1 - \mathbf{h}) < \mathfrak{d}\mathbf{b}$, dostali bychom spor. Tedy $\mathbf{g} - \mathbf{g}_1 = 0$, takže $\mathbf{g} = \mathbf{g}_1$ a proto také $\mathbf{h} = \mathbf{h}_1$. Tím je jednoznačnost polynomů $\mathbf{g}$, $\mathbf{h}$ ukázána a důkaz je hotov.

3.8. Poznámka. Předchozí tvrzení je známo jako věta o dělení polynomů. Jeho důkaz je konstruktivní, tedy popisuje algoritmus pro toto dělení. Polynomy $\mathbf{g}$ a $\mathbf{h}$ se nazývají *neúplný podíl* a *zbytek* po dělení polynomu $\mathbf{a}$ polynomem $\mathbf{b}$. Jedná se o dobře známý algoritmus, který je analogický algoritmu užívanému pro dělení celých čísel.

3.9. Příklad. Aplikujme algoritmus dělení na polynomy $\mathbf{a} = 1+2z+z^2-4z^3-z^5$, $\mathbf{b} = 2 + z - 3z^2 - z^3 \in \mathbb{Q}[z]$. Máme
$\mathbf{a}_1 = \mathbf{a}-z^2\mathbf{b} = 1+2z+z^2-4z^3-z^5-z^2(2+z-3z^2-z^3) = 1+2z-z^2-5z^3+3z^4$,
$\mathbf{a}_2 = \mathbf{a}_1+3z\mathbf{b} = 1+2z-z^2-5z^3+3z^4+3z(2+z-3z^2-z^3) = 1+8z+2z^2-14z^3$,
$\mathbf{a}_3 = \mathbf{a}_2 - 14\mathbf{b} = 1 + 8z + 2z^2 - 14z^3 - 14(2 + z - 3z^2 - z^3) = -27 - 6z^{-1} + 44z^2$.
Tedy dostáváme

$$\mathbf{g} = 14 - 3z + z^2,\ \mathbf{h} = -27 - 6z + 44z^2.$$

3.10. Tvrzení. *Pro libovolné polynomy $\mathbf{a}, \mathbf{b} \in T[z]$ existuje jejich největší společný dělitel (tj. $(\mathbf{a}, \mathbf{b}) \neq \emptyset$).*

Důkaz. Jestliže $\mathbf{a}|\mathbf{b}$, resp. $\mathbf{b}|\mathbf{a}$, pak zřejmě $\mathbf{a} \in (\mathbf{a}, \mathbf{b})$, resp. $\mathbf{b} \in (\mathbf{a}, \mathbf{b})$. Předpokládejme nyní, že $\mathbf{a} \nmid \mathbf{b}$ a $\mathbf{b} \nmid \mathbf{a}$. Pak $\mathbf{b} \neq 0$, tedy podle 3.7 existují polynomy $\mathbf{g}_1, \mathbf{h}_1 \in T[z]$ tak, že

$$\mathbf{a} = \mathbf{b}\mathbf{g}_1 + \mathbf{h}_1,$$

$$\mathfrak{d}\mathbf{h}_1 < \mathfrak{d}\mathbf{b}.$$

Protože $\mathbf{b} \nmid \mathbf{a}$, platí $\mathbf{h}_1 \neq 0$. Aplikujme nyní znovu 3.7, a to na polynomy $\mathbf{b}$ a $\mathbf{h}_1$. Tedy existují polynomy $\mathbf{g}_2, \mathbf{h}_2 \in T[z]$ tak, že

$$\mathbf{b} = \mathbf{h}_1\mathbf{g}_2 + \mathbf{h}_2,$$

$$\mathfrak{d}\mathbf{h}_2 < \mathfrak{d}\mathbf{h}_1.$$

Jestliže $\mathbf{h}_2 = 0$, pak $\mathbf{h}_1 \in (\mathbf{b}, \mathbf{h}_1)$, takže $\mathbf{h}_1 \in (\mathbf{a}, \mathbf{b})$. Pokud ovšem $\mathbf{h}_2 \neq 0$, aplikujeme 3.7 na polynomy $\mathbf{h}_1$ a $\mathbf{h}_2$. Opakováním tohoto postupu nakonec dostaneme

