Oldřich Kowalski

O positivně definitních basích nad obory integrity reálných čísel

Časopis pro pěstování matematiky, Vol. 86 (1961), No. 2, 132--147

Persistent URL: `http://dml.cz/dmlcz/108208`

Časopis pro pěstování matematiky, roč. 86 (1961), Praha

O POSITIVNĚ DEFINITNÍCH BASÍCH NAD OBORY INTEGRITY REÁLNÝCH ČÍSEL

OLDŘICH KOWALSKI, Brno

(Došlo dne 12. května 1958, po úpravě dne 14. dubna 1960)

V této práci se zabývám problémem: Je dán reálný číselný obor integrity $\mathbf{O}$; studují se konečné množiny kladných čísel $\{\omega_1, \ldots, \omega_k\}$ té vlastnosti, že každý kladný prvek β rozšířeného oboru integrity $\mathbf{O}[\omega_1, \ldots, \omega_k]$ lze vyjádřit ve tvaru

$$\beta = \sum_{i_1, \ldots, i_k = 0}^{s} h_{i_1}, \ldots, {}_{i_k}\omega_1^{i_1} \ldots, \omega_k^{i_k}$$

kde $h_{i_1}, \ldots, {}_{i_k}$ jsou vesměs nezáporná čísla z oboru $\mathbf{O}$.

1. ZÁKLADNÍ OZNAČENÍ A POJMY

V celé práci značí $\mathbf{T}$ těleso reálných čísel, $\mathbf{O}, \mathbf{O}_1, \ldots$ (resp. $\mathbf{T}_1, \mathbf{T}_2, \ldots$) obory integrity v tělese $\mathbf{T}$ (resp. podtělesa $\mathbf{T}$); $\mathbf{O}^+$ značí množinu kladných čísel v $\mathbf{O}$. Jsou-li $\alpha_1, \ldots, \alpha_k$ reálná čísla, pak $\mathbf{O}[\alpha_1, \ldots, \alpha_k]$ resp. $\mathbf{O}(\alpha_1, \ldots, \alpha_k)$ je nejmenší obor integrity resp. těleso obsahující $\mathbf{O}$ a čísla $\alpha_1, \ldots, \alpha_k$.

Po těchto poznámkách přistoupíme k základní definici.

Definice 1.1. *Množina $\{\omega_1, \omega_2, \ldots, \omega_k\}$ kladných čísel je positivně definitní base nad oborem integrity $\mathbf{O}$, jestliže každé číslo β z množiny $(\mathbf{O}[\omega_1, \omega_2, \ldots, \omega_k])^+$ lze vyjádřit ve tvaru*

$$\beta = \sum_{i_1=0}^{s_1} \sum_{i_2=0}^{s_2} \ldots \sum_{i_k=0}^{s_k} h_{i_1,i_2,\ldots,i_k} \omega_1^{i_1}\omega_2^{i_2} \ldots \omega_k^{i_k} \tag{1}$$

kde $h_{i_1,i_2,\ldots,i_k} \in \mathbf{O}$, $h_{i_1,i_2,\ldots,i_k} \geqq 0$ pro všechny k-tice $i_1, \ldots, i_k$. V případě $k = 1$ mluvíme specielně o positivně definitním prvku (čísle) nad oborem integrity $\mathbf{O}$.

Poznámka 1.1. Nad libovolným oborem integrity $\mathbf{O}$ můžeme sestrojit nekonečně mnoho triviálních positivně definitních basí. Takovou basí je každá množina $\{a_1, a_2, \ldots, a_k\}$ prvků z $\mathbf{O}^+$. V dalších odstavcích poznáme, že existují také netriviální base.

Věta 1.1. *Je-li množina $\{\omega_1, \ldots, \omega_k\}$ positivně definitní base nad oborem integrity $\mathbf{O}$, pak je $\{\omega_1, \ldots, \omega_k\}$ positivně definitní basí nad podílovým tělesem $\mathbf{P_O}$ oboru integrity $\mathbf{O}$.*

Důkaz. Buď $\beta \in (\mathbf{P_O}[\omega_1, \ldots, \omega_k])^+$; pak existuje číslo $s \in \mathbf{O}^+$ takové, že $s\beta \in (\mathbf{O}[\omega_1, \ldots, \omega_k])^+$. Odtud lze $s\beta$ vyjádřit ve tvaru (1) s koeficienty $h_{i_1, i_2, \ldots, i_k}$ z oboru $\mathbf{O}$, tedy β lze vyjádřit rovněž ve tvaru (1) s koeficienty $\frac{1}{s} h_{i_1, i_2, \ldots, i_k} \geqq 0$ z tělesa $\mathbf{P_O}$.

Snadno zjistíme, že každý positivně definitní prvek nad $\mathbf{O}$ je algebraický nad $\mathbf{O}$. O tom mluví

Věta 1.2. *Je-li ω positivně definitním prvkem nad oborem integrity $\mathbf{O}$, pak ω vyhovuje algebraické rovnici nad oborem $\mathbf{O}$ tvaru*

$$a_m x^m + \ldots + a_1 x - a_0 = 0\,, \tag{2}$$

kde

$$a_m > 0,\ a_{m-1} \geqq 0,\ \ldots,\ a_2 \geqq 0,\ a_1 > 0,\ a_0 > 0\,.$$

Důkaz. Zvolme v $\mathbf{O}^+$ číslo $a > \omega$, pak $a - \omega \in (\mathbf{O}[\omega])^+$ a podle předpokladu existuje vyjádření tvaru

$$a - \omega = \sum_{i=0}^{s} h_i \omega^i\,, \quad \text{kde} \quad h_i \in \mathbf{O}\,, \quad h_i \geqq 0 \quad \text{pro} \quad i = 0, 1, \ldots, s \quad \text{a} \quad h_s \neq 0\,.$$

Platí tedy $h_s\omega^s + \ldots + (h_1 + 1)\,\omega - (a - h_0) = 0$. Zřejmě $a - h_0 > 0$. Číslo ω tedy vyhovuje rovnici tvaru (2), cbd.

Další věta podává důležitý příklad positivně definitní base:

Věta 1.3. *Buď dán obor integrity $\mathbf{O}$; nechť $\omega_1, \omega_2, \ldots, \omega_k$ jsou čísla z $\mathbf{T}^+$ té vlastnosti, že*

$$\begin{aligned} &\omega_1 \text{ je positivně definitní nad } \mathbf{O}\,,\\ &\omega_2 \text{ je positivně definitní nad } \mathbf{O}[\omega_1]\,,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &\omega_k \text{ je positivně definitní nad } \mathbf{O}[\omega_1, \ldots, \omega_{k-1}]\,, \end{aligned} \tag{3}$$

pak množina $\{\omega_1, \omega_2, \ldots, \omega_k\}$ je positivně definitní base nad oborem $\mathbf{O}$.

Důkaz. Věta zřejmě platí pro $k = 1$. Předpokládejme tedy platnost věty pro nějaké $k = r$ a dokažme ji odtud i pro $k = r + 1$.

Nechť tedy čísla $\omega_1, \omega_2, \ldots, \omega_{r+1}$ splňují předpoklady (3). Položme $\mathbf{O}_r = \mathbf{O}[\omega_1, \ldots, \omega_r]$. Zřejmě platí vztah

$$\mathbf{O}[\omega_1, \ldots, \omega_r, \omega_{r+1}] = \mathbf{O}_r[\omega_{r+1}]$$

a prvek ω_{r+1} je dále podle předpokladu positivně definitní nad $\mathbf{O}_r$. Odtud plyne, že libovolné $\beta \in (\mathbf{O}[\omega_1, \ldots, \omega_{r+1}])^+$ lze vyjádřit ve tvaru $\beta = \sum_{i=0}^{s} \lambda_i \omega_{r+1}^i$, kde $\lambda_i \in \mathbf{O}_r$, $\lambda_i \geqq 0$ pro $i = 0, 1, \ldots, s$. Podle indukčního předpokladu lze všechny nenulové koeficienty λ_i vyjádřit ve tvaru (1), kde klademe $k = r$, odtud ihned dostáváme vyjádření prvku β ve tvaru (1), ovšem pro $k = r + 1$.

Tím je důkaz úplnou indukcí proveden.

