Pokroky matematiky, fyziky a astronomie

Matěj Doležálek

Kvaterniony a důkaz Lagrangeovy věty o čtyřech čtvercích

Pokroky matematiky, fyziky a astronomie, Vol. 64 (2019), No. 3, 145–160

Persistent URL: http://dml.cz/dmlcz/147884

Kvaterniony a důkaz Lagrangeovy věty o čtyřech čtvercích

Matěj Doležálek

Abstrakt. Článek představuje užití kvaternionů k důkazu Lagrangeovy věty o čtyřech čtvercích a použití stejných myšlenek k důkazům univerzálnosti dalších kvadratických forem. Užito je vlastností normy a ideálů v jistých kvaternionových oborech.

Lagrangeovu větu o čtyřech čtvercích dokázal poprvé v roce 1770 Joseph-Louis Lagrange. Zní:

Každé přirozené číslo lze zapsat jako součet čtyř čtverců celých čísel.

Historie tohoto tvrzení je však delší. Před jeho důkazem bylo známo jako *Bachetova domněnka*, podle Clauda Gasparda Bacheta de Méziriac, který roku 1621 ve svém latinském překladu Diofantovy *Aritmetiky* poznamenal, že Diofantos toto tvrzení zdánlivě zná a předpokládá. Zatímco původní Lagrangeův důkaz využíval pouze elementárních nástrojů, v tomto článku představíme důkaz pocházející od Adolfa Hurwitze, který využívá algebraických vlastností kvaternionů. Ukážeme také, že zobecněním jeho postupu lze i o mnoha dalších kvadratických formách (homogenních kvadratických polynomech s celočíselnými koeficienty) dokázat, že jsou univerzální (při dosazování celých čísel jsou jejich hodnotami všechna přirozená čísla) – viz tabulku 1.

$x^2+y^2+z^2+w^2$	$(x^2+2y^2)+(yz-xw)+2(z^2+2w^2)$
$(x^2+xy+y^2)+(z^2+zw+w^2)$	$(x^2+xy+y^2)+(yz-xw)+2(z^2+zw+w^2)$
$(x^2+xy+y^2)+2(z^2+zw+w^2)$	$(x^2+xy+2y^2)+(yz-xw)+(z^2+zw+2w^2)$
$(x^2+xy+2y^2)+(z^2+zw+2w^2)$	$(x^2+xy+2y^2)+2(yz-xw)+2(z^2+zw+2w^2)$
$(x^2+xy+2y^2)+2(z^2+zw+2w^2)$	$(x^2+xy+3y^2)+3(yz-xw)+2(z^2+zw+3w^2)$
$(x^2+xy+3y^2)+2(z^2+zw+3w^2)$	$(x^2+xy+y^2)+(yz-xw)+(z^2+zw+w^2)$
$(x^2+xy+2y^2)+3(z^2+zw+2w^2)$	$(x^2+xy+3y^2)+(yz-xw)+(z^2+zw+3w^2)$
$(x^2+xy+5y^2)+2(z^2+zw+5w^2)$	$(x^2+xy+5y^2)+2(yz-xw)+2(z^2+zw+5w^2)$

Tab. 1. Některé kvadratické formy, jejichž univerzálnost lze dokázat pomocí kvaternionů

1. Hurwitzovy kvaterniony

Kvaterniony mají tvar $\theta = x + y\mathrm{i} + z\mathrm{j} + w\mathrm{k}$, kde x, y, z, $w \in \mathbb{R}$ a i, j, k splňují

$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = \mathrm{ijk} = -1.$$

(Obecněji lze kvaterniony definovat nad libovolným okruhem.)

Matěj Doležálek, Gymnázium dr. A. Hrdličky, Komenského 147, 396 01 Humpolec, e-mail: matej.dolezalek.271828@gmail.com

Pro kvaternion θ definujeme jeho *sdružený kvaternion* $\overline{\theta} = x - y\mathrm{i} - z\mathrm{j} - w\mathrm{k}$ a jeho *normu*

$$N(\theta) = \theta\overline{\theta} = \overline{\theta}\theta = x^2 + y^2 + z^2 + w^2.$$

Množinu všech kvaternionů značme $\mathbb{H}(\mathbb{R})$.