$$\mathbf{a} = \mathbf{b}\mathbf{g}_1 + \mathbf{h}_1,$$

$$\mathbf{b} = \mathbf{h}_1\mathbf{g}_2 + \mathbf{h}_2,$$

$$\mathbf{h}_1 = \mathbf{h}_2\mathbf{g}_3 + \mathbf{h}_3,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\mathbf{h}_k = \mathbf{h}_{k+1}\mathbf{g}_{k+2} + \mathbf{h}_{k+2},$$

$$\mathbf{h}_{k+1} = \mathbf{h}_{k+2}\mathbf{g}_{k+3},$$

neboť $\mathfrak{d}\mathbf{b} > \mathfrak{d}\mathbf{h}_1 > \mathfrak{d}\mathbf{h}_2 > \ldots > \mathfrak{d}\mathbf{h}_{k+2} \geq 0$, takže po konečném počtu kroků je zbytek nulový. Pak $\mathbf{h}_{k+2} \in (\mathbf{h}_{k+1}, \mathbf{h}_{k+2})$, tedy $\mathbf{h}_{k+2} \in (\mathbf{h}_k, \mathbf{h}_{k+1}), \ldots, \mathbf{h}_{k+2} \in (\mathbf{a}, \mathbf{b})$.

3.11. Poznámka. Také důkaz předchozího tvrzení je konstruktivní, tedy popisuje algoritmus pro nalezení největšího společného dělitele dvou polynomů. Tento algoritmus se nazývá Euklidův a je analogií známého (Euklidova) algoritmu pro hledání největšího společného dělitele celých čísel.

3.12. Příklad. Nalezněme největšího společného dělitele polynomů $\mathbf{a} = 2 - z - 2z^2 + z^3$, $\mathbf{b} = -2z + z^2$. Aplikací algoritmu z důkazu tvrzení 3.10 dostaneme

$$\mathbf{a} = \mathbf{b}z + 2 - z,$$

$$\mathbf{b} = (2 - z)(-z).$$

Tedy polynom $2 - z$ je největším společným dělitelem polynomů $\mathbf{a}$ a $\mathbf{b}$.

3.13. Tvrzení. *Buďte $\mathbf{a}, \mathbf{b} \in T[z]$ polynomy a nechť $\mathbf{d} \in (\mathbf{a}, \mathbf{b})$. Pak existují polynomy $\mathbf{p}, \mathbf{q} \in T[z]$ takové, že platí*

$$\mathbf{d} = \mathbf{ap} + \mathbf{bq}.$$

Je-li navíc $\mathfrak{d}\mathbf{a} \geq 1$ i $\mathfrak{d}\mathbf{b} \geq 1$, lze $\mathbf{p}$ a $\mathbf{q}$ zvolit tak, že $\mathfrak{d}\mathbf{p} < \mathfrak{d}\mathbf{b}$ a $\mathfrak{d}\mathbf{q} < \mathfrak{d}\mathbf{a}$.

Důkaz. Předpokládejme nejprve, že $\mathbf{a}|\mathbf{b}$. Pak $\mathbf{a} \in (\mathbf{a}, \mathbf{b})$, tedy podle 3.6 existuje $c \in T$, $c \neq 0$ tak, že platí $\mathbf{d} = \mathbf{a}c + \mathbf{b}0$. V tomto případě tedy tvrzení platí a podobně platí také v případě $\mathbf{b}|\mathbf{a}$. Předpokládejme nyní, že $\mathbf{a} \nmid \mathbf{b}$ a $\mathbf{b} \nmid \mathbf{a}$. Pak $\mathfrak{d}\mathbf{a} \geq 1$ i $\mathfrak{d}\mathbf{b} \geq 1$ a Euklidovým algoritmem (viz důkaz tvrzení 3.10) nalezneme největšího společného dělitele $\mathbf{h}_{k+2}$ polynomů $\mathbf{a}$ a $\mathbf{b}$. Tedy podle 3.6 existuje $c \in T$, $c \neq 0$ tak, že $\mathbf{d} = c\mathbf{h}_{k+2}$. Z předposlední rovnosti schématu z důkazu tvrzení 3.10 dostáváme

$$\mathbf{d} = c\mathbf{h}_k - c\mathbf{h}_{k+1}\mathbf{g}_{k+2}.$$

Postupujeme-li nyní ve schématu od předposlední rovnosti směrem vzhůru, z následující rovnosti dostáváme