Právě dokázaná věta nás přivádí k této definici:

Definice 1.2. *Positivně definitní base $\{\omega_1, \ldots, \omega_k\}$ nad oborem integrity* $\mathbf{O}$ *se nazývá komposiční nad* $\mathbf{O}$, *jestliže prvky ω_i při vhodném očíslování splňují předpoklady* (3).

Poznámka 1.2. Autoru není známo, zdali nad nějakým oborem $\mathbf{O}$ existují positivně definitní base, které nejsou komposiční nad $\mathbf{O}$. Většina dále odvozených výsledků se týká právě komposičních basí.

Jako protějšek k větě 1.3 uvedeme toto slabší tvrzení:

Věta 1.4. *Buď $\mathfrak{M} = \{\omega_1, \ldots, \omega_k\}$ positivně definitní base nad oborem integrity* $\mathbf{O}$. *Je-li $\mathfrak{N} = \{\omega_{i_1}, \ldots, \omega_{i_s}\}$ libovolná podmnožina množiny $\mathfrak{M}$, pak množina $\mathfrak{M} - \mathfrak{N}$ je positivně definitní base nad oborem integrity $\mathbf{O}[\omega_{i_1}, \ldots, \omega_{i_s}]$.*

Důkaz věty je snadný a přenechávám jej čtenáři.

Z věty 1.2 snadno plyne

Věta 1.5. *Je-li $\{\omega_1, \ldots, \omega_k\}$ komposiční base nad oborem integrity* $\mathbf{O}$, *pak obor $\mathbf{O}[\omega_1, \ldots, \omega_k]$ je konečným algebraickým rozšířením oboru* $\mathbf{O}$.

Podrobnosti důkazu přenechávám čtenáři (viz [1], str. 111–112).

Poznámka 1.3. Autoru není známo, zůstane-li věta 1.5 v platnosti za obecnějšího předpokladu, že množina $\{\omega_1, \ldots, \omega_k\}$ je positivně definitní base nad oborem $\mathbf{O}$.

Zřejmé jsou tyto věty:

Věta 1.6. *Je-li množina $\{\omega_1, \ldots, \omega_k\}$ komposiční base nad oborem* $\mathbf{O}$, *pak je $\{\omega_1, \ldots, \omega_k\}$ komposiční basí i nad tělesem* $\mathbf{P_O}$.

Věta 1.7. *Je-li $\{\omega_1, \ldots, \omega_k\}$ positivně definitní base nad oborem* $\mathbf{O}$ *a $\{\mu_1, \ldots, \mu_s\}$ positivně definitní base nad oborem $\mathbf{O}[\omega_1, \ldots, \omega_k]$, pak je $\{\omega_1, \ldots, \omega_k, \mu_1, \ldots, \mu_s\}$ positivně definitní base nad* $\mathbf{O}$.

2. ZÁKLADNÍ LEMMA

Následující pomocná věta nám umožní konstruovat netriviální komposiční base nad obory integrity:

Lemma 2.1. *Nechť* $\mathbf{O}$ *je obor integrity s jedničkou a nechť číslo $\omega > 0$ vyhovuje rovnici*

$$f(x) = a_m x^m + \ldots + a_2 x^2 + a_1 x - 1 = 0 \tag{4}$$

takové, že

a) $a_i \in \mathbf{O}$ *pro* $i = 1, \ldots, m$,

b) $a_m > 0,\ a_{m-1} \geqq 0, \ldots, a_2 \geqq 0$,

c) *je-li* $\alpha \neq \omega$, $f(\alpha) = 0$, *pak* $|\alpha| > \omega$.

Potom je ω positivně definitní prvek nad oborem integrity $\mathbf{O}$.

Důkaz. Především je vidět z Descartesovy věty, že ω je jediný kladný (a tudíž jednoduchý) kořen rovnice (4). Odtud snadno plyne, že funkce $f(x)$ je rostoucí v čísle ω. Označme $f'(x)$ první derivaci funkce $f(x)$; poněvadž je $f'(\omega) \neq 0$, platí $f'(\omega) > 0$. Máme ukázat, že každé číslo $\lambda \in (\mathbf{O}[\omega])^+$ lze vyjádřit ve tvaru

$$\lambda = \sum_{i=0}^{s} h_i \omega^i , \tag{5}$$

kde $h_i \in \mathbf{O}$, $h_i \geqq 0$ pro $i = 1, \ldots, s$.

A) Předpokládejme nejprve, že $\lambda \in (\mathbf{O}[\omega])^+$ je tvaru

$$\lambda = b_0 + b_1\omega + \ldots + b_{m-1}\omega^{m-1} , \tag{6}$$

kde

$$b_i \in \mathbf{O} \quad \text{pro} \quad i = 0, 1, \ldots, m-1 .$$

Uvažujme posloupnost $\boldsymbol{b}_n = (b_{0,n}, b_{1,n}, \ldots, b_{m-1,n})$ m-členných vektorů, která je definována pro $n = 0, 1, 2, \ldots$ počáteční podmínkou $\boldsymbol{b}_0 = (b_0, b_1, \ldots, b_{m-1})$ a systémem m rekurentních podmínek

$$\begin{aligned} b_{0,n+1} &= a_1 b_{0,n} + b_{1,n} , \\ b_{1,n+1} &= a_2 b_{0,n} + b_{2,n} , \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{m-2,n+1} &= a_{m-1} b_{0,n} + b_{m-1,n} , \\ b_{m-1,n+1} &= a_m b_{0,n} \end{aligned} \tag{7}$$

pro $n = 0, 1, 2, \ldots$ Tuto posloupnost vektorů nazveme posloupností příslušnou k číslu λ. Je zřejmé, že složky všech vektorů $\boldsymbol{b}_n$ leží v oboru $\mathbf{O}$.

Ukážeme nyní, že platí

$$\lambda = b_{0,n}\omega^n + b_{1,n}\omega^{n+1} + \ldots + b_{m-1,n}\omega^{n+m-1} \tag{8}$$

pro $n = 0, 1, 2, \ldots$ Tvrzení je zřejmě správné pro $n = 0$. Předpokládejme tedy, že platí rovnost (8) pro jisté n, dokážeme odtud její platnost i pro hodnotu $n + 1$. Z rovnosti $1 = a_1\omega + \ldots + a_m\omega^m$ plyne

$$b_{0,n}\omega^n = a_1 b_{0,n}\omega^{n+1} + \ldots + a_m b_{0,n}\omega^{n+m} .$$

Dosadíme-li poslední vztah do pravé strany rovnosti (8), dostaneme podle (7)

$$\lambda = b_{0,n+1}\omega^{n+1} + \ldots + b_{m-1,n+1}\omega^{n+m} .$$

Rovnost (8) tedy platí i pro hodnotu $n + 1$ a tím je dokázána pro $n = 0, 1, 2, \ldots$

Položme v systému rovností (7) postupně $n = k, k + 1, \ldots, k + m - 1$, pak vylučováním z těchto m systémů získáme vztahy

$$\begin{aligned} b_{0,k+m} &= a_1 b_{0,k+m-1} + \ldots + a_m b_{0,k} , \\ b_{1,k+m} &= a_2 b_{0,k+m-1} + \ldots + a_m b_{0,k+1} , \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{m-2,k+m} &= a_{m-1} b_{k+m-1} + a_m b_{0,k+m-2} , \\ b_{m-1,k+m} &= a_m b_{k+m-1} . \end{aligned} \tag{9}$$

První ze vztahů (9) je rekurentní podmínka pro posloupnost $\{b_{0,n}\}$ prvních složek vektorů $\boldsymbol{b}_n$. Posloupnost $\{b_{0,n}\}$ tedy vyhovuje diferenční rovnici

$$x_{k+m} - a_1 x_{k+m-1} - \ldots - a_m x_k = 0 . \tag{10}$$

Jak je známo z theorie lineárních diferenčních rovnic s konstantními koeficienty (viz např. [2], str. 296–297), tvoří všechna řešení této diferenční rovnice m-rozměrný vektorový prostor nad tělesem komplexních čísel. Jedna z možných basí tohoto prostoru se určí následovně:

Předně napíšeme tzv. charakteristickou rovnici diferenční rovnice (10)

$$g(x) = x^m - a_1 x^{m-1} - a_2 x^{m-2} - \ldots - a_{m-1} x - a_m = 0 .$$

Nechť $\{\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \ldots, \beta_s\}$ je množina kořenů rovnice $g(x) = 0$, kde $\alpha_1, \ldots, \alpha_r$ jsou jednoduché kořeny a kořen β_i má násobnost $c_i > 1$ pro $i = 1, 2, \ldots, s$. Pak je příslušná base tvořena (lineárně nezávislými) posloupnostmi

$$\begin{array}{ll} 1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{n-1}, \ldots, & (1 \leqq i \leqq r) \\ \left.\begin{array}{l} 1, \beta_j, \beta_j^2, \ldots, \beta_j^{n-1}, \ldots, \\ 0, \beta_j, 2\beta_j^2, \ldots, (n-1)\,\beta_j^{n-1}, \ldots, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0, \beta_j, 2^{c_j-1}\beta_j^2, \ldots, (n-1)^{c_j-1}\,\beta_j^{n-1}, \ldots \end{array}\right\} & (1 \leqq j \leqq s), \end{array}$$

kde ovšem $r + c_1 + c_2 + \ldots + c_s = m$. Existují tedy vhodné koeficienty $d_1, d_2, \ldots, d_m$ takové, že platí

$$\begin{aligned} b_{0,n} = {} & d_1 \alpha_1^{n-1} + \ldots + d_r \alpha_r^{n-1} + d_{r+1} \beta_1^{n-1} + \ldots + \\ & + d_{r+c_1} (n-1)^{c_1-1}\, \beta_1^{n-1} + \ldots + d_m (n-1)^{c_s-1}\, \beta_s^{n-1} . \end{aligned} \tag{11}$$

Uvažme, že platí $g(x) = -x^m f\left(\frac{1}{x}\right)$. Z předpokladů učiněných o rovnici $f(x) = 0$ pak plyne, že rovnice $g(x) = 0$ má jediný kladný kořen $\frac{1}{\omega}$, který je v absolutní hodnotě větší, než kterýkoliv jiný kořen této rovnice. Vzhledem k tomu, že $\frac{1}{\omega}$ je jednoduchý kořen, můžeme položit $\frac{1}{\omega} = \alpha_1$. Dělíme-li obě strany (11) číslem α_1^{n-1}, dostáváme na pravé straně rovnosti součet čísla d_1 a čísel tvaru $C(n-1)^h \mu^{n-1}$, kde μ, h a C jsou konstanty, $|\mu| < 1$. Pro takové konstanty však zřejmě vždy platí $\lim_{n \to \infty} C(n-1)^h \,.\, \mu^{n-1} = 0$. Odtud plyne

$$\lim_{n \to \infty} b_{0,n} \omega^{n-1} = \lim_{n \to \infty} \frac{b_{0,n}}{\alpha_1^{n-1}} = d_1 , \quad \text{tedy} \quad \lim_{n \to \infty} b_{0,n} \omega^n = d_1 \omega .$$

Ze vztahů (9) teď dostaneme

$$\lim_{n\to\infty} b_{0,n}\omega^n = \lim_{k\to\infty} b_{0,k+m}\omega^{k+m} =$$

$$= \lim_{k\to\infty} (a_1\omega b_{0,k+m-1}\omega^{k+m-1} + \ldots + a_m\omega^m b_{0,k}\omega^k) = (a_1\omega + \ldots + a_m\omega^m)\, d_1\omega\,.$$

Podobně

$$\lim_{n\to\infty} b_{1,n}\omega^{n+1} = \lim_{k\to\infty} b_{1,k+m}\omega^{k+m+1} = (a_2\omega^2 + \ldots + a_m\omega^m)\, d_1\omega\,,$$

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

$$\lim_{n\to\infty} b_{m-2,n}\omega^{n+m-2} = \lim_{k\to\infty} b_{m-2,k+m}\omega^{k+2m-2} = (a_{m-1}\omega^{m-1} + a_m\omega^m)\, d_1\,\omega,$$

$$\lim_{n\to\infty} b_{m-1,n}\omega^{n+m-1} = \lim_{k\to\infty} b_{m-1,n}\omega^{k+2m-1} = a_m\omega^m\,.\,d_1\omega\,.$$

Sečtením těchto m vztahů obdržíme

$$\lambda = \lim_{n\to\infty} (b_{0,n}\omega^n + b_{1,n}\omega^{n+1} + \ldots + b_{m-1,n}\omega^{n+m-1}) =$$

$$= (a_1\omega + 2a_2\omega^2 + \ldots + ma_m\omega^m)\, d_1\omega = f'(\omega)\,.\,d_1\omega^2\,.$$

Odtud $d_1\omega = \lambda/[\omega f'(\omega)]$ a dostáváme

$$\lim_{n\to\infty} b_{i,n}\omega^{n+1} = \frac{a_{i+1}\omega^{i+1} + \ldots + a_m\omega^m}{\omega f'(\omega)}\,\lambda \tag{12}$$

pro $i = 0, 1, \ldots, m - 1$, speciálně $\lim_{n\to\infty} b_{0,n}\omega^n = \lambda/[\omega f'(\omega)]$. Vzhledem k předpokladům b) lemmatu a poněvadž $\lambda > 0, f'(\omega) > 0$, jsou všechny limity ve vzorcích (12) kladná čísla. Odtud plyne, že pro dosti velké přirozené číslo n_1 je $b_{i,n_1} > 0$ pro $i = 0, 1, \ldots, m - 1$; položíme-li ve vztahu (8) $n = n_1$, dostáváme vyjádření čísla λ v požadovaném tvaru (5).

B) Nechť $\lambda \in (\mathbf{O}[\omega])^+$ je voleno libovolně, pak je číslo λ možno vyjádřit ve tvaru $\lambda = \sum_{i=0}^{s} b_i\omega_i$, kde $b_i \in \mathbf{O}$ pro $i = 0, 1, \ldots, s$ a $s \geqq m - 1$.

Nechť $\mathbf{c}_n = (c_{0,n}, c_{1,n}, \ldots, c_{m-1,n})$ pro $n = 0, 1, \ldots$ je posloupnost vektorů příslušná k číslu $\lambda_0 = \dfrac{1}{\omega} = a_1 + a_2\omega + \ldots + a_m\omega^{m-1}$. Pak platí $1 = c_{0,n}\omega^{n+1} + \ldots + c_{m-1,n}\omega^{n+m}$ pro $n = 0, 1, \ldots$ Odtud plyne

$$\lambda = \sum_{i=0}^{s-m} b_i\omega^i(c_{0,s-m-i}\,\omega^{s-m-i+1} + \ldots + c_{m-1,s-m-1}\omega^{s-i}) + \sum_{i=s-m+1}^{s} b_i\omega^i = \omega^{s-m+1}\lambda_1\,,$$

kde $\lambda_1 > 0$ je tvaru (6) a podle odstavce A) se tedy dá vyjádřit ve tvaru (5). Na základě posledního vztahu se dá i λ vyjádřit ve tvaru (5) c. b. d.

Věta 3.1. *Buď $\mathbf{O}$ obor integrity s jedničkou a nechť číslo $\omega > 0$ vyhovuje rovnici*

$$f(x) = a_m x^m + \ldots + a_2 x^2 + a_1 x - 1 = 0 \tag{13}$$

takové, že

a) $a_i \in \mathbf{O}$ *pro* $i = 1, 2, \ldots, m$, b) $a_m > 0,\ a_{m-1} \geqq 0, \ldots, a_2 \geqq 0,\ a_1 > 0$.

Pak je ω positivně definitním prvkem nad oborem integrity $\mathbf{O}$.

Důkaz. Chceme ukázat, že rovnice (13) patří pod typ rovnic (4) z lemmatu 2.1. Vlastnosti a) a b) rovnice (4) splňuje zřejmě i rovnice (13). Zbývá dokázat vlastnost c).

Podle trojúhelníkové nerovnosti platí pro každé komplexní číslo z

$$|a_m z^m + \ldots + a_1 z| \leqq a_m |z|^m + \ldots + a_1 |z| \,.$$

Předpokládejme, že kořen α rovnice (13) splňuje rovnost

$$|a_m \alpha^m + \ldots + a_1 \alpha| = a_m |\alpha|^m + \ldots + a_1 |\alpha| \,.$$

Je známo, že pak musí platit vztahy $a_m \alpha^m = t_m w, \ldots, a_1 \alpha = t_1 w$, kde w je vhodné komplexní číslo a $t_1, \ldots, t_m$ jsou nezáporná čísla. Odtud

$$1 = a_1 \alpha + \ldots + a_m \alpha^m = w(t_1 + \ldots + t_m)$$

a ježto $t_1 + \ldots + t_m > 0$, máme $w > 0$. Odtud $a_1 \alpha = t_1 w > 0$, a protože $a_1 > 0$, plyne $\alpha > 0$.

Rovnice (13) má však jediný kladný kořen ω, tedy nutně $\alpha = \omega$. Pro každý kořen α rovnice (13), kde $\alpha \neq \omega$, tedy platí

$$a_m |\alpha|^m + \ldots + a_1 |\alpha| > |a_m \alpha^m + \ldots + a_1 \alpha| = 1 = a_m \omega^m + \ldots + a_1 \omega \,,$$

a poněvadž funkce $a_m x^m + \ldots + a_1 x$ je rostoucí pro $x > 0$, platí $|\alpha| > \omega$. Věta je tedy důsledkem lemmatu 2.1.

Z dokázané věty ihned plyne důležité lemma:

Lemma 3.1. *Je-li ω positivně definitním prvkem nad tělesem $\mathbf{T}_1$, pak je positivně definitním prvkem nad každým nadoborem $\mathbf{O} \supset \mathbf{T}_1$.*

Důkaz. Buď dán obor $\mathbf{O} \supset \mathbf{T}_1$. Podle věty 1.2 vyhovuje prvek ω algebraické rovnici tvaru $a_m x^m + \ldots + a_1 x - a_0 = 0$, kde $a_i \in \mathbf{T}_1$ pro $i = 0, 1, \ldots, m$, $a_m > 0$, $a_{m-1} \geqq 0, \ldots, a_2 \geqq 0$, $a_1 > 0$, $a_0 > 0$. Potom ω vyhovuje také rovnici $a_0^{-1} a_m x^m + \ldots + a_0^{-1} a_1 x - 1 = 0$ nad oborem $\mathbf{O}$, která je tvaru (13). Podle věty 3.1 je prvek ω positivně definitním prvkem nad oborem integrity $\mathbf{O}$, c. b. d.

Tvrzení lemmatu zobecníme v následující větě:

Věta 3.2. *Nechť množina $\{\omega_1, \ldots, \omega_k\}$ je komposiční base nad oborem integrity $\mathbf{O}$. Pak je $\{\omega_1, \ldots, \omega_k\}$ komposiční basí nad každým nadoborem $\mathbf{O}_1$ podílového tělesa $\mathbf{P}_{\mathbf{O}}$.*

Důkaz. Podle věty 1.6 je $\{\omega_1, \ldots, \omega_k\}$ komposiční base nad tělesem $\mathbf{P}_{\mathbf{O}}$. Odtud chceme ukázat, že $\{\omega_1, \ldots, \omega_k\}$ je komposiční base nad zvoleným oborem $\mathbf{O}_1 \supset \mathbf{P}_{\mathbf{O}}$. Pro $k = 1$ je tvrzení důsledkem lemmatu 3.1. Nechť je tedy tvrzení správné pro jisté $k = r$. Buď $\{\omega_1, \ldots, \omega_r, \omega_{r+1}\}$ komposiční base nad $\mathbf{P}_{\mathbf{O}}$. Pak při vhodném očíslování je $\{\omega_1, \ldots, \omega_r\}$ komposiční base nad $\mathbf{P}_{\mathbf{O}}$ a ω_{r+1} je positivně definitní prvek nad tělesem $\mathbf{P}_{\mathbf{O}}[\omega_1, \ldots, \omega_r] = \mathbf{P}_{\mathbf{O}}(\omega_1, \ldots, \omega_r)$, (viz poznámku před definicí 1.1). Podle indukčního předpokladu je $\{\omega_1, \ldots, \omega_r\}$ komposiční base nad oborem $\mathbf{O}_1$ a podle lemmatu 3.1 je ω_{r+1} positivně definitní prvek nad oborem $\mathbf{O}_1[\omega_1, \ldots, \omega_r] \supset \mathbf{P}_{\mathbf{O}}(\omega_1, \ldots, \omega_r)$. Tedy $\{\omega_1, \ldots, \omega_{r+1}\}$ je komposiční base nad $\mathbf{O}_1$. Tím je důkaz proveden.

Poznámka 3.1. Vzniká opět problém: Platí obdobná věta pro každou positivně definitní basi nad oborem $\mathbf{O}$?

Označme $\mathbf{R}$ těleso racionálních čísel. Pak z věty 3.2 plyne tento důsledek:

Důsledek 3.1. *Je-li $\{\omega_1, \ldots, \omega_k\}$ komposiční base (ω positivně definitní prvek) nad tělesem $\mathbf{R}$, pak je $\{\omega_1, \ldots, \omega_k\}$ komposiční base (ω positivně definitní prvek) nad libovolným reálným číselným tělesem.*

Odtud vyplývá zvláštní důležitost studia positivně definitních prvků a komposičních basí nad tělesem $\mathbf{R}$.

Z lemmatu 3.1 dostáváme ještě další výsledek:

Věta 3.3. *Jsou-li $\omega_1, \ldots, \omega_k$ positivně definitní prvky nad tělesem $\mathbf{T}_1$, pak množina $\{\omega_1, \ldots, \omega_k\}$ je komposiční base nad tělesem $\mathbf{T}_1$.*

Důkaz. Pro $k = 1$ je tvrzení triviální. Předpokládejme, že věta platí pro $k = r$ a buďte $\omega_1, \ldots, \omega_{r+1}$ positivně definitní prvky nad $\mathbf{T}_1$. Pak podle indukčního předpokladu je $\omega_1, \ldots, \omega_r$ komposiční base nad $\mathbf{T}_1$ a podle lemmatu 3.1 je ω_{r+1} positivně definitním prvkem nad $\mathbf{T}_1(\omega_1, \ldots, \omega_r)$. Podle definice 1.2 je tedy $\{\omega_1, \ldots, \omega_{r+1}\}$ komposiční base nad $\mathbf{T}_1$. Tím je důkaz proveden.

Věta 3.4. *Buďte $\{\omega_1, \ldots, \omega_k\}$, $\{\mu_1, \ldots, \mu_s\}$ dvě komposiční base nad tělesem $\mathbf{T}_1$. Pak je množina $\{\omega_1, \ldots, \omega_k, \mu_1, \ldots, \mu_s\}$ komposiční base nad tělesem $\mathbf{T}_1$.*

Věta 3.5. *Je-li $\{\omega_1, \ldots, \omega_k\}$ positivně definitní base nad tělesem $\mathbf{T}_1$ a $\{\mu_1, \ldots, \mu_s\}$ komposiční base nad tělesem $\mathbf{T}_1$, pak je množina $\{\omega_1, \ldots, \omega_k, \mu_1, \ldots, \mu_s\}$ positivně definitní base nad $\mathbf{T}_1$.*

Důkazy těchto dvou vět přenechávám čtenáři.

V předchozích úvahách byly nalezeny dvě podmínky pro to, aby prvek ω byl positivně definitním nad oborem integrity $\mathbf{O}$. Byla to nutná podmínka z věty 1.2 a postačující podmínka z věty 3.1. V případě tělesa se dají tyto dvě podmínky spojit v jedinou:

Věta 3.6. *Prvek $\omega \in \mathbf{T}^+$ je positivně definitní nad tělesem $\mathbf{T}_1$ tehdy a jen tehdy, když vyhovuje algebraické rovnici tvaru*

$$a_m x^m + \ldots + a_1 x - a_0 = 0 \,, \tag{14}$$

kde

a) $a_i \in \mathbf{T}_1$ *pro* $i = 0, 1, \ldots, m$, b) $a_m > 0,\ a_{m-1} \geqq 0, \ldots, a_2 \geqq 0,\ a_1 > 0,\ a_0 > 0.$

Důkaz. Věta je důsledek vět 1.2 a 3.1.

Věta 3.6 podává jistou celkovou charakterisaci všech positivně definitních prvků nad tělesem T_1. Nedává však možnost efektivně rozhodnout o daném (kladném) čísle ω, je-li positivně definitním prvkem nad T_1, či nikoliv. Můžeme říci, že charakterisace podaná ve větě 3.6 není dokonalá.

Abychom mohli formulovat problém dokonalé charakterisace, odvodíme si předně jednu nutnou podmínku.

Věta 3.7. *Jestliže ireducibilní rovnice $p(x) = 0$ z oboru $T_1[x]$ má kladný kořen ω, který je positivně definitním prvkem nad tělesem T_1, potom platí:*

(15) a) *ω je jediný kladný kořen rovnice $p(x) = 0$,*
b) *je-li α další kořen této rovnice, pak $|\alpha| > \omega$.*

Důkaz. Číslo ω zřejmě vyhovuje rovnici $f(x) = 0$ tvaru (14), která, jak známo, má jediný kladný kořen ω a je-li α jiný kořen rovnice $f(x) = 0$, pak platí $|\alpha| > \omega$. V důsledku ireducibility polynomu $p(x)$ a vztahu $p(\omega) = 0$ platí rozklad $f(x) = p(x)\, h(x)$ v oboru $T_1[x]$. Odtud i rovnice $p(x) = 0$ má vlastnosti a), b).

Je zřejmé, že jestliže rovnice $p(x) = 0$ ireducibilní v $T_1[x]$ splňuje podmínky (15), pak její kladný kořen ω je positivně definitním prvkem nad T_1 tehdy a jen tehdy, když v oboru $T_1[x]$ je $p(x)$ dělitelem jistého polynomu $f(x)$ tvaru (14). Problém dokonalé charakterisace lze formulovat jako úlohu stanovit metodu, jíž lze konečným počtem kroků rozhodnout o libovolném ireducibilním polynomu $p(x)$ z oboru $T_1[x]$ a s vlastnostmi (15), je-li faktorem polynomu $f(x)$ z $T_1[x]$ tvaru (14), či nikoliv.

Udáme jen některá dílčí řešení tohoto problému. Jde o vyhledávání podmínek, které spolu s podmínkou (15) stačí k tomu, aby ireducibilní polynom $p(x)$ z $T_1[x]$ byl faktorem polynomu tvaru (14).

Snadno se zjistí, že jednou z takových podmínek je předpoklad, že $p(x)$ je stupně nejvýše druhého. Pokud jde o polynomy $p(x)$ stupně vyššího než druhého, podařilo se mi odvodit jeden speciální výsledek pro kubické rovnice nad tělesem racionálních čísel (viz níže uvedenou větu 4.6).

4. NETRIVIÁLNÍ BASE NAD OBOREM C CELÝCH ČÍSEL

V předchozím odstavci jsme studovali komposiční base nad reálnými číselnými obory integrity a tělesy. Mnohé výsledky byly odvozeny jen pro reálná tělesa, kde se celá teorie značně zjednoduší. Téměř stejně jednoduchá teorie se však dá vybudovat nad oborem C celých racionálních čísel.

Předně si pro obor C odvodíme větu analogickou k větě 3.6:

Věta 4.1. *Číslo $\omega \in T^+$ je positivně definitním prvkem nad oborem C tehdy a jen tehdy, když buď $\omega \in C^+$, nebo ω vyhovuje rovnici tvaru*

$$a_m x^m + \ldots + a_1 x - 1 = 0 \tag{16}$$

takové, že

a) $a_i \in \mathbf{C}$ *pro* $i = 1, \ldots, m,$ b) $a_m > 0,\ a_{m-1} \geqq 0,\ \ldots,\ a_2 \geqq 0,\ a_1 > 0.$

Důkaz. První část věty je důsledkem věty 3.1. Dokažme druhou část: Nechť $\omega \in \mathbf{T}$ je positivně definitní prvek nad oborem $\mathbf{C}$. Pak nastanou tyto možnosti:

a) $\omega - 1 = 0$, tj. $\omega \in \mathbf{C}^+$.

b) $\omega - 1 > 0$, pak podle předpokladu existuje vyjádření tvaru $\omega - 1 = a_m\omega^m + \ldots + a_1\omega + a_0$, kde $a_i \in \mathbf{C}$, $a_i \geqq 0$ pro $i = 0, 1, \ldots, m$, $a_m > 0$, tj. $\omega = a_m\omega^m + \ldots + a_1\omega + (a_0 + 1)$. Protože je $\omega < \omega^2 < \omega^3 < \ldots$, nelze tuto rovnost splnit jinak, než že $m = 0$, $\omega = a_0 + 1$ a tedy $\omega \in \mathbf{C}^+$.

c) $\omega - 1 < 0$, pak lze psát $1 - \omega = a_m\omega^m + \ldots + a_1\omega + a_0$, kde $a_i \in \mathbf{C}$, $a_i \geqq 0$ pro $i = 0, 1, \ldots, m$ a $a_m > 0$, tedy jinak psáno

$$a_m\omega^m + \ldots + (a_1 + 1)\,\omega + (a_0 - 1) = 0\,.$$

Odtud zřejmě plyne $a_0 - 1 < 0$ a to spolu s nerovností $a_0 \geqq 0$ dává $a_0 = 0$. Prvek ω tedy vyhovuje rovnici tvaru (16) a tím je důkaz proveden.

Pro positivně definitní prvky a base nad oborem $\mathbf{C}$ platí teď několik tvrzení, která uvádím bez důkazu.

Věta 4.2. *Jsou-li* $\omega_1, \ldots, \omega_k$ *positivně definitní prvky nad oborem* $\mathbf{C}$, *pak je množina* $\{\omega_1, \ldots, \omega_k\}$ *komposiční basí nad každým oborem integrity* $\mathbf{O}$ *s jedničkou.*

Věta 4.3. *Jsou-li* $\omega_1, \ldots, \omega_k$ *positivně definitní prvky nad oborem* $\mathbf{C}$ *a je-li* $\{\mu_1, \ldots, \mu_s\}$ *komposiční base nad* $\mathbf{C}$, *pak je množina* $\{\omega_1, \ldots, \omega_k, \mu_1, \ldots, \mu_s\}$ *komposiční base nad oborem* $\mathbf{C}$.

Věta 4.4. *Jsou-li* $\omega_1, \ldots, \omega_k$ *positivně definitní prvky nad oborem* $\mathbf{C}$ *a je-li* $\{\mu_1, \ldots, \mu_s\}$ *positivně definitní base nad oborem* $\mathbf{C}$, *pak je množina* $\{\omega_1, \ldots, \omega_k, \mu_1, \ldots, \mu_s\}$ *positivně definitní base nad oborem* $\mathbf{C}$.

Obraťme se teď k problému dokonalé charakterisace positivně definitních prvků nad oborem $\mathbf{C}$. Předně platí věta obdobná k větě 3.7:

Věta 4.5. *Buď* $p(x)$ *primitivní ireducibilní polynom z oboru* $\mathbf{C}[x]$ *s kladným koeficientem při nejvyšší mocnině x. Jestliže rovnice* $p(x) = 0$ *má kladný kořen* ω, *který je positivně definitním prvkem nad oborem* $\mathbf{C}$ *a nepatří do* $\mathbf{C}^+$, *pak platí*

(17) a) ω *je jediný kladný kořen rovnice* $p(x) = 0$,
b) *je-li* α *jiný kořen této rovnice, pak platí* $|\alpha| > \omega$,
c) *absolutní člen polynomu* $p(x)$ *je* -1.

Důkaz. Podle věty 4.1 je číslo ω kořenem rovnice $f(x) = 0$ tvaru (16) z $\mathbf{C}[x]$, v důsledku ireducibility polynomu $p(x)$ a Gaussova lemmatu existuje celočíselný polynom $h(x)$ takový, že $f(x) = p(x)\,h(x)$. Z vlastností polynomu $f(x)$ plyne ihned a) a b) ze (17) a dále je zřejmé, že absolutní člen polynomu $p(x)$ je buď 1 nebo -1. Jelikož koeficient u nejvyšší mocniny x v polynomu $p(x)$ je kladný, je ovšem podle a) tento absolutní člen roven -1. (To plyne např. z Descartesovy věty).

Problém dokonalé charakterisace positivně definitních prvků nad $\mathbf{C}$ spočívá teď v udání metody, jak konečným počtem kroků rozhodnout o libovolném ireducibilním polynomu $p(x)$ z $\mathbf{C}[x]$ a s vlastnostmi (17), je-li faktorem polynomu $f(x)$ z $\mathbf{C}[x]$ tvaru (16), či nikoliv. Podobně jako v případě těles hledáme dílčí řešení problému. Snadno se zjistí, že je-li $p(x)$ ireducibilní polynom stupně nejvýše druhého, který splňuje podmínky (17), pak je $p(x)$ tvaru (16) a tedy jeho kladný kořen ω je positivně definitním prvkem nad oborem $\mathbf{C}$. Tím jsme dokázali:

1. Racionální číslo ω je positivně definitním prvkem nad oborem $\mathbf{C}$ tehdy a jen tehdy, když buďto $\omega \in \mathbf{C}^+$, nebo $\omega = 1/n$, kde n je přirozené číslo.

2. Kvadratické číslo ω je positivně definitním prvkem nad oborem $\mathbf{C}$ právě tehdy, když vyhovuje ireducibilní rovnici tvaru $ax^2 + bx - 1 = 0$, kde a, b jsou přirozená čísla.

Na rozdíl od uvedeného případu polynomů stupně nejvýše druhého neplatí nic obdobného pro polynomy vyšších stupňů. Již v množině ireducibilních polynomů třetího stupně z $\mathbf{C}[x]$ existují polynomy, které vyhovují všem podmínkám (17) a přesto nejsou tvaru (16). V těchto případech již nastávají značné obtíže, což ukážeme na tomto speciálním výsledku:

Věta 4.6. *Je-li $p(x) = a^3x^3 + a^2bx^2 + acx - 1$ polynom z $\mathbf{C}[x]$ splňující podmínky* a), b) *z* (17), *pak je kladný kořen ω polynomu $p(x)$ positivně definitním prvkem nad oborem $\mathbf{C}$.*

Důkaz. A) V případě $b \geqq 0$ je polynom $p(x)$ tvaru (4) a tvrzení plyne z lemmatu 2.1.

B) Buď $b < 0$, pak položme $q(x) = x^3 + bx^2 + cx - 1$. Zřejmě platí $q(ax) = p(x)$ a polynom $q(x)$ proto splňuje podmínky a), b) ze (17). Rovnice $q(x) = 0$ má tedy jediný kladný kořen δ a jsou-li α_1, α_2 další kořeny této rovnice, pak $\delta < |\alpha_1|$, $\delta < |\alpha_2|$. Odtud $\delta^3 < \delta \,.\, |\alpha_1|\,|\alpha_2| = |\delta\alpha_1\alpha_2| = 1$ a tedy $\delta < 1$. Z toho předně plyne, že $c = (1 - \delta^3 - b\delta^2)/\delta$ je kladné číslo. Podle Descartesovy věty nemá rovnice $q(x) = 0$ záporný kořen, má tedy dva kořeny komplexně sdružené, $\alpha_1 = \alpha$, $\alpha_2 = \bar{\alpha}$. Ze vztahů $q(0) = -1$, $q(\delta) = 0$, $0 < \delta < 1$ plyne $q(1) = 1 + b + c - 1 > 0$ a odtud $b + c \geqq 1$.

Položme $g = -b$, $h = b + c$, pak je $g \geqq 1$, $h \geqq 1$ a $q(x) = x^3 - gx^2 + (g + h)x - 1$.

Ukážeme, že polynom $q(x)$ je faktorem jistého polynomu z $\mathbf{C}[x]$ tvaru (16) a to užitím zvláštní modifikace metody neurčitých koeficientů.

Uvažujme rekurentní posloupnosti $\{r_n\}$, $\{s_n\}$ určené podmínkami:

$$(18)\qquad \begin{aligned} r_{-1} &= r_0 = 0\,, \quad r_1 = 1\,,\\ r_n &= g \,.\, r_{n-1} - (g + h)\, r_{n-2} + r_{n-3} \quad \text{pro} \quad n \geqq 2\,, \end{aligned}$$

$$(19)\qquad \begin{aligned} s_0 &= 0\,, \quad s_1 = 1\,, \quad s_2 = g\,,\\ s_n &= (g + h)\, s_{n-1} - g \,.\, s_{n-2} + s_{n-3} \quad \text{pro} \quad n \geqq 3\,. \end{aligned}$$

Předně ukážeme, že posloupnost $\{s_n\}$ je neklesající pro všechna n a pro $n \geqq 3$ dokonce rostoucí.

Snadno se vidí, že $1 = s_1 \leqq s_2 \leqq g \, . \, s_2 \leqq s_3$. Dále platí podle (19) $s_4 - g \, . \, s_3 = h \, . \, s_3 - g \, . \, s_2 + s_1 \geqq s_3 - g \, . \, s_2 + 1 \geqq 1$, tedy $s_4 - g \, . \, s_3 > 0$.

Buď $n \geqq 4$ a předpokládejme, že platí $s_k - g \, . \, s_{k-1} > 0$ pro $4 \leqq k \leqq n$ a $s_k > 0$ pro $1 \leqq k \leqq n$. Pak podle (19) $s_{n+1} - g \, . \, s_n = h \, . \, s_n - g \, . \, s_{n-1} + s_{n-2} > s_n - g \, . \, s_{n-1} > 0$, využijeme-li indukčního předpokladu; tedy $s_{n+1} - g \, . \, s_n > 0$ a $s_{n+1} > 0$. Tím je dokázáno indukcí, že platí $s_{n+1} > g \, . \, s_n$ (a tedy $s_{n+1} > s_n$) pro všechna $n \geqq 3$. Speciálně odtud plyne, že $\lim_{n \to \infty} s_n = +\infty$.

Vyšetříme dále posloupnost $\{r_n\}$. Ukážeme, že existuje index $m \geqq 2$ takový, že $1 = r_1 \leqq r_2 \leqq \ldots \leqq r_m, \; r_m > r_{m+1}$. Rovnice $q(x) = 0$ je zřejmě charakteristickou rovnicí rekurentního vztahu (18) (viz [2], str. 296–297) a lze tedy psát

$$r_n = A \, . \, \delta^{n+1} + B \, . \, \alpha^{n+1} + C \, . \, \bar{\alpha}^{n+1} \quad \text{pro} \quad n = -1, 0, 1, \ldots$$

s vhodnými komplexními koeficienty A, B, C. Z počátečních podmínek $r_{-1} = r_0 = 0$, $r_1 = 1$ se určí

$$A = \frac{1}{(\alpha - \delta)(\bar{\alpha} - \delta)}, \quad B = \frac{1}{(\alpha - \delta)(\alpha - \bar{\alpha})}, \quad C = \frac{1}{(\bar{\alpha} - \delta)(\bar{\alpha} - \alpha)}.$$

Odtud A je kladné číslo a B, C jsou čísla komplexně sdružená. Důkaz teď provedeme sporem. Předpokládejme, že posloupnost $\{r_n\}$ je neklesající, pak platí speciálně $r_n \geqq r_1 = 1$ pro $n = 1, 2, \ldots$ Protože $\delta < 1$, je $\lim_{n \to \infty} A \, . \, \delta^n = 0$ a odtud skoro pro všechna n je $B \, . \, \alpha^n + \bar{B} \, . \, \bar{\alpha}^n = r_{n-1} - A \, . \, \delta^n > 0$. Z toho plyne, že pro všechna $n \geqq N$, kde N je dostatečně velké číslo, platí $\mathrm{Re}(B \, . \, \alpha^n) > 0$. Označme ϕ_1, ϕ amplitudy čísel B, α, pak má platit $\cos(\phi_1 + n\phi) > 0$ pro všechna $n \geqq N$. Snadno se ukáže, že to není možno splnit, protože $0 < \phi < 2\pi$. Předpoklad, že posloupnost $\{r_n\}$ je neklesající, vede tedy ke sporu. Protože platí $r_1 \leqq r_2 = g$, nutně existuje požadované relativní maximum r_m a při tom platí $m \geqq 2$.

Nyní protože posloupnost $\{s_n\}$ je neklesající a platí $\lim_{n \to \infty} s_n = +\infty$, existuje index t takový, že $s_t \leqq r_m \leqq s_{t+1}$, $t \geqq 1$.

Definujme čísla c_i pro $-2 \leqq i \leqq m + t + 4$ vztahy:

$$c_{-2} = c_{-1} = c_0 = 0, \; c_1 = r_1, \; c_2 = r_2, \; \ldots, \; c_m = r_m, \; c_{m+1} = r_m,$$
$$c_{m+2} = s_t, \; \ldots, \; c_{m+t} = s_2, \; c_{m+t+1} = s_1 = 1,$$
$$c_{m+t+2} = c_{m+t+3} = c_{m+t+4} = 0.$$

Označme $h(x) = c_1 x^{m+t} + \ldots + c_{m+t} \, . \, x + c_{m+t+1}$, ukážeme, že polynom $q(x) \, . \, h(x)$ je již tvaru (16). Jelikož $q(x) = x^3 - g \, . \, x^2 + (g + h) x - 1$, platí

$$q(x) \, . \, h(x) = \sum_{i=1}^{m+t+4} (c_i - g \, . \, c_{i-1} + (g + h) c_{i-2} - c_{i-3}) \, . \, x^{m+t+4-i} = \sum_{i=1}^{m+t+4} d_i \, . \, x^{m+t+4-i}.$$

Předně platí $d_1 = c_1 = r_1 = 1$, dále pro $2 \leqq i \leqq m$ máme podle (18) $d_i = r_i - g \,.\, r_{i-1} + (g + h)\, r_{i-2} - r_{i-3} = 0$. Dále

$$d_{m+1} = r_m - g \,.\, r_m + (g + h)\, r_{m-1} - r_{m-2} > r_{m+1} - g \,.\, r_m + (g + h)\, r_{m-1}\, r_{m-2} = 0\,,$$

$$d_{m+2} = s_t - g \,.\, r_m + (g + h)\, r_m - r_{m-1} = s_t + h \,.\, r_m - r_{m-1} > 0\,,$$

protože $s_t > 0$ a $r_m \geqq r_{m-1}$.

$$d_{m+3} = s_{t-1} - g \,.\, s_t + (g + h)\, r_m - r_m = s_{t-1} + g(r_m - s_t) + (h - 1)\, r_m \geqq 0\,,$$

neboť $r_m \geqq s_t$.

Nyní, je-li $t = 1$, pak

$$d_{m+4} = (g + h)\, s_1 - r_m \geqq (g + h)\, s_1 - s_2 = h > 0\,,$$

je-li však $t \geqq 2$, pak s využitím podmínky (19) dostaneme

$$\begin{aligned} d_{m+4} &= s_{t-2} - g \,.\, s_{t-1} + (g + h)\, s_t - r_m \geqq \\ &\geqq s_{t-2} - g \,.\, s_{t-1} + (g + h)\, s_t - s_{t+1} = 0\,. \end{aligned}$$

Konečně pro $m + 5 \leqq i \leqq m + t + 4$ platí

$$d_i = c_i - g \,.\, c_{i-1} + (g + h)\, c_{i-2} - c_{i-3}\,,$$

kde $c_i = s_{m+t+2-i}$ pro $i \leqq m + t + 2$ a $c_{m+t+3} = c_{m+t+4} = 0$. Podmínka (19) pak dává $d_i \geqq 0$ pro $m + 5 \leqq i \leqq m + t + 2$.

Dále je $d_{m+t+3} = (g + h)\, s_1 - s_2 = h > 0$; koeficient u x^1 v polynomu $q(x) \,.\, h(x)$ je tedy kladný.

Konečně $d_{m+t+4} = - s_1 = - 1$. Tím je ukázáno, že polynom $q(x) \,.\, h(x)$ je tvaru (16). Odtud je zřejmě i polynom $q(ax) \,.\, h(ax) = p(x) \,.\, h(ax)$ tvaru (16) a tedy kladný kořen ω rovnice $p(x) = 0$ je positivně definitní prvkem nad oborem $\mathbf{C}$.

Poznámka 4.1. Konstrukce polynomu $h(x)$ takového, že $q(x) \,.\, h(x)$ je tvaru (16), naznačená v důkaze, není ovšem jediná možná. Zdá se však, že při jakékoliv konstrukci vhodného polynomu $h(x)$ budou hrát podstatnou roli limitní úvahy.

Schema uvedené v důkaze věty budeme teď s nepatrnou obměnou ilustrovat na několika příkladech:

$$(x^3 - x^2 + 2x - 1)(x + 1) = x^4 + x^2 + x - 1\,,$$

$$\begin{aligned} (x^3 - 3x^2 + 4x - 1)(x^5 + 3x^4 + 5x^3 + 4x^2 + 3x + 1) &= \\ = x^8 + 8x^4 + 3x^3 + 5x^2 + x - 1\,, \end{aligned}$$

$$\begin{aligned} (x^3 - 4x^2 + 5x - 1)(x^{11} + 4x^{10} + 11x^9 + 25x^8 + 49x^7 + 82x^6 + 108x^5 + \\ + 71x^4 + 65x^3 + 16x^2 + 4x + 1) = x^{14} + 239x^6 + 3x^5 + 194x^4 + x - 1\,. \end{aligned}$$

Literatura

[1] *Van der Waerden*: Moderne Algebra, I. Teil, Berlin 1937.

[2] *M. E. Nörlund*: Vorlesungen über Differenzenrechnung, Berlin 1924.

Резюме

О ПОЛОЖИТЕЛЬНО ОПРЕДЕЛЕННЫХ БАЗАХ НАД КОЛЬЦАМИ ДЕЙСТВИТЕЛЬНЫХ ЧИСЕЛ

ОЛДРЖИХ КОВАЛСКИ (OLDŘICH KOWALSKI), Брно

Множество $\{\omega_1, \ldots, \omega_k\}$ положительных чисел называется *положительно определенной базой* над действительным кольцом $\mathbf{O}$, если всякий положительный элемент ω расширенного кольца $\mathbf{O}[\omega_1, \ldots, \omega_k]$ записывается в виде

$$\beta = \sum_{i_1=\mathbf{O}}^{s_1} \sum_{i_2=\mathbf{O}}^{s_2} \ldots \sum_{i_k=\mathbf{O}}^{s_k} h_{i_1,\ldots,i_k} \, \omega_1^{i_1} \ldots \omega_k^{i_k},$$

где $h_{i_1,\ldots,i_k} \in \mathbf{O}$, $h_{i_1,\ldots,i_k} \geqq \mathbf{O}$ для всех перестановок $i_1, i_2, \ldots, i_k$. В случае, когда $k = 1$, получается понятие *положительно определенного элемента* над кольцом $\mathbf{O}$.

Доказывается, что *если даны такие положительные числа $\omega_1, \ldots, \omega_k$, что ω_1 положительно определенно над кольцом $\mathbf{O}$, ω_2 положительно определенно над кольцом $\mathbf{O}[\omega_1], \ldots, \omega_k$ положительно определенно над кольцом $\mathbf{O}[\omega_1, \ldots, \omega_{k-1}]$, то множество $\{\omega_1, \ldots, \omega_k\}$ является положительно определенной базой над кольцом $\mathbf{O}$.* Положительно определенная база указанного вида называется *композиционной.* В настоящей работе нерешен вопрос о том, имеются ли положительно определенные базы, которые не являются композиционными.

Доказывается, что *если числа $\omega_1, \ldots, \omega_k$ образуют композиционную базу над кольцом $\mathbf{O}$, то кольцо $\mathbf{O}[\omega_1, \ldots, \omega_k]$ является конечным алгебраическим расширением кольца $\mathbf{O}$.* Именно, всякий *положительно определенный элемент над $\mathbf{O}$ является корнем многочлена вида*

$$f(x) = a_m x^m + \ldots + a_2 x^2 + a_1 x - a_0, \tag{1}$$

где $a_i \in \mathbf{O}$ для $i = 0, 1, \ldots, m$ и $a_m > 0$, $a_{m-1} \geqq 0, \ldots, a_2 \geqq 0$, $a_1 > 0$, $a_0 > 0$. Сверх этого мы получаем:

(2) *ω является единственным положительным корнем многочленна $f(x)$. Если $\alpha \neq \omega$ является другим корнем многочленна $f(x)$, то справедливо неравенство $|\alpha| > \omega$.*

С другой стороны, *если кольцо $\mathbf{O}$ содержит единицу и если положительное число ω является корнем многочлена вида*

$$g(x) = a_m x^m + \ldots + a_2 x^2 + a_1 x - 1, \tag{3}$$

где $a_i \in \mathbf{O}$ для $i = 1, \ldots, m$ и $a_m > 0$, $a_{m-1} \geqq 0, \ldots, a_2 \geqq 0$, $a_1 > 0$, то ω является положительно определенным элементом над кольцом $\mathbf{O}$.

Доказываются следующие предложения:

Если множество $\{\omega_1, \ldots, \omega_k\}$ *есть композиционная база (или число* ω *есть положительно определенный элемент) над кольцом* $\mathbf{O}$, *то* $\{\omega_1, \ldots, \omega_k\}$ *является композиционной базой (или* ω *является положительно определенным элементом) над всяким кольцом* $\mathbf{O}_1$, *которое содержит поле частных* $\mathbf{P}_{\mathbf{O}}$ *от* $\mathbf{O}$.

Положительное число ω *тогда и только тогда является положительно определенным элементом над полем* $\mathbf{T}_1$ *(или над кольцом целых чисел* $\mathbf{C}$*), когда оно является корнем многочлена вида* (1) *над полем* $\mathbf{T}_1$ *(или многочленом вида* (3) *над кольцом* $\mathbf{C}$*).*

Всякое множество $\{\omega_1, \ldots, \omega_k\}$ *положительно определенных элементов над полем* $\mathbf{T}_1$ *(или над кольцом* $\mathbf{C}$*) является композиционной базой над полем* $\mathbf{T}_1$ *(или над кольцом* $\mathbf{C}$*).*

Далее изучаются неприводимые многочлены над полем $\mathbf{T}_1$ или над кольцом $\mathbf{C}$, которые могут иметь своим корнем положительно определенный элемент над полем $\mathbf{T}_1$ или над $\mathbf{C}$. Доказывается, что *все такого рода многочлены* $f(x)$ *обладают свойствами* (2).

Приходится к формулировке проблемы совершенной характеристики всех положительно определенных элементов над полем $\mathbf{T}_1$ или над кольцом $\mathbf{C}$. В связи с этой проблемой доказывается следующий специальный результат:

Если многочлен вида $g(x) = a^3x^3 + a^2bx^2 + acx - 1 = 0, a > 0$, *над кольцом* $\mathbf{C}$ *обладает положительным корнем* ω *и если для* $g(x)$ *и* ω *выполнены условия* (2), *то* ω *является положительно определенным элементом над кольцом* $\mathbf{C}$.

Zusammenfassung

ÜBER POSITIV DEFINITE BASEN ÜBER REELLEN INTEGRITÄTSBEREICHEN

Oldřich Kowalski, Brno

Eine Menge $\{\omega_1, \ldots, \omega_k\}$ der positiven Zahlen nennen wir eine *positiv definite Basis* über dem reellen Integritätsbereiche $\mathbf{O}$, wenn sich jedes positive Element β des erweiterten Bereiches $\mathbf{O}[\omega_1, \ldots, \omega_k]$ in der Form

$$\beta = \sum_{i_1=0}^{s_1} \sum_{i_2=0}^{s_2} \ldots \sum_{i_k=0}^{s_k} h_{i_1,\ldots,i_k} \omega_1^{i_1} \ldots \omega^{ki}$$

ausdrücken lässt, wobei $h_{i_1,\ldots,i_k} \in \mathbf{O}$, $h_{i_1,\ldots,i_k} \geqq 0$ für alle n-tupel von Zahlen $i_1, \ldots, i_k$. Im Falle $k = 1$ sprechen wir besonders über ein *positiv definites Element* über dem Integritätsbereiche $\mathbf{O}$.

Es wird folgendes bewiesen: *Sind* $\omega_1, \ldots, \omega_k$ *solche positive Zahlen, dass* ω_1 *positiv definit über dem Bereiche* $\mathbf{O}$, ω_2 *positiv definit über dem Bereiche* $\mathbf{O}[\omega_1]$, $\ldots$, ω_k *positiv definit über dem Bereiche* $\mathbf{O}[\omega_1, \omega_2, \ldots, \omega_k]$ *ist, so ist die Menge* $\{\omega_1, \ldots, \omega_k\}$

positive definite Basis über dem Bereiche $\mathbf{O}$. Jede positiv definite Basis dieser Form wird eine *Kompositionsbasis* genannt. Die Frage, ob positiv definite Basen existieren, die keine Kompositionsbasen sind, wird in dieser Arbeit nicht gelöst.

Es lässt sich folgendes zeigen:

Ist $\{\omega_1, \ldots, \omega_k\}$ *eine Kompositionsbasis über dem Bereiche* $\mathbf{O}$, *so ist der Bereich* $\mathbf{O}[\omega_1, \ldots, \omega_k]$ *eine endliche algebraische Erweiterung des Bereiches* $\mathbf{O}$. *Besonders jedes positiv definite Element* ω *über* $\mathbf{O}$ *genügt einer algebraischen Gleichung von der Form*

$$f(x) = a_m x^m + \ldots + a_2 x^2 + a_1 x - a_0 = 0\,, \tag{1}$$

wobei $a_i \in \mathbf{O}$ *für* $i = 0, 1, \ldots, m$ *und* $a_m > 0, a_{m-1} \geqq 0, \ldots, a_2 \geqq 0, a_1 > 0, a_0 > 0$ *ist;* ausserdem gilt

(2) *ω ist die einzige positive Wurzel der Gleichung $f(x) = 0$, ist α eine weitere Wurzel der Gleichung $f(x) = 0$, so ist $|\alpha| > \omega$.*

Andererseits, *ist* $\mathbf{O}$ *ein reeller Integritätsbereich mit dem Einheitselement und genügt eine positive Zahl* ω *der algebraischen Gleichung von der Form*

$$a_m x^m + \ldots + a_2 x^2 + a_1 x - 1 = 0\,, \tag{3}$$

wobei $a_i \in \mathbf{O}$ *für* $i = 1, \ldots, m$, $a_m > 0$, $a_{m-1} \geqq 0, \ldots, a_2 \geqq 0$, $a_1 > 0$ *gilt, so ist* ω *ein positiv definites Element über dem Bereiche* $\mathbf{O}$.

Es werden weiter folgende Behauptungen bewiesen:

Ist $\{\omega_1, \ldots, \omega_k\}$ *eine Kompositionsbasis (bzw.* ω *ein positiv definites Element) über dem Bereiche* $\mathbf{O}$, *so ist* $\{\omega_1, \ldots, \omega_k\}$ *eine Kompositionsbasis (bzw.* ω *ein positiv definites Element) über jedem Oberbereiche* $\mathbf{O}_1$ *des Quotientenkörpers* $\mathbf{P}_{\mathbf{O}}$.

Eine positive Zahl ω *ist dann und nur dann ein positiv definites Element über dem Körper* $\mathbf{T}_1$ *(bzw. über dem Integritätsbereiche der ganzen Zahlen* $\mathbf{C}$*), wenn sie einer Gleichung von der Form* (1) *über dem Körper* $\mathbf{T}$ *(bzw. einer Gleichung von der Form* (3) *über dem Bereiche* $\mathbf{C}$*) genügt.*

Sind $\omega_1, \ldots, \omega_k$ *positiv definite Elemente über dem Körper* $\mathbf{T}_1$ *(bzw. dem Bereiche* $\mathbf{C}$*), so ist die Menge* $\{\omega_1, \ldots, \omega_k\}$ *eine Kompositionsbasis über dem Körper* $\mathbf{T}_1$ *(bzw. dem Bereiche* $\mathbf{C}$*).*

Es werden weiter irreduzible Gleichungen über dem Körper $\mathbf{T}_1$ (bzw. dem Bereiche $\mathbf{C}$) behandelt, die als Wurzel ein positiv definites Element ω über $\mathbf{T}_1$ (bzw. über $\mathbf{C}$) zulassen. Es zeigt sich, dass *jede solche Gleichung* $f(x) = 0$ *die Eigenschaften* (2) *besitzt.* Es wird das Problem der vollkommenen Charakterisierung der positiv definiten Elemente über dem Körper $\mathbf{T}_1$ (bzw. über dem Bereiche $\mathbf{C}$) formuliert. In diesem Zusammenhang wird ein Spezialergebniss bewiesen:

Hat die Gleichung $g(x) = a^3x^3 + a^2bx^2 + acx - 1 = 0$ *mit* $a > 0$ *über dem Bereiche* $\mathbf{C}$ *eine positive Wurzel* ω, *die die Eigenschaften* (2) *besitzt, so ist* ω *ein positiv definites Element über dem Bereiche* $\mathbf{C}$.