Připomeňme nejzákladnější vlastnosti kvaternionů. Zaprvé jejich násobení obecně není komutativní (např. $\mathrm{ij} = \mathrm{k}$, ale $\mathrm{ji} = -\mathrm{k}$), nicméně je asociativní a distributivní vzhledem ke sčítání (zleva i zprava). Dále pro $\alpha, \beta \in \mathbb{H}(\mathbb{R})$ platí $\overline{(\alpha\beta)} = \overline{\beta} \cdot \overline{\alpha}$, z čehož potom plyne

$$N(\alpha\beta) = \alpha\beta \cdot \overline{(\alpha\beta)} = \alpha\beta \cdot \overline{\beta}\overline{\alpha} = N(\alpha)N(\beta).$$

Zaveďme nyní množiny

$$\begin{aligned} \mathbb{H}(\mathbb{Z}) &= \{a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k} : a, b, c, d \in \mathbb{Z}\}, \\ \mathbb{J} &= \left\{ \frac{a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}}{2} : a, b, c, d \in \mathbb{Z} \wedge a \equiv b \equiv c \equiv d \pmod 2 \right\}. \end{aligned}$$

Prvky množiny $\mathbb{H}(\mathbb{Z})$ nazývejme *celočíselnými kvaterniony*[1]. Účel jejich zkoumání je zjevný – Lagrangeova věta hovoří o součtech čtyř čtverců celých čísel, což jsou ale přesně normy prvků $\mathbb{H}(\mathbb{Z})$. Méně zjevný účel může mít zavedení $\mathbb{J}$. Důvodem je to, že $\mathbb{J}$ má mnohé užitečné vlastnosti, které $\mathbb{H}(\mathbb{Z})$ postrádá.

Prvky $\mathbb{J}$ nazývejme *Hurwitzovými kvaterniony*. Označíme-li $\zeta = \frac{1+\mathrm{i}+\mathrm{j}+\mathrm{k}}{2}$, lze $\mathbb{J}$ přepsat jako

$$\{a\zeta + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}\colon a, b, c, d \in \mathbb{Z}\},$$

z čehož už lze snadno ověřit, že Hurwitzovy kvaterniony jsou uzavřené na násobení (platí $\theta_1\theta_2 \in \mathbb{J}$ pro každá dvě $\theta_1, \theta_2 \in \{\zeta, \mathrm{i}, \mathrm{j}, \mathrm{k}\}$). Všimněme si též, že všechny Hurwitzovy kvaterniony mají celočíselné normy – to plyne např. z toho, že z uzavřenosti na násobení musí být $N(\theta) = \theta \cdot \overline{\theta} \in \mathbb{J}$, ale přitom také $N(\theta) \in \mathbb{R}$, takže

$$N(\theta) \in \mathbb{J} \cap \mathbb{R} = \mathbb{Z}.$$

Dále dokažme dvě užitečné vlastnosti Hurwitzových kvaternionů.

Věta 1. *Pro libovolná nenulová $\alpha, \beta \in \mathbb{J}$ existuje $\gamma \in \mathbb{J}$ takové, že*

$$N(\alpha - \gamma\beta) < N(\beta).$$

Důkaz. Položíme-li $\varphi = \frac{\alpha\overline{\beta}}{N(\beta)}$, platí v $\mathbb{H}(\mathbb{R})$ rovnost

$$\alpha = \varphi\beta.$$

Budiž $\varphi = a + b\mathrm{i} + c\mathrm{j} + d\mathrm{k}$ a zvolme $e, f, g, h \in \mathbb{Z}$ tak, že

$$|a - e|, |b - f|, |c - g|, |d - h| \leqq \frac{1}{2}$$

[1] Nazývají se též *Lipschitzovými kvaterniony*.

– to jistě lze (jednoduše zaokrouhlíme a, b, c, d vždy na nejbližší celé číslo). Budiž potom $\gamma = e + f\mathrm{i} + g\mathrm{j} + h\mathrm{k}$ (tedy $\gamma \in \mathbb{H}(\mathbb{Z}) \subset \mathbb{J}$) a položme

$$\delta = \alpha - \gamma\beta = (\varphi - \gamma)\beta.$$

Nyní je $N(\delta) = N(\varphi - \gamma)N(\beta)$. Přitom

$$N(\varphi - \gamma) = |a-e|^2 + |b-f|^2 + |c-g|^2 + |d-h|^2 \leqq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1.$$