$$\mathbf{h}_{k+1} = \mathbf{h}_{k-1} - \mathbf{h}_k\mathbf{g}_{k+1}.$$

Tuto rovnost využijeme pro dosazení za $\mathbf{h}_{k+1}$ do výše uvedeného vztahu pro $\mathbf{d}$ a dostaneme
$\mathbf{d} = c\mathbf{h}_k - c\mathbf{h}_{k-1}\mathbf{g}_{k+2} + c\mathbf{h}_k\mathbf{g}_{k+1}\mathbf{g}_{k+2} = c\mathbf{h}_k(1 + \mathbf{g}_{k+1}\mathbf{g}_{k+2}) - c\mathbf{h}_{k-1}\mathbf{g}_{k+2}$.
Opakováním tohoto postupu v předposledním kroku dostaneme $\mathbf{d} = \mathbf{bu} + \mathbf{h}_1\mathbf{v}$ pro nějaké $\mathbf{u}, \mathbf{v} \in T[z]$. Užitím první rovnosti schématu z důkazu tvrzení 3.10 pak máme

$$\mathbf{d} = \mathbf{bu} + \mathbf{av} - \mathbf{bg}_1\mathbf{v} = \mathbf{av} + \mathbf{b}(\mathbf{u} - \mathbf{g}_1\mathbf{v}) = \mathbf{at} + \mathbf{bw},$$

kde $\mathbf{t} = \mathbf{v}$, $\mathbf{w} = \mathbf{u} - \mathbf{g}_1\mathbf{v}$. Podle tvrzení 3.7 existují polynomy $\mathbf{r}, \mathbf{s}, \mathbf{p}, \mathbf{q} \in T[z]$ tak, že platí $\mathbf{t} = \mathbf{br} + \mathbf{p}$ a $\mathbf{w} = \mathbf{as} + \mathbf{q}$, přičemž $\mathfrak{d}\mathbf{p} < \mathfrak{d}\mathbf{b}$ a $\mathfrak{d}\mathbf{q} < \mathfrak{d}\mathbf{a}$. Po dosazení a upravě dostaneme

$$\mathbf{d} = \mathbf{abr} + \mathbf{bas} + \mathbf{ap} + \mathbf{bq}.$$

Připusťme nyní, že $\mathbf{ab}(\mathbf{r} + \mathbf{s}) \neq 0$. Pak $\mathfrak{d}(\mathbf{ab}(\mathbf{r} + \mathbf{s})) \geq \mathfrak{d}\mathbf{a} + \mathfrak{d}\mathbf{b}$. Ale

$$\mathbf{ab}(\mathbf{r} + \mathbf{s}) = \mathbf{d} - \mathbf{ap} - \mathbf{bq},$$

takže $\mathfrak{d}(\mathbf{ab}(\mathbf{r} + \mathbf{s})) \leq \max\{\mathfrak{d}\mathbf{d}, \mathfrak{d}\mathbf{a} + \mathfrak{d}\mathbf{p}, \mathfrak{d}\mathbf{b} + \mathfrak{d}\mathbf{q}\} < \mathfrak{d}\mathbf{a} + \mathfrak{d}\mathbf{b}$, neboť $\mathfrak{d}\mathbf{d} < \mathfrak{d}\mathbf{a} + \mathfrak{d}\mathbf{b}$, $\mathfrak{d}\mathbf{a} + \mathfrak{d}\mathbf{p} < \mathfrak{d}\mathbf{a} + \mathfrak{d}\mathbf{b}$ a $\mathfrak{d}\mathbf{b} + \mathfrak{d}\mathbf{q} < \mathfrak{d}\mathbf{a} + \mathfrak{d}\mathbf{b}$. To je ale spor, takže $\mathbf{ab}(\mathbf{r} + \mathbf{s}) = 0$. Proto $\mathbf{d} = \mathbf{ap} + \mathbf{bq}$ a důkaz je hotov.

3.14. Příklad. Nechť $\mathbf{a} = 2 - z - 2z^2 + z^3$, $\mathbf{b} = -2z + z^2$. Z příkladu 3.12 víme, že polynom $\mathbf{d} = 2 - z$ je největší společný dělitel polynomů $\mathbf{a}$, $\mathbf{b}$. Z algoritmu popsaného v důkazu tvrzení 3.13 (který je založen na Euklidovu algoritmu užitém k řešení příkladu 3.12) je zřejmé, že polynomy $\mathbf{p} = 1$ a $\mathbf{q} = -z$ mají vlastnost

$$\mathbf{d} = \mathbf{ap} + \mathbf{bq},$$

$$\partial\mathbf{p} < \partial\mathbf{b},\ \partial\mathbf{q} < \partial\mathbf{a}.$$

3.15. Poznámka. Jestliže $\mathbf{a}, \mathbf{b} \in T[z]$ jsou polynomy a $\mathbf{d} \in (\mathbf{a}, \mathbf{b})$, pak podle 3.13 existují polynomy $\mathbf{p}, \mathbf{q} \in T[z]$ s vlastností

$$\mathbf{ap} + \mathbf{bq} = \mathbf{d}.$$

Zřejmě platí

$$\mathbf{ab} + \mathbf{b}(-\mathbf{a}) = 0.$$

Protože $\mathbf{d} \in (\mathbf{a}, \mathbf{b})$, existují polynomy $\mathbf{r}, \mathbf{s} \in T[z]$ takové, že

$$\mathbf{b} = \mathbf{dr},\ -\mathbf{a} = \mathbf{ds}.$$

Odtud $\mathbf{adr} + \mathbf{bds} = 0$, tedy $\mathbf{ar} + \mathbf{bs} = 0$. Vztahy

$$\mathbf{ap} + \mathbf{bq} = \mathbf{d},$$

$$\mathbf{ar} + \mathbf{bs} = 0$$

lze zapsat stručněji v maticovém tvaru

$$\begin{bmatrix} \mathbf{p} & \mathbf{q} \\ \mathbf{r} & \mathbf{s} \end{bmatrix} \begin{bmatrix} \mathbf{a} \\ \mathbf{b} \end{bmatrix} = \begin{bmatrix} \mathbf{d} \\ 0 \end{bmatrix}.$$

Jedná se ovšem o matice, jejichž prvky jsou polynomy. O takových maticích bude podrobněji pojednáno v následující kapitole.

3.16. Definice. Polynom $\mathbf{a} \in T[z]$ se nazývá *kauzální*, jestliže je jednotkou oboru integrity $T\{z\}$.

3.17. Poznámka. Protože $T[z] \subseteq T\{z\}$, je každý polynom kauzální formální mocninnou řadou, nemusí však být kauzálním polynomem.

Jako důsledek tvrzení 2.9 dostáváme:

3.18. Tvrzení. *Polynom $\mathbf{a} \in T[z]$ je kauzální, právě když je nulového řádu.*

3.19. Definice. Polynom $\mathbf{a} \in T[z]$ se nazývá *stabilní* vzhledem k dané hodnotě v T, jestliže je jednotkou oboru integrity $T^+\{z\}$.

3.20. Poznámka. Platí analogie Poznámky 3.17: Zatímco každý polynom je stabilní formální mocninou řadou, nemusí být stabilním polynomem. Každý stabilní polynom je ovšem kauzálním polynomem.

3.21. Tvrzení. *(1) Nulový polynom není stabilní vzhledem k žádné hodnotě v T.*

(2) Jednotky v $T[z]$ (tj. polynomy nulového stupně) jsou stabilními polynomy vzhledem k libovolné hodnotě v T.

(3) Jsou-li $\mathbf{a}, \mathbf{b} \in T[z]$ stabilní polynomy vzhledem k hodnotě H v T, pak také $\mathbf{ab}$ je stabilní polynom vzhledem k H.

Důkaz. (1) Zřejmě $0\mathbf{a} = 0$ pro libovolný prvek $\mathbf{a} \in T[z]$.

(2) Je-li $\mathbf{a} \in T[z]$ jednotka, pak $\mathbf{a} = a_0 \neq 0$. Pro $b = \frac{1}{a_0} \in T[z] \subseteq T^+\{z\}$ je $\mathbf{ab} = 1$, tedy $\mathbf{a}$ je jednotka v $T^+\{z\}$.

(3) Nechť $\mathbf{a}, \mathbf{b} \in T[z]$ jsou stabilní polynomy. Pak $\mathbf{a}, \mathbf{b}$ jsou jednotky v $T^+\{z\}$, existují tedy prvky $\mathbf{c}, \mathbf{d} \in T^+\{z\}$ tak, že $\mathbf{ac} = 1$ a $\mathbf{bd} = 1$. Odtud $(\mathbf{ab})(\mathbf{cd}) = (\mathbf{ab})(\mathbf{dc}) = \mathbf{a}(\mathbf{bd})\mathbf{c} = \mathbf{ac} = 1$, tedy $\mathbf{ab}$ je jednotka v $T^+\{z\}$ neboli stabilní polynom.

3.22. Příklad. Je-li polynom $\mathbf{a} \in T[z]$ stabilní vzhledem k dané hodnotě v T, pak má samozřejmě nulový řád. Neplatí však opačné tvrzení, jak ukazuje následující příklad: Buď $\mathbf{a} = 1 - 2z \in \mathbb{R}[z]$. Pak $\mathbf{a}$ má nulový řád, tedy je jednotkou v $\mathbb{R}\{z\}$. Snadno se ověří, že inverzním prvkem k $\mathbf{a}$ v $\mathbb{R}\{z\}$ je formální mocninná řada $\mathbf{b} = 1 + 2z + 4z^2 + 8z^3 + ...$ Avšak $\mathbf{b} \notin \mathbb{R}^+\{z\}$ vzhledem absolutní hodnotě, tedy $\mathbf{a}$ není stabilní polynom.

Bez důkazu nyní uvedeme kritérium pro určení stability polynomů nad $\mathbb{R}$ vzhledem k absolutní hodnotě.

3.23. Tvrzení. *Nechť $\mathbf{a} = a_0 + a_1 z + ... + a_n z^n \in \mathbb{R}[z]$ je polynom stupně n. Položme*

$$\lambda_0 = -\frac{a_n}{a_0},$$

$a_{10} = a_0 - \frac{a_n^2}{a_0}$, $a_{11} = a_1 - \frac{a_{n-1}a_n}{a_0}$,..., $a_{1,n-1} = a_{n-1} - \frac{a_1 a_n}{a_0}$,

$a_{i+1,0} = a_{i0} - \frac{a_{i,n-i}^2}{a_{i0}}$, $a_{i+1,1} = a_{i1} - \frac{a_{i,n-i-1}a_{i,n-i}}{a_{i0}}$,..., $a_{i+1,n-i-1} = a_{i,n-i-1} - \frac{a_{i1}a_{i,n-i}}{a_{i0}}$,

$$\lambda_i = -\frac{a_{i,n-i}}{a_{i0}}$$

pro $i = 1, 2, ..., n-2$ a

$$\lambda_{n-1} = -\frac{a_{n-1,1}}{a_{n-1,0}}.$$

Pak polynom $\mathbf{a}$ je stabilní vzhledem k absolutní hodnotě, právě když $a_0 \neq 0$, $a_{i0} \neq 0$ pro všechna $i = 1, 2, ..., n-1$ a $|\lambda_i| < 1$ pro všechna $i = 0, 1, ..., n-1$.

3.24. Příklad. Užitím kritéria 3.23 zjistěme, zda polynom $\mathbf{a} = 2 - 2z^2 + z^3 - z^4 \in \mathbb{R}[z]$ je stabilní vzhledem k absolutní hodnotě. Máme

$$\lambda_0 = -\frac{a_4}{a_0} = \frac{1}{2},$$

$a_{10} = a_0 - \frac{a_4^2}{a_0} = \frac{3}{2}$, $a_{11} = a_1 - \frac{a_3 a_4}{a_0} = \frac{1}{2}$, $a_{12} = a_2 - \frac{a_2 a_4}{a_0} = -3$, $a_{13} = a_3 - \frac{a_1 a_4}{a_0} = 1$,

$$\lambda_1 = -\frac{a_{13}}{a_{10}} = -\frac{2}{3},$$

$a_{20} = a_{10} - \frac{a_{13}^2}{a_{10}} = \frac{5}{6}$, $a_{21} = a_{11} - \frac{a_{12}a_{13}}{a_{10}} = \frac{5}{2}$, $a_{22} = a_{12} - \frac{a_{11}a_{13}}{a_{10}} = -\frac{10}{3}$,

$$\lambda_2 = -\frac{a_{22}}{a_{20}} = 4.$$

Dále již není třeba pokračovat, neboť $|\lambda_2| \geq 1$. Polynom $\mathbf{a}$ tedy není stabilní vzhledem k absolutní hodnotě.

3.25. Definice. *Polynomiálním zlomkem* nad tělesem T rozumíme výraz

$$\frac{\mathbf{a}_2}{\mathbf{a}_1},$$

kde $\mathbf{a}_1, \mathbf{a}_2 \in T[z]$, $\mathbf{a}_1 \neq 0$.
Dva polynomiální zlomky $\frac{\mathbf{a}_2}{\mathbf{a}_1}$, $\frac{\mathbf{b}_2}{\mathbf{b}_1}$ považujeme za sobě rovné, právě když $\mathbf{a}_1\mathbf{b}_2 = \mathbf{a}_2\mathbf{b}_1$. Součet a součin polynomiálních zlomků definujeme takto:

$$\frac{\mathbf{a}_2}{\mathbf{a}_1} + \frac{\mathbf{b}_2}{\mathbf{b}_1} = \frac{\mathbf{a}_1\mathbf{b}_2 + \mathbf{a}_2\mathbf{b}_1}{\mathbf{a}_1\mathbf{b}_1},$$

$$\frac{\mathbf{a}_2}{\mathbf{a}_1}\frac{\mathbf{b}_2}{\mathbf{b}_1} = \frac{\mathbf{a}_2\mathbf{b}_2}{\mathbf{a}_1\mathbf{b}_1}.$$

Množinu všech tříd sobě rovných polynomiálních zlomků nad tělesen T označíme symbolem $T(z)'$. Množinu všech tříd polynomiálních zlomků, které obsahují zlomky tvaru $\frac{\mathbf{a}_2}{\mathbf{a}_1}$, kde $\mathcal{O}(\mathbf{a}_1) = 0$, označíme symbolem $T\{z\}'$.

Následující tvrzení je zřejmé:

3.26. Tvrzení. *Množina $T(z)'$ s výše definovanými operacemi sčítání a násobení tvoří těleso. Nulovým, resp. jednotkovým prvkem tohoto tělesa je třída polynomiálních zlomků tvaru $\frac{0}{\mathbf{a}_1}$, kde $\mathbf{a}_1 \neq 0$, resp. tvaru $\frac{\mathbf{a}_1}{\mathbf{a}_1}$, kde $\mathbf{a}_1 \neq 0$. Opačným prvkem ke třídě obsahující polynomiální zlomek $\frac{\mathbf{a}_2}{\mathbf{a}_1}$, $\mathbf{a}_1 \neq 0$, je třída obsahující polynomiální zlomek $\frac{-\mathbf{a}_2}{\mathbf{a}_1}$. Inverzním prvkem ke třídě obsahující polynomiální zlomek $\frac{\mathbf{a}_2}{\mathbf{a}_1}$, $\mathbf{a}_1 \neq 0 \neq \mathbf{a}_2$, je třída obsahující polynomiální zlomek $\frac{\mathbf{a}_1}{\mathbf{a}_2}$.*

3.27. Tvrzení. *Množina $T\{z\}'$ s výše definovanými operacemi sčítání a násobení je obor integrity, který je izomorfní s oborem integrity $T\{z\}$.*

Důkaz. $T\{z\}'$ je zřejmě podokruhem tělesa $T(z)'$, tedy je oborem integrity. Buď $\frac{\mathbf{a}_2}{\mathbf{a}_1}$ libovolný polynomiální zlomek, kde $\mathcal{O}(\mathbf{a}_1) = 0$. Nechť $\mathbf{a}_1 = a_0 + a_1 z + ... + a_n z^n$, $\mathbf{a}_2 = b_0 + b_1 z + ... + b_m z^m$. Ke třídě polynomiálních zlomků, která obsahuje zlomek $\frac{\mathbf{a}_2}{\mathbf{a}_1}$ přiřaďme formální mocninou řadu $d_0 + d_1 z + d_2 z^2 + ...$ definovanou následovně:

$$d_0 = \frac{b_0}{a_0},$$

$$d_i = \frac{b_i - \sum_{j=1}^{\min\{n,i\}} a_j d_{i-j}}{a_0} \text{ pro } 1 \leq i \leq m,$$

$$d_i = -\frac{\sum_{j=1}^{\min\{n,i\}} a_j d_{i-j}}{a_0} \text{ pro } i > m.$$

Tato formální mocninná řada je zřejmě kauzální, neboť označíme-li

$$c_k = -\frac{a_{n-k}}{a_0} \text{ pro } k = 0, 1, ..., n-1,$$

pak platí

$$d_i = c_0 d_{i-n} + c_1 d_{i-n+1} + ... + c_{n-1} d_{i-1} \text{ pro } i \geq n,\ i > m.$$

Lze snadno ověřit, že výše uvedené přiřazení definuje bijekci oboru integrity $T\{z\}'$ na $T\{z\}$ zachovávající sčítání i násobení, takže jsou oba obory integrity izomorfní. Inverzní zobrazení k této bijekci přiřazuje libovolné kauzální formální mocninné řadě

$$d_0 + d_1 z + d_2 z^2 + ...$$

třídu polynomiálních zlomků obsahující zlomek $\frac{\mathbf{a}_2}{\mathbf{a}_1}$, který je dán následovně:

Nechť $d_{j+r} = c_0 d_j + c_1 d_{j+1} + ... + c_{r-1} d_{j+r-1}$ pro každé $j = s, s+1, ...$. Pak položíme

$\mathbf{a}_1 = 1 - c_{r-1} z - ... - c_0 z^r$,

$\mathbf{a}_2 = d_0 + (d_1 - c_{r-1} d_0) z + (d_2 - c_{r-1} d_1 - c_{r-2} d_0) z^2 + ... + (d_r - c_{r-1} d_{r-1} - ... - c_0 d_0) z^r + (d_{r+1} - c_{r-1} d_r - ... - c_0 d_1) z^{(r+1)} + ... + (d_{r+s-1} - c_{r-1} d_{r+s-2} - ... - c_0 d_{s-1}) z^{(r+s-1)}$.

3.28. Příklad. Určeme kauzální formální mocninnou řadu $\mathbf{a}$, která je izomorfismem z 3.27 přiřazena polynomiálnímu zlomku $\frac{1+z}{1+z+z^2}$ (takováto řada se často nazývá *rozvojem* daného zlomku). Podle konstrukce z důkazu tvrzení 3.27 máme:

$$d_0 = \frac{b_0}{a_0} = 1,$$

$$d_1 = \frac{b_1 - a_1 d_0}{a_0} = 0,$$

$$d_i = -\frac{\sum_{j=1}^{2} a_j d_{i-j}}{a_0} \text{ pro } i \geq 2,$$

$$\text{tedy } d_2 = -\frac{a_1 d_1 + a_2 d_0}{a_0} = -1,$$

$$d_3 = -\frac{a_1 d_2 + a_2 d_1}{a_0} = 1,$$

$$d_4 = -\frac{a_1 d_3 + a_2 d_2}{a_0} = 0,$$

$$d_5 = -\frac{a_1 d_4 + a_2 d_3}{a_0} = -1,$$

$$d_6 = -\frac{a_1 d_5 + a_2 d_4}{a_0} = 1, \text{ atd.}$$

Takže $\mathbf{a} = 1 - z^2 + z^3 - z^5 + z^6 - z^7 + ...$.

3.29. Příklad. Určeme polynomiální zlomek patřící do třídy, které je při izomorfismu z 3.27 přiřazena kauzální formální mocninná řada $\mathbf{a} = z + 2z^2 + 3z^3 + z^4 + 5z^5 - 3z^6 + 13z^7 - 19z^8 + 45z^9 - 83z^{10} + 173z^{11} - ....$ Zřejmě $d_{j+2} = 2d_j - d_{j+1}$ pro $j = 2, 3, ...$. Podle konstrukce z důkazu tvrzení 3.26 položíme:

$\mathbf{a}_1 = 1 + z - 2z^2$,

$\mathbf{a}_2 = z + (2 - (-1) \cdot 1)z^2 + (3 - (-1) \cdot 2 - 2 \cdot 1)z^3 = z + 3z^2 + 3z^3$.

Tedy

$$\frac{z + 3z^2 + 3z^3}{1 + z - 2z^2}$$

je hledaný polynomiální zlomek.