PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020

EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

O CIRKULANTNÍCH MATICÍCH STUPNĚ 9

Viktor DUBOVSKÝ
VŠB – Technická univerzita Ostrava

1 ÚVOD

Na začátek připomeňme definici a základní vlastnosti cirkulantních matic. Matici řádu n nazýváme *cirkulantní maticí*, jestliže každý její řádek získáme cyklickým posunem řádku nad ním. To znamená, že jde o matici tvaru

$$\mathbf{A} = \begin{pmatrix} a_0 & a_1 & a_2 & & & \cdots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & a_2 & & \cdots & a_{n-2} \\ & a_{n-1} & a_0 & a_1 & \ddots & & \vdots \\ \vdots & & \ddots & a_0 & \ddots & & \\ & & & \ddots & \ddots & & a_2 \\ & & & & & & a_1 \\ a_1 & \cdots & & & & a_{n-1} & a_0 \end{pmatrix}.$$

Je tedy zjevné, že taková matice je zcela určena svým prvním řádkem, proto ji budeme značit $\mathbf{A} = circ_n\,(a_0, a_1, \ldots, a_{n-1})$. Z prvků prvního řádku - a_i - můžeme prvek matice $\mathbf{A}$ ležící na j-tém řádku a v k-tém sloupci - A_{jk} - určit pomocí následujícího vztahu

$$a_{jk} = a_{k-j} \pmod n.$$

Snadno lze ověřit, že součet i součin dvou cirkulantních matic je opět cirkulantní maticí, což znamená, že množina všech cirkulantních matic spolu se standardními operacemi sčítání a násobení matic tvoří okruh, který bude v dalším značit $\mathcal{C}_n$.

Jedním z důležitých vztahů, kterých využíváme, je fakt, že cirkulantní matice lze diagonalizovat pomocí *Fourierovy matice* $\mathbf{F}_n$, tj. matice

$$\mathbf{F}_n = \left(\frac{\zeta_n^{ij}}{\sqrt{n}}\right)_{i,j=0,1,\ldots,n-1,}$$

kde ζ_n je primitivní n-tý kořen z jedničky $\zeta_n = \mathrm{e}^{\frac{2\pi \mathrm{i}}{n}} = \cos\frac{2\pi\mathrm{i}}{n} + \mathrm{i}\sin\frac{2\pi\mathrm{i}}{n}$.

Uvažujme součin $\mathbf{D} = \mathbf{FAF}^{-1}$, kde $\mathbf{F}$ je *Fourierova matice* řádu n a cirkulantní matice $\mathbf{A} = circ_n\,(a_0, a_1, \ldots, a_{n-1})$ potom výsledná matice $\mathbf{D}$ je diagonální. Prvky diagonály λ_i jsou vlastní čísla matice $\mathbf{A}$ a rovnají se

$$\lambda_i = a_0 + a_1\zeta_n^i + a_2\zeta_n^{2i} + \cdots + a_{n-1}\zeta_n^{(n-1)i}. \tag{1}$$

PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020
EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO
Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

Protože Fourierova matice $\mathbf{F}$ je unitární, jsou si determinanty $|\mathbf{A}|$ a $|\mathbf{D}|$ rovny a můžeme psát $|\mathbf{A}| = \prod_{i=0}^{n-1} \lambda_i$. Pro $i = 0$ je $\lambda_0 = a_0 + a_1 + \cdots + a_{n-1}$ a λ_i pro $i = 1, 2, \ldots, n-1$ můžeme nahlížet jako prvky n-tého cyklotomického tělesa $\mathbb{Q}(\zeta_n)$.

Díky tomuto vztahu můžeme použít cirkulantní matice k reprezentaci prvků a aritmetiky cyklotomických těles $\mathbb{Q}(\zeta_n)$.

V případě, kdy je $n = l$, kde l je liché prvočíslo, lze tuto reprezentaci obdržet poměrně snadno. Vlastní čísla λ_i, pro $i = 1, 2, \ldots, l-1$, jsou vzájemně konjugované prvky tělesa $\mathbb{Q}(\zeta_n)$ a tedy platí

$$|\mathbf{A}| = \prod_{i=0}^{l-1} \lambda_i = (a_0 + a_1 + \cdots + a_{n-1}) \prod_{i=1}^{l-1} \lambda_i = (a_0 + a_1 + \cdots + a_{n-1}) \, \mathrm{N}_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\lambda_1) =$$
$$= (a_0 + a_1 + \cdots + a_{n-1}) \, \mathrm{N}_{\mathbb{Q}(\zeta_l)/\mathbb{Q}} \left(a_0 + a_1\zeta_n + a_2\zeta_n^2 + \cdots + a_{n-1}\zeta_n^{(n-1)}\right),$$

kde $\mathrm{N}_{\mathbb{Q}(\zeta_l)/\mathbb{Q}}(\alpha)$ značí normu prvku $\alpha \in \mathbb{Q}(\zeta_l)$.

Problémem je, že množina $1, \zeta_l, \zeta_l^2, \ldots, \zeta_l^{l-1}$ není bází $\mathbb{Q}(\zeta_l)$, protože obsahuje l lineárně závislých prvků. Z tvaru l-tého cyklotomického polynomu $\Phi_l(x) = 1 + x + x^2 + \cdots + x^{l-1}$ však vidíme, že $\zeta_l + \zeta_l^2 + \cdots + \zeta_l^{l-1} = -1$. Můžeme tedy vytvořit bázi $\zeta_l, \zeta_l^2, \ldots, \zeta_l^{l-1}$, která je navíc celou normální bází $\mathbb{Q}(\zeta_l)$. Samotnou reprezentaci $\mathbb{Q}(\zeta_l)$ pak získáme pomocí faktorového okruhu $\mathcal{C}_l/\mathcal{I}$, kde $\mathcal{I} \subset \mathcal{C}_l$ je ideál tvořený maticemi typu $\circ_{l(a,a,\ldots,a)}$. Detaily lze nalézt v článku [1].

V případě $n = pq$, kdy n je součinem dvou různých lichých prvočísel p, q, se potýkáme s problémy, že vlastní čísla λ_i s $i \equiv 0 \pmod{p}$ patří do tělesa $\mathbb{Q}(\zeta_q)$, λ_i s $i \equiv 0 \mod q$ patří do tělesa $\mathbb{Q}(\zeta_p)$, a jen prvky λ_i s $\gcd(i, n) = 0$ patří do $\mathbb{Q}(\zeta_n)$. Ovšem pokud použijeme celou normální bázi tvořenou zde prvky ζ_n^i s exponenty i nesoudělnými s n, lze opět obdržet reprezentaci tělesa $\mathbb{Q}(\zeta_n)$ (viz [2]).

V tomto článku ukážeme podobný způsob reprezentace pro těleso $\mathbb{Q}(\zeta_9)$. Bohužel však pro $n = 9$, a také pro $n = l^2$ s lichým prvočíslem l, není n-té cyklotomické těleso slabě rozvětvené a tedy nemá celou normální bázi. Proto budeme pracovat pouze celou mocninnou bází.

2 ZÁKLADNÍ POZOROVÁNÍ

Stupeň tělesa $\mathbb{Q}(\zeta_9)$ je $[\mathbb{Q}(\zeta_9) : \mathbb{Q}] = \varphi(9) = 6$, kde $\varphi(n)$ je Eulerova funkce. Celá mocninná báze $\mathbb{Q}(\zeta_9)$ je tvořena prvky $1, \zeta_9, \zeta_9^2, \ldots, \zeta_9^5$, každý prvek $\gamma \in \mathbb{Q}(\zeta_9)$ teda může být zapsán ve tvaru $\gamma = c_0 + c_1\zeta_9 + c_2\zeta_9^2 + \cdots + c_5\zeta_9^5$. Galoisova grupa rozšíření $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ je generována automorfismem

$$\phi : \mathbb{Q}(\zeta_9) \longrightarrow \mathbb{Q}(\zeta_9), \quad \phi : \zeta_9 \longmapsto \zeta_9^2$$

a je isomorfní s multiplikativní grupou $\left(\mathbb{Z}_9^\times, \cdot\right)$.

Prvek $\phi(\gamma)$ konjugovaný s γ má tvar

$$\phi(\gamma) = c_0 + c_1\zeta_9^2 + c_2\left(\zeta_9^2\right)^2 + \cdots + c_5\left(\zeta_9^2\right)^5 = c_0 + c_1\zeta_9^2 + c_2\zeta_9^4 + c_3\zeta_9^6 + c_4\zeta_9^8 + c_5\zeta_9^{10}.$$

PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020
EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO
Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

Protože $\zeta_9^9 = 1$, lze nahradit člen ζ_9^{10} členem ζ_9. K dalším úpravám musíme použít vztahů, které obdržíme z cyklotomického polynomu $\Phi_9(x) = 1 + x^3 + x^6$ a rovnosti $\Phi_9(\zeta_9) = 1 + \zeta_9^3 + \zeta_9^6 = 0$, z níž plynou vztahy

$$\zeta_9^6 = -1 - \zeta_9^3, \quad \zeta_9^7 = -\zeta_9 - \zeta_9^4, \quad \zeta_9^8 = -\zeta_9^2 - \zeta_9^5, \tag{2}$$

a podobně pro vyšší mocniny. Takto obdržíme

$$\phi(\gamma) = (c_0 - c_3) + c_5\zeta_9 + (c_1 - c_4)\zeta_9^2 - c_3\zeta_9^3 + c_2\zeta_9^4 - c_4\zeta_9^5.$$

Stejným způsobem vyjádříme všechny konjugace γ, které označíme γ_i, kde $\gamma_1 = \gamma, \gamma_2 = \phi(\gamma_1)$, a tak dále pro $i = 1, 2, \ldots 6$.

Nechť $\mathbf{A}$ značí cirkulantní matici řádu 9, $\mathbf{A} = circ_9(a_0, a_1, \ldots, a_8)$. Jak již bylo zmíněno výše vlastní čísla této matice jsou prvky tělesa $\mathbb{Q}(\zeta_9)$. Tento vztah opět vede k myšlence nalezení homomorfismu mezi okruhem $\mathcal{C}_9$ a tělese $\mathbb{Q}(\zeta_9)$. Definujme tedy zobrazení ψ a to takto

$$\psi : \mathcal{C}_9 \longrightarrow \mathbb{Q}(\zeta_9), \quad \psi : \mathbf{A} \longmapsto a_0 + a_1\zeta_9 + a_2\zeta_9^2 + \cdots + a_8\zeta_9^8.$$

Abychom ukázali, že ψ je homomorfismem, musíme ověřit, že $\psi(\mathbf{A} + \mathbf{B}) = \psi(\mathbf{A}) + \psi(\mathbf{B})$ a $\psi(\mathbf{A} \cdot \mathbf{B}) = \psi(\mathbf{A}) \cdot \psi(\mathbf{B})$.

První vztah je zřejmý. V druhém uvažujme matice $\mathbf{A} = circ_9(a_0, a_1, \ldots, a_8)$, $\mathbf{B} = circ_9(b_0, b_1, \ldots, b_8)$ a jejich součin $\mathbf{C} = \mathbf{A} \cdot \mathbf{B} = circ_9(c_0, c_1, \ldots, c_8)$, pro jehož prvky platí

$$c_k = \sum_{\substack{i+j \equiv k \\ (\mathrm{mod}\ 9)}} a_i b_j. \tag{3}$$

Násobením prvků $\alpha = a_0 + a_1\zeta_9 + \cdots + a_8\zeta_9^8$ a $\beta = b_0 + b_1\zeta_9 + \cdots + b_8\zeta_9^8$ v tělese $\mathbb{Q}(\zeta_9)$ dostáváme prvek $\gamma = c_0 + c_1\zeta_9 + \cdots + c_8\zeta_9^8$ s koeficienty c_k, které také splňují rovnici (3). Přičemž zde nevyjadřujeme γ v mocninné bázi, ale pouze upravujeme mocniny ζ_9 pomocí vztahu $\zeta_9^9 = 1$, tj. modulo 9.

Z předchozího je vidět, že ψ je opravdu homomorfismus. Zjevně obrazem ψ je celé těleso $\mathbb{Q}(\zeta_9)$, takže ψ je surjektivní. Příklad matic $circ_9(0, 0, \ldots, 0) \neq circ_9(1, 1, \ldots, 1)$ a jejich obrazů $\psi(circ_9(0, 0, \ldots, 0)) = 0$ a $\psi(circ_9(1, 1, \ldots, 1)) = 0$ však ukazuje, že ψ není injektivní.

Zkoumejme tedy obraz matice $\mathbf{A} = circ_9(a_0, a_1, \ldots, a_8)$ v tělese $\mathcal{C}_9$. Využitím vztahů (2) dostáváme

$$\begin{aligned}
&\psi(circ_9(a_0, a_1, \ldots, a_8)) = a_0 + a_1\zeta_9 + \cdots + a_8\zeta_9^8 \\
&= a_0 + a_1\zeta_9 + a_2\zeta_9^2 + \cdots + a_7\left(-\zeta_9 - \zeta_9^4\right) + a_8\left(-\zeta_9^2 - \zeta_9^5\right) \\
&= (a_0 - a_6) + (a_1 - a_7)\zeta_9 + (a_2 - a_8)\zeta_9^2 + (a_3 - a_6)\zeta_9^3 + (a_4 - a_7)\zeta_9^4 + (a_5 - a_8)\zeta_9^5.
\end{aligned}$$

PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020
EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO
Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

Odtud je patrné, že pokud má matice $\mathbf{A}$ patřit jádru homomorfismu ψ, tj. má-li platit $\psi(\mathbf{A}) = 0$, pak platí následují rovnosti

$$a_0 - a_6 = 0, \quad a_1 - a_7 = 0, \quad a_2 - a_5 = 0, \quad a_3 - a_6 = 0, \quad a_4 - a_7 = 0, \quad a_2 - a_8 = 0,$$
$$a_0 = a_6, \quad a_1 = a_7, \quad a_2 = a_5, \quad a_3 = a_6, \quad a_4 = a_7, \quad a_2 = a_8,$$
$$a_0 = a_3 = a_6, \quad a_2 = a_5 = a_8, \quad a_1 = a_4 = a_7.$$

Jádro, $\ker(\psi)$, je tedy množina

$$\mathcal{I}_9 = \{circ_9(x, y, z, x, y, z, x, y, z) ; x, y, z \in \mathbb{Q}\}. \tag{4}$$

Nyní můžeme vytvořit faktorový okruh $\mathcal{C}_9/\mathcal{I}_9$. K důkazu, že $\mathcal{C}_9/\mathcal{I}_9$ je těleso, zbývá ukázat, že ideál $\mathcal{I}_9$ je maximální, to znamená, že pokud existuje ideál $\mathcal{J} \subset \mathcal{C}_9$ takový, že $\mathcal{I}_9 \subset \mathcal{J} \subset \mathcal{C}_9$, pak je buď $\mathcal{I}_9 = \mathcal{J}$ nebo $\mathcal{J} = \mathcal{C}_9$.

Nechť tedy nyní je $\mathbf{A} = circ_9(a_0, a_1, \ldots, a_8) \notin \mathcal{I}_9$ a $\mathcal{J}$ je ideál generovaný maticí $\mathbf{A}$ a ideálem $\mathcal{I}_9$. Sestavme matici $\mathbf{A}^\times = circ_9(x, y, z, x, y, z, x, y, z)$, kde x, y, z mají tvar

$$x = \frac{1 - (a_0 + a_3 + a_6)}{3}, \quad y = -\frac{a_1 + a_4 + a_7}{3}, \quad z = -\frac{a_2 + a_5 + a_8}{3}.$$

Dále označme součet $\mathbf{A} + \mathbf{A}^\times$ jako $\mathbf{J}$ a zkoumejme jeho vlastní čísla λ_i, jak bylo popsáno v (1). Pro $i = 0$ jde o součet prvků prvního řádku. Pro matici $\mathbf{J}$ tedy máme

$$\lambda_0 = a_0 + a_1 + \cdots + a_8 + 3x + 3y + 3z = 1.$$

Pro $i = 1$ to je

$$\begin{aligned}\lambda_1 &= (a_0 + x) + (a_1 + y)\zeta_9 + (a_2 + z)\zeta_9^2 + \cdots + (a_8 + z)\zeta_9^8 \\ &= (a_0 + x - a_6 - x) + (a_1 + y - a_7 - y)\zeta_9 + \cdots + (a_5 + z - a_8 - z)\zeta_9^5 \\ &= (a_0 - a_6) + (a_1 - a_7)\zeta_9 + \cdots + (a_5 - a_8)\zeta_9^5.\end{aligned}$$

Protože $\mathbf{A} \notin \mathcal{I}_9$, musí být alespoň jeden z koeficientů λ_1 nenulový, což znamená, že $\lambda_1 \neq 0$. Obdobně můžeme ukázat nenulovost pro všechny λ_i s $\gcd(i, 9) = 1$.

Konečně λ_3 lze vyjádřit jako

$$\begin{aligned}\lambda_1 &= (a_0 + x) + (a_1 + y)\zeta_9^3 + (a_2 + z)\zeta_9^6 + (a_3 + z)\zeta_9^9 + \cdots + (a_8 + z)\zeta_9^{24} \\ &= (a_0 + x) + (a_1 + y)\zeta_9^3 + (a_2 + z)\zeta_9^6 + (a_3 + z) + \cdots + (a_8 + z)\zeta_9^6 \\ &= (a_0 + a_3 + a_6 + 3x) + (a_1 + a_4 + a_7 + 3y)\zeta_9^3 + (a_2 + a_5 + a_8 + 3z)\zeta_9^6.\end{aligned}$$

Odtud vidíme, že $\lambda_3 = 1$. Stejně ukážeme, že také $\lambda_6 = 1$.

Determinant $|\mathbf{J}|$ je tedy nenulový, a proto v okruhu $\mathcal{C}_9$ existuje její inverze $\mathbf{J}^{-1}$. Matici $\mathbf{J}$ jsme uvažovali jako prvek ideálu $\mathcal{J}$ a proto pro každou matici$\mathbf{C} \in \mathcal{C}_9$ musí být součin $\mathbf{C} \cdot \mathbf{J}$ prvkem ideálu $\mathcal{J}$. Specielně tedy $\mathbf{J}^{-1} \cdot \mathbf{J}$ je prvkem $\mathcal{J}$, což ukazuje, že $\mathcal{J} = \mathcal{C}_9$. Ukázali jsme tedy, že $\mathcal{I}_9$ je maximální ideál okruhu $\mathcal{C}_9$ a faktorový okruh $\mathcal{C}_9/\mathcal{I}_9$ je tělesem.

PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020
EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO
Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

Každá třída v $\mathcal{C}_9/\mathcal{I}_9$ obsahuje právě jeden prvek tvaru $circ_9\left(c_0, c_1, \ldots, c_5, 0, 0, 0\right)$, který reprezentuje $\gamma = c_0 + c_1\zeta_9 + \cdots + c_5\zeta_9^5 \in \mathbb{Q}\left(\zeta_9\right)$. Uvažujme, že $\gamma \neq 0$ a $\gamma^{-1} = d_0 + d_1\zeta_9 + \cdots + d_5\zeta_9^5 \in \mathbb{Q}\left(\zeta_9\right)$ je jeho inverzí. Označme $\bar{\mathbf{C}}$ třídu $circ_9\left(c_0, c_1, \ldots, c_5, 0, 0, 0\right)$ a $\bar{\mathbf{D}}$ třídu $circ_9\left(d_0, d_1, \ldots, d_5, 0, 0, 0\right)$, potom jsou tyto třídy inverzemi i ve faktorovém okruhu $\mathcal{C}_9/\mathcal{I}_9$. To znamená, že tělesa $\mathcal{C}_9/\mathcal{I}_9$ a $\mathbb{Q}\left(\zeta_9\right)$ jsou isomorfní, tj. $\mathcal{C}_9/\mathcal{I}_9 \simeq \mathbb{Q}\left(\zeta_9\right)$.

Označme množinu všech cirkulantních matic tvaru $\mathbf{A} = circ_9\left(a_0, a_1, \ldots, a_5, 0, 0, 0\right)$ jako $\mathcal{C}_9^*$. Zjevně $\psi\left(\mathcal{C}_9^*\right) = \mathbb{Q}\left(\zeta_9\right)$ a pro $\mathbf{A}, \mathbf{B} \in \mathcal{C}_9^*$ platí také $\psi\left(\mathbf{A} + \mathbf{B}\right) = \psi\left(\mathbf{A}\right) + \psi\left(\mathbf{B}\right)$. To však nemusí být pravda v případě součinu těchto matic.

Abychom tedy z $\mathcal{C}_9^*$ získali okruh musíme operaci násobení takových matice definovat jinak. Opět tedy uvažujme $\mathbf{A} = circ_9\left(a_0, a_1, \ldots, a_5, 0, 0, 0\right)$ a $\mathbf{B} = circ_9\left(b_0, b_1, \ldots, b_5, 0, 0, 0\right)$ a α, β jako jim odpovídající prvky z tělesa in $\mathbb{Q}\left(\zeta_9\right)$. Definujme součin $\mathbf{A} * \mathbf{B}$ jako

$$\begin{aligned}
&\mathbf{A} * \mathbf{B} = circ_9\left(a_0, a_1, \ldots, a_5, 0, 0, 0\right) * circ_9\left(b_0, b_1, \ldots, b_5, 0, 0, 0\right) = \\
&= circ_9\left(a_0, \ldots, a_5, 0, 0, 0\right) \cdot circ_9\left(b_0, \ldots, b_5, 0, 0, 0\right) - circ_9\left(c_6, c_7, c_8, \ldots, c_6, c_7, c_8\right) = \\
&= circ_9\left(c_0 - c_6, c_1 - c_7, c_2 - c_8, c_3 - c_6, c_4 - c_7, c_5 - c_8, 0, 0, 0\right) \in \mathcal{C}_9^*,
\end{aligned}$$

kde $c_k = \sum_{\substack{i+j \equiv k \\ (\mathrm{mod}\ 9)}} a_i b_j$ jako ve vztahu (3).

S pomocí (3) a (4) lze odvodit a ukázat, že

$$\begin{aligned}
&\psi\left(\mathbf{A} * \mathbf{B}\right) = \psi\left(\mathbf{A} \cdot \mathbf{B} - circ_9\left(c_6, c_7, c_8, c_6, c_7, c_8, c_6, c_7, c_8\right)\right) = \\
&= \psi\left(\mathbf{A} \cdot \mathbf{B}\right) - \psi\left(circ_9\left(c_6, c_7, c_8, c_6, c_7, c_8, , c_6, c_7, c_8\right)\right) = \\
&= \psi\left(\mathbf{A} \cdot \mathbf{B}\right) - 0 = \psi\left(\mathbf{A}\right) \cdot \psi\left(\mathbf{B}\right) = \alpha \cdot \beta \in \mathbb{Q}\left(\zeta_9\right),
\end{aligned}$$

odkud pak dále plyne, že zobrazení ψ zúžené na $\mathcal{C}_9^*$, tj.

$$\psi : \mathcal{C}_9^* \longrightarrow \mathbb{Q}\left(\zeta_9\right), \quad \psi : \mathbf{A} \longmapsto a_0 + a_1\zeta_9 + a_2\zeta_9^2 + \cdots + a_5\zeta_9^5$$

je také homomorfismem. Navíc, protože jeho jádro je triviální, ukázali jsme také, že $(\mathcal{C}_9^*, +, *) \simeq \mathbb{Q}\left(\zeta_9\right)$.

3 REPREZENTACE TĚLESA $\mathbb{Q}\left(\zeta_9\right)$

Isomorfismy a reprezentace prvků $\mathbb{Q}\left(\zeta_9\right)$, které jsme získali v předchozí části, jsou jednoduše odvoditelné, ovšem v některých ohledech nedostatečné. Například reprezentuje-li matice $\mathbf{C} = circ_9\left(c_0, c_1, \ldots, c_5, 0, 0, 0\right)$ prvek $\gamma \in \mathbb{Q}\left(\zeta_9\right)$, pak determinant $|\mathbf{C}|$ není roven normě prvku γ, tj. $\mathrm{N}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}\left(\gamma\right)$. Stejně tak stopa matice $\mathbf{C}$ není rovna stopě prvku γ, tj. $\mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}\left(\gamma\right)$. Také násobení $\mathcal{C}_9^*$ či práce s třídami v $\mathcal{C}_9/\mathcal{I}_9$může být poněkud zdlouhavá.

Nechť tedy nyní je $\alpha = a_0 + a_1\zeta_9 + \cdots + a_5\zeta_9^5 \neq 0$ prvek $\mathbb{Q}\left(\zeta_9\right)$ a $\alpha^{-1} = x_0 + x_1\zeta_9 + \cdots + x_5\zeta_9^5$ je prvek k němu inverzní a uvažujme jim odpovídající matice z tělesa $\mathcal{C}_9^*$, které byly popsány výše. Máme tedy rovnost

$$circ_9\left(a_0, a_1, \ldots, a_5, 0, 0, 0\right) * circ_9\left(x_0, x_1, \ldots, x_5, 0, 0, 0\right) = circ_9\left(1, 0, \ldots, 0\right),$$

PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020

EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

která vede k soustavě lineárních rovnic

$$\begin{aligned}
c_0 - c_6 &= a_0x_0 - a_5x_1 - a_4x_2 - a_3x_3 + (-a_2 + a_5)\,x_4 + (-a_1 + a_4)\,x_5 = 1,\\
c_1 - c_7 &= a_1x_0 + a_0x_1 - a_5x_2 - a_4x_3 - a_3x_4 + (-a_2 + a_5)\,x_5 = 0,\\
c_2 - c_8 &= a_2x_0 + a_1x_1 + a_0x_2 - a_5x_3 - a_4x_4 - a_3x_5 = 0,\\
c_3 - c_6 &= a_3x_0 + (a_2 - a_5)\,x_1 + (a_1 - a_4)\,x_2 + (a_0 - a_3)\,x_3 - a_2x_4 - a_1x_5 = 0,\\
c_4 - c_7 &= a_4x_0 + a_3x_1 + (a_2 - a_5)\,x_2 + (a_1 - a_4)\,x_3 + (a_0 - a_3)\,x_4 - a_2x_5 = 0,\\
c_5 - c_8 &= a_5x_0 + a_4x_1 + a_3x_2 + (a_2 - a_5)\,x_3 + (a_1 - a_4)\,x_4 + (a_0 - a_3)\,x_5 = 0,
\end{aligned}$$

kde $c_k = \sum_{\substack{i+j\equiv k\\ (\mathrm{mod}\ 9)}} a_ix_j$. Zapišme soustavu jako

$$\begin{pmatrix}
a_0 & -a_5 & -a_4 & -a_3 & -a_2+a_5 & -a_1+a_4\\
a_1 & a_0 & -a_5 & -a_4 & -a_3 & -a_2+a_5\\
a_2 & a_1 & a_0 & -a_5 & -a_4 & -a_3\\
a_3 & a_2-a_5 & a_1-a_4 & a_0-a_3 & -a_2 & -a_1\\
a_4 & a_3 & a_2-a_5 & a_1-a_4 & a_0-a_3 & -a_2\\
a_5 & a_4 & a_3 & a_2-a_5 & a_1-a_4 & a_0-a_3
\end{pmatrix}
\begin{pmatrix} x_0\\ x_1\\ x_2\\ x_3\\ x_4\\ x_5 \end{pmatrix}
=
\begin{pmatrix} 1\\ 0\\ 0\\ 0\\ 0\\ 0 \end{pmatrix} \tag{5}$$

a označme $\mathbf{T}_\alpha$ matici soustavy ze vztahu (5).

Každému prvku $\alpha = a_0 + a_1\zeta_9 + \cdots + a_5\zeta_9^5 \in \mathbb{Q}(\zeta_9)$ tak lze přiřadit matici $\mathbf{T}_\alpha$ a vektor $\delta_\alpha = (a_0, a_1, \ldots, a_5)$. Označme $\mathcal{C}_\mathbf{T}$ množinu všech matic $\mathbf{T}_\alpha$, tj. $\mathcal{C}_\mathbf{T} = \{\mathbf{T}_\alpha; \alpha \in \mathbb{Q}(\zeta_9)\}$. S tímto značením máme

Věta 1. *Pro matici $\mathbf{T}_\alpha$ a $\mathcal{C}_\mathbf{T}$ platí:*

1. $\mathcal{C}_\mathbf{T} \simeq \mathbb{Q}(\zeta_9)$,
2. $\mathbf{T}_\alpha \cdot \delta_\beta = \delta_{\alpha\cdot\beta}$,
3. $\mathrm{N}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\alpha) = |\mathbf{T}_\alpha|$,
4. $\mathrm{Tr}_{\mathbb{Q}(\zeta_9)/\mathbb{Q}}(\alpha) = \mathrm{Tr}(\mathbf{T}_\alpha)$.

Důkaz. Násobení prvkem α definuje na $\mathbb{Q}(\zeta_9)$ $\mathbb{Q}$-lineární transformaci

$$t_\alpha : \mathbb{Q}(\zeta_9) \longrightarrow \mathbb{Q}(\zeta_9), \quad x \longmapsto \alpha x.$$

Matice $\mathbf{T}_\alpha$ je reprezentací této transformace vzhledem k celé mocninné bázi $1, \zeta_9, \ldots, \zeta_9^5$. Odsud vztahy 3, 4 plynou jako definice normy a stopy v rozšíření $\mathbb{Q}(\zeta_9)/\mathbb{Q}$. Zbytek plyne z úvah provedených výše. □

PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020
EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO
Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

4 REPREZENTACE PODTĚLES TĚLESA $\mathbb{Q}(\zeta_9)$

Abychom získali reprezentaci podtěles $\mathbb{Q}(\zeta_9)$ využijeme opět rovnic (5), ovšem tentokrát s prvky uvažovaného podtětelasa. Jak již bylo v úvodu zmíněno, Galoisova grupa rozšíření $\mathbb{Q}(\zeta_9)/\mathbb{Q}$ je isomorfní s multiplikativní grupou $\mathbb{Z}_9^\times$. Tato grupa má dvě podgrupy a tedy těleso $\mathbb{Q}(\zeta_9)$ má dvě podtělesa. Podgrupy jsou $(\{1,4,7\},\cdot)$ a $(\{1,8\},\cdot)$ a jim odpovídající tělesa jsou $\mathbb{Q}(\zeta_3)$ a $\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)$.

4.1 Těleso $\mathbb{Q}(\zeta_3)\subset\mathbb{Q}(\zeta_9)$

Těleso $\mathbb{Q}(\zeta_3)$ je zjevně podtělesem $\mathbb{Q}(\zeta_9)$, neboť platí $\zeta_9^3=\zeta_3$. Jeho báze je tvořena prvky $1,\zeta_3$ a každý jeho prvek $\alpha\in\mathbb{Q}(\zeta_3)$ lze zapsat ve tvaru $\alpha=a_0+a_1\zeta_3=a_0+a_1\zeta_9^3$. Soustava rovnic (5) se po dosazení $(a_0,0,0,a_1,0,0)$ a $(x_0,0,0,x_1,0,0)$ změní na

$$\begin{pmatrix} a_0 & 0 & 0 & -a_1 & 0 & 0\\ 0 & a_0 & 0 & 0 & -a_1 & 0\\ 0 & 0 & a_0 & 0 & 0 & -a_1\\ a_1 & 0 & 0 & a_0-a_1 & 0 & 0\\ 0 & a_1 & 0 & 0 & a_0-a_1 & 0\\ 0 & 0 & a_1 & 0 & 0 & a_0-a_1 \end{pmatrix}\begin{pmatrix} x_0\\0\\0\\x_1\\0\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\\0\\0\end{pmatrix}.$$

Nový systém obsahuje pouze dvě lineárně nezávislé rovnice a můžeme jej přepsat do tvaru

$$\begin{pmatrix} a_0 & -a_1\\ a_1 & a_0-a_1\end{pmatrix}\begin{pmatrix}x_0\\x_1\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}. \tag{6}$$

Označíme-li $\mathbf{T}_{\alpha,\mathbb{Q}(\zeta_3)}$ matici soustavy (6) a $\delta_{\alpha,\mathbb{Q}(\zeta_3)}=(a_0,a_1)$, dostaneme požadovanou reprezentaci prvků $\alpha=a_0+a_1\zeta_3\in\mathbb{Q}(\zeta_3)$.

4.2 Těleso $\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)\subset\mathbb{Q}(\zeta_9)$

V případě tělesa $\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)$, maximálního reálného podtělesa $\mathbb{Q}(\zeta_9)$, je situace komplikována faktem, že toto těleso má pouze celou mocninnou bázi tvořenou prvky $1,\left(\zeta_9+\zeta_9^{-1}\right),\left(\zeta_9+\zeta_9^{-1}\right)^2$, takže každý prvek $\alpha\in\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)$ píšeme ve tvaru

$$\alpha=a_0+a_1\left(\zeta_9+\zeta_9^{-1}\right)+a_2\left(\zeta_9+\zeta_9^{-1}\right)^2 \text{ s } a_0,a_1,a_2\in\mathbb{Q}.$$

Abychom však mohli využít (5), musíme α vyjádřit vzhledem k celé mocninné bázi $1,\zeta_9,\zeta_9^2,\ldots,\zeta_9^5$ tělesa $\mathbb{Q}(\zeta_9)$, to znamená psát

$$\begin{aligned}\zeta_9+\zeta_9^{-1}&=\zeta_9+\zeta_9^8=\zeta_9-\zeta_9^2-\zeta_9^5,\\ \left(\zeta_9+\zeta_9^{-1}\right)^2&=\zeta_9^2+2+\zeta_9^{16}=2+\zeta_9^2+\zeta_9^7=2-\zeta_9+\zeta_9^2-\zeta_9^4,\end{aligned}$$

a tedy

$$\alpha=(a_0+2a_2)+(a_1-a_2)\zeta_9-(a_1-a_2)\zeta_9^2-a_2\zeta_9^4-a_1\zeta_9^5. \tag{7}$$

PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020
EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO
Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

S koeficienty α jako v (7) přejde soustava (5) do tvaru

$$\begin{pmatrix} a_0+2a_2 & a_1 & a_2 & 0 & -a_2 & -a_1 \\ a_1-a_2 & a_0+2a_2 & a_1 & a_2 & 0 & -a_2 \\ a_2-a_1 & a_1-a_2 & a_0+2a_2 & a_1 & a_2 & 0 \\ 0 & a_2 & a_1 & a_0+2a_2 & a_1-a_2 & a_2-a_1 \\ -a_2 & 0 & a_2 & a_1 & a_0+2a_2 & a_1-a_2 \\ -a_1 & -a_2 & 0 & a_2 & a_1 & a_0+2a_2 \end{pmatrix} \begin{pmatrix} x_0+2x_2 \\ x_1-x_2 \\ -x_1+x_2 \\ 0 \\ -x_2 \\ -x_1 \end{pmatrix} =$$

$$= \begin{pmatrix} a_0+2a_2 & 2a_1-a_2 & 2a_0-a_1+6a_2 \\ a_1-a_2 & a_0-a_1+3a_2 & -a_0+3a_1-4a_2 \\ a_2-a_1 & -a_0+a_1-3a_2 & a_0-3a_1+4a_2 \\ 0 & 0 & 0 \\ -a_2 & -a_1 & -a_0-3a_2 \\ -a_1 & -a_0-3a_2 & a_2-3a_1 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Rovnice v novém systému jsou lineárně závislé, hodnost matice soustavy je 3, a použitím Gaussovy eliminace, odečtením řádků 5 a 6 od řádků $1, 2, 3$, dostáváme soustavu v následujícím tvaru a z ní reprezentující matici $\mathbf{T}_{\alpha,\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)}$

$$\begin{pmatrix} a_0 & -a_2 & -a_1 \\ a_1 & a_0+3a_2 & 3a_1-a_2 \\ a_2 & a_1 & a_0+3a_2 \\ 0 & 0 & 0 \\ -a_2 & -a_1 & -a_0-3a_2 \\ -a_1 & -a_0-3a_2 & a_2-3a_1 \end{pmatrix} \rightarrow \mathbf{T}_{\alpha,\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)} = \begin{pmatrix} a_0 & -a_2 & -a_1 \\ a_1 & a_0+3a_2 & 3a_1-a_2 \\ a_2 & a_1 & a_0+3a_2 \end{pmatrix} \tag{8}$$

4.3 Reprezentace podtěles

Nechť K je podtěleso $\mathbb{Q}(\zeta_9)$, tj. $\mathbb{Q}(\zeta_3)$ nebo $\mathbb{Q}\left(\zeta_9+\zeta_9^{-1}\right)$, dále nechť $\mathbf{T}_{\alpha,K}$ a $\delta_{\alpha,K}$ jsou jako v (6) resp. v (8), a konečně $\mathcal{C}_{\mathbf{T},K} = \{\mathbf{T}_{\alpha,K}; \alpha \in K\}$ značí množiny všech takových matic, potom

Věta 2. *Pro matice $\mathbf{T}_{\alpha,K}$ a $\mathcal{C}_{\mathbf{T},K}$ platí:*

1. $\mathcal{C}_{\mathbf{T},K} \simeq K$,
2. $\mathbf{T}_{\alpha,K} \cdot \delta_{\beta,K} = \delta_{\alpha\cdot\beta,K}$,
3. $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = |\mathbf{T}_{\alpha,K}|$,
4. $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}(\mathbf{T}_{\alpha,K})$.

Důkaz. V důkazu postupujeme stejně jako v důkazu Věty 1. □

PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020

EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

5 PŘÍKLAD

Uvažujme těleso $K = \mathbb{Q}\left(\zeta_9 + \zeta_9^{-1}\right)$ a označme prvky jeho báze jako $\varepsilon_1 = 1, \varepsilon_2 = \zeta_9 + \zeta_9^{-1}$ and $\varepsilon_3 = \varepsilon_2^2 = \left(\zeta_9 + \zeta_9^{-1}\right)^2$, odpovídající matice $\mathbf{T}$ a vektory δ jsou

$$\mathbf{T}_{\varepsilon_1,K} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \delta_{\varepsilon_1,K} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix},$$

$$\mathbf{T}_{\varepsilon_2,K} = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & 3 \\ 0 & 1 & 0 \end{pmatrix}, \quad \delta_{\varepsilon_2,K} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix},$$

$$\mathbf{T}_{\varepsilon_3,K} = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 3 & -1 \\ 1 & 0 & 3 \end{pmatrix}, \quad \delta_{\varepsilon_3,K} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}.$$

Prvek ε_2^3 můžeme vyjádřit například jako $\mathbf{T}_{\varepsilon_2,K} \cdot \delta_{\varepsilon_3,K}$ nebo $\mathbf{T}_{\varepsilon_3,K} \cdot \delta_{\varepsilon_2,K}$, v obou případech obdržíme samozřejmě stejný výsledek $(-1, 3, 0)$. Odtud vidíme, že $\varepsilon_2^3 = -1+3\varepsilon_2$ a dále $\varepsilon_2^3 - 3\varepsilon_2 + 1 = 0$. Tímto jsme také nalezli minimální polynom prvku $\zeta_9 + \zeta_9^{-1}$ a tělesa $\mathbb{Q}\left(\zeta_9 + \zeta_9^{-1}\right)$, který má tvar $x^3 - 3x + 1$.

Pro $\alpha = 3 + 2\left(\zeta_9 + \zeta_9^{-1}\right) + \left(\zeta_9 + \zeta_9^{-1}\right)^2 \in K$ máme

$$\mathbf{T}_{\alpha,K} = 3\mathbf{T}_{\varepsilon_1,K} + 2\mathbf{T}_{\varepsilon_2,K} + \mathbf{T}_{\varepsilon_3,K} = \begin{pmatrix} 3 & -1 & 2 \\ 2 & 6 & 5 \\ 1 & 2 & 6 \end{pmatrix}.$$

Dále můžeme například spočíst $\mathrm{N}_{K/\mathbb{Q}}(\alpha) = |\mathbf{T}_{\alpha,K}| = 89$, $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \mathrm{Tr}(\mathbf{T}_{\alpha,K}) = 15$ či α^2 jako

$$\mathbf{T}_{\alpha,K} \cdot \delta_{\alpha,K} = \begin{pmatrix} 3 & -1 & -2 \\ 2 & 6 & 5 \\ 1 & 2 & 6 \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \\ 1 \end{pmatrix} = (5, 23, 13),$$

tj. $\alpha^2 = 5 + 23\left(\zeta_9 + \zeta_9^{-1}\right) + 13\left(\zeta_9 + \zeta_9^{-1}\right)^2$.

Všechny zde provedené výpočty byly jednoduše proveditelné, protože využívají pouze základní maticové operace namísto aritmetiky těles algebraických čísel.

LITERATURA

1. J. Kostra. "A Note on Representation of Cyclotomic Fields", *Acta Mathematica et Informatica Universitatis Ostraviensis*, Vol. 4, 1996, p. 29–35.

2. M. Pomp, R. Havelek. "On representation of cyclotomic fields $\mathbb{Q}(\zeta_{pq})$", *Acta Mathematica et Informatica Universitatis Ostraviensis*, Vol. 7, 1999, p. 71–78.

PŘEKRAČUJEME HRANICE
PRZEKRACZAMY GRANICE
2014—2020

EVROPSKÁ UNIE / UNIA EUROPEJSKA
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
EUROPEJSKI FUNDUSZ ROZWOJU REGIONALNEGO

Projekt jest współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego oraz z budżetu państwa RP
"Przekraczamy Granice"

CIRKULANTNÍ MATICE STUPNĚ 9

Abstrakt: *Cirkulantní matice nabízí širokou škálu aplikací v mnoha různých odvětvích matematiky, jako jsou analýza dat a časový řad, zpracování signálů či Fourierova transformace.*
Další výsledky využívající vlastností cirkulantních matic můžeme nalézt v algebraické teorii čísel, což je dáno tím, že z okruhu cirkulantních matic prvočíselného stupně p, lze vytvořit faktorový okruh isomorfní s p-tým cyklotomickým tělesem, $\mathbb{Q}(\zeta_p)$.
V článku je ukázán vztah mezi okruhem cirkulantních matic stupně 9, $\mathcal{C}_9$, a devátým cyklotomickým tělesem.

Klíčová slova: *cirkulantní matice, cyklotomické těleso*

A NOTE ON CIRCULANT MATRICES OF DEGREE 9

Abstract: *Circulant matrices provide quite a wide range of applications in many different branches of mathematics, such as data and time-series analysis, signal processing or Fourier transformation.*
Huge number of results concerning circulant matrices can be found in algebraic number theory. This is because we can construct factor ring isomorphic to the p-th cyclotomic field $\mathbb{Q}(\zeta_p)$ from the ring of circulant matrices degree p, where p is a prime.
In this paper the connection between ring of circulant matrices of degree 9, $\mathcal{C}_9$, and the cyclotomic field $\mathbb{Q}(\zeta_9)$ is shown.

Keywords: *circulant matrix, cyclotomic field*

Datum odeslání článku do redakce: 04.2017
Datum přijetí článku redakcí: 05.2017

RNDr. Viktor DUBOVSKÝ, Ph.D.,
VŠB - Technická univerzita Ostrava
Katedra matematiky a deskriptivní geometrie
17. listopadu 15, 708 33, Ostrava, Česká republika
tel.: +420 597 324 152, e-mail: viktor.dubovsky@vsb.cz