Pokud v předchozí nerovnosti nenastane rovnost, pak jsme hotovi, neboť potom nutně $N(\delta) < N(\beta)$. Pokud rovnost nastane, pak musí být

$$|a-e| = |b-f| = |c-g| = |d-h| = \frac{1}{2},$$

což ale znamená $\varphi = \gamma + \frac{\pm 1 \pm \mathrm{i} \pm \mathrm{j} \pm \mathrm{k}}{2}$ pro nějakou volbu znamének, neboli $\varphi \in \mathbb{J}$. Protože $\alpha = \varphi\beta$, namísto původní volby γ stačí zvolit $\gamma' = \varphi$. □

Lemma 2. *Pro libovolné prvočíslo p existuje $\theta \in \mathbb{J}$ takové, že $N(\theta)$ je násobkem p, ale nikoliv p^2.*

Důkaz. Pro $p = 2$ máme triviálně $N(1 + \mathrm{i}) = 2$, tudíž nadále uvažujme p liché.

Nechť $\mathbb{Z}_p$ značí množinu zbytkových tříd mod p, dále položme $S = \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$. Pro $x \in S$ výraz $x^2 \pmod p$ nabývá $\frac{p+1}{2}$ různých hodnot, neboť pro nenulová $x_1, x_2 \in S$ díky $0 < x_1 + x_2 \leqq p - 1 < p$ (tedy $p \nmid x_1 + x_2$) z $x_1^2 \equiv x_2^2 \pmod p$ plyne

$$\begin{aligned} x_1^2 - x_2^2 &\equiv 0 \pmod p, \\ (x_1 - x_2)(x_1 + x_2) &\equiv 0 \pmod p, \\ x_1 - x_2 &\equiv 0 \pmod p, \\ x_1 &\equiv x_2 \pmod p, \end{aligned}$$

zatímco $x^2 \equiv 0 \pmod p$, právě pokud $x \equiv 0 \pmod p$. Obdobně pro $y \in S$ výraz $-y^2 - 1 \pmod p$ nabývá taktéž $\frac{p+1}{2}$ různých hodnot. Označíme-li tedy

$$U = \{x^2 \pmod p \colon x \in S\}, \qquad V = \{-y^2 - 1 \pmod p \colon y \in S\},$$

platí $|U| + |V| = p + 1 > p = |\mathbb{Z}_p|$ a zároveň $U, V \subseteq \mathbb{Z}_p$, čímž z Dirichletova principu nejsou U, V disjunktní. Existují tedy $x, y \in S$ taková, že

$$\begin{aligned} x^2 &\equiv -y^2 - 1 \pmod p, \\ x^2 + y^2 + 1 &\equiv 0 \pmod p. \end{aligned}$$

Máme tak $N(1 + x\mathrm{i} + y\mathrm{j}) = mp$ pro

$$m = \frac{x^2 + y^2 + 1}{p} \leqq \frac{2 \cdot \left(\frac{p-1}{2}\right)^2 + 1}{p} < \frac{2 \cdot \frac{p^2}{4} + 1}{p} \leqq \frac{\frac{3}{4}p^2}{p} \leqq \frac{3}{4}p < p,$$

přitom jistě $x^2 + y^2 + 1 \geqq 1 > 0$. Z toho dohromady $p \nmid m$, čímž je důkaz hotov. □

2. Ideály a eukleidovské obory

Abychom byli schopni pomocí Hurwitzových kvaternionů dokázat Lagrangeovu větu, zaveďme několik pojmů z teorie okruhů. *Oborem* rozumějme okruh s operacemi $+$, $\cdot$, v němž je součin dvou nenulových prvků vždy nenulový.

Definice 3. Budiž R obor. Neprázdnou množinu $I \subseteq R$ nazvěme *levým ideálem* R, pokud pro každá x, $y \in I$ a $r \in R$ platí $x + y \in I$ a zároveň $r \cdot x \in I$. Levý ideál nazvěme *hlavním*, pokud je tvaru $Ra = \{ra\colon r \in R\}$ pro nějaké $a \in R$. Obor R, v němž jsou všechny levé ideály hlavní, nazvěme *levým oborem hlavních ideálů*.

Rozmysleme si dvě jednoduchá pozorování o ideálech v oboru. Zaprvé pro ideály I, J je jejich součet $I + J$, tj. množina

$$\{x + y\colon x \in I, y \in J\},$$

vždy opět ideálem. Zadruhé jsou dva hlavní ideály Ra, Rb totožné právě tehdy, pokud $a = ub$ pro nějakou jednotku u (prvek, který je dělitelem prvku 1).

Definice 4. Obor R nazvěme *zleva eukleidovským*, pokud existuje funkce $d\colon R \to \mathbb{N}_0$ taková, že pro každá nenulová a, $b \in R$ existují x, $y \in R$ splňující

$$a = xb + y, \qquad d(y) < d(b).$$

Původ označení (zleva) eukleidovského oboru je prostý: definice říká, že v takovýchto oborech lze sestrojit obdobu Eukleidova algoritmu k nalezení největšího (pravého) společného dělitele a, b (největšího ve smyslu hodnoty funkce d). Všimněme si, že větou 1 jsme dokázali, že $\mathbb{J}$ je zleva eukleidovský obor. Ukažme nyní, že každý zleva eukleidovský obor je levým oborem hlavních ideálů.

Lemma 5. *Budiž R zleva eukleidovský obor a budiž I jeho levý ideál. Potom je I hlavní.*

Důkaz. Pokud $I = \{0\}$, dokazované tvrzení platí – nadále tedy předpokládejme $I \neq \{0\}$. Uvažujme funkci d popsanou v definici 4. Zvolme $g \in I \setminus \{0\}$ tak, že $d(g)$ je minimální. Dále mějme libovolné $s \in I \setminus \{0\}$. Pro spor nechť $s \notin Rg$ – potom z definice zleva eukleidovského okruhu existují x, y taková, že

$$s = xg + y, \qquad d(y) < d(g).$$

Z uzavřenosti levého ideálu na násobení prvkem R zleva a na sčítání je $y = s - xg \in I$. Pokud by bylo $y = 0$, znamenalo by to $s = xg \in Rg$, což neplatí. Je tedy $y \in I \setminus \{0\}$ a zároveň $d(y) < d(g)$. To je spor s tím, jak bylo zvoleno g, tudíž pro každé $s \in I \setminus \{0\}$ musí platit $s \in Rg$. Vzhledem k $0 = 0 \cdot g \in Rg$ pak tedy $I \subseteq Rg$. Z definice ideálu ale $Rg \subseteq I$, čili dohromady $I = Rg$. □

Pomocí hlavních ideálů ve zleva eukleidovkém oboru R lze nyní vztah „g je největším společným pravým dělitelem a, b“ zapsat jako $Ra + Rb = Rg$.

3. Lagrangeova věta

Představme nyní Hurwitzův důkaz Lagrangeovy věty. Využijeme vlastností ideálů ke zkoumání ireducibilních prvků, tj. prvků, které nejsou jednotkami a nelze je vyjádřit jako součin dvou nejednotek. V průběhu důkazu pozorujme, že využíváme pouze následujících pět vlastností oboru $\mathbb{J}$:

(i) $\mathbb{Z} \subseteq \mathbb{J} \subseteq \mathbb{H}(\mathbb{R})$.

(ii) $\mathbb{J}$ tvoří se sčítáním a násobením kvaternionů obor.

(iii) $N(\theta) \in \mathbb{N}_0$ pro každé $\theta \in \mathbb{J}$.

(iv) Pro každé prvočíslo p existuje $\theta \in \mathbb{J}$ takové, že $N(\theta)$ je násobkem p, ale nikoliv p^2 (lemma 2).

(v) $\mathbb{J}$ je levým oborem hlavních ideálů.

Lemma 6. *Kvaternion $\varepsilon \in \mathbb{J}$ je jednotkou, právě když $N(\varepsilon) = 1$.*

Důkaz. Pokud $N(\varepsilon) = 1$, pak $\varepsilon\overline{\varepsilon} = 1$, přičemž z

$$\varepsilon + \overline{\varepsilon} = (\varepsilon + 1)(\overline{\varepsilon} + 1) - \varepsilon\overline{\varepsilon} - 1 = N(\varepsilon + 1) - N(\varepsilon) - 1 \in \mathbb{Z} \subseteq \mathbb{J}$$

je i $\overline{\varepsilon} \in \mathbb{J}$, takže je ε jednotkou. Naopak, pokud je ε jednotkou, pak existuje $\varphi \in \mathbb{J}$ takové, že $\varepsilon\varphi = 1$. Potom ale znormováním díky $N(\varepsilon)$, $N(\varphi) \in \mathbb{N}_0$ nutně $N(\varepsilon) = N(\varphi) = 1$. □

Věta 7. *Pro libovolná nenulová $\theta \in \mathbb{J}$, $m \in \mathbb{Z}$ nechť je g největší společný dělitel čísel m, $N(\theta)$. Potom platí $\mathbb{J}\theta + \mathbb{J}m = \mathbb{J}\lambda$ pro nějaké $\lambda \in \mathbb{J}$ splňující $g \mid N(\lambda)$.*

Důkaz. $\mathbb{J}\theta + \mathbb{J}m$ je levým ideálem $\mathbb{J}$, tudíž musí být hlavní, neboli roven $\mathbb{J}\lambda$ pro nějaké $\lambda \in \mathbb{J}$. Platnost $\mathbb{J}\theta + \mathbb{J}m = \mathbb{J}\lambda$ speciálně implikuje existenci α, $\beta \in \mathbb{J}$ takových, že

$$\begin{aligned} \alpha\theta + \beta m &= \lambda, \\ \alpha\theta &= \lambda - \beta m. \end{aligned}$$

Použitím normy na obou stranách pak dostaneme

$$\begin{aligned} N(\alpha)N(\theta) &= (\lambda - \beta m)\overline{(\lambda - \beta m)} = (\lambda - \beta m)(\overline{\lambda} - \overline{\beta}m) = \\ &= N(\lambda) - m(\beta\overline{\lambda} + \lambda\overline{\beta}) + m^2 N(\beta). \end{aligned} \tag{1}$$

Platí

$$\begin{aligned} \beta\overline{\lambda} + \lambda\overline{\beta} &= (\beta\overline{\beta} + \beta\overline{\lambda} + \lambda\overline{\beta} + \lambda\overline{\lambda}) - \beta\overline{\beta} - \lambda\overline{\lambda} = \\ &= (\beta + \lambda) \cdot \overline{(\beta + \lambda)} - \beta\overline{\beta} - \lambda\overline{\lambda} = N(\beta + \lambda) - N(\beta) - N(\lambda), \end{aligned}$$

což je z podmínky (iii) celé číslo. V rovnosti (1) tak vystupují celá čísla, tedy přechodem ke zbytkům mod g obdržíme

$$0 \equiv N(\lambda) \pmod{g}.$$

□

Věta 8. *Mějme ireducibilní $\pi \in \mathbb{J}$ a uvažujme libovolné prvočíslo p, jež dělí $N(\pi)$. Potom $p \in \mathbb{J}\pi$.*

Důkaz. Pro spor nechť $p \notin \mathbb{J}\pi$. Nechť je $\mathbb{J}\pi + \mathbb{J}p = \mathbb{J}\lambda$ – podle věty 7 potom p jako největší společný dělitel p, $N(\pi)$ dělí $N(\lambda)$, neboli λ není jednotkou. Platí $\pi \in \mathbb{J}\lambda$, neboli $\pi = \alpha\lambda$ pro nějaké $\alpha \in \mathbb{J}$. Dále je $p \in \mathbb{J}\lambda$, ale zároveň $p \notin \mathbb{J}\pi$, takže určitě $\mathbb{J}\pi \neq \mathbb{J}\lambda$, a tudíž α není jednotkou. Vyjádřili jsme tedy π jako součin dvou nejednotek – musí tak být reducibilní, což je spor. □

Věta 9. *Libovolné prvočíslo p je v $\mathbb{J}$ reducibilní.*

Důkaz. Z lemmatu 2 existují $n \in \mathbb{N}$, $\theta \in \mathbb{J}$ splňující $p \nmid n$ a zároveň $N(\theta) = np$. Zvolme nejmenší přirozené n s touto vlastností a uvažujme příslušné θ – to pak uvážením normy nemůže být jednotkou. Pro spor nechť je p ireducibilní v $\mathbb{J}$. Potom musí být $n > 1$, neboť jinak $p = \theta\overline{\theta}$, což by značilo reducibilitu p.

Ukažme, že θ je reducibilní. Nechť je pro spor ireducibilní – potom dle věty 8 platí $p \in \mathbb{J}\theta$, neboli existuje $\eta \in \mathbb{J}$ splňující $p = \eta\theta$. Použitím normy na obou stranách obdržíme

$$\begin{aligned} p^2 &= N(\eta) \cdot np, \\ p &= n \cdot N(\eta) = n\eta\overline{\eta}. \end{aligned}$$

Z ireducibility p musí právě dvě z $n, \eta, \overline{\eta}$ být jednotkami. Přitom ale vzhledem k $N(\eta) = N(\overline{\eta})$ je η jednotkou, právě pokud je jí $\overline{\eta}$. Obě $\eta, \overline{\eta}$ nemohou být nejednotkami, jsou tedy obě jednotkami. Z toho

$$p = nN(\eta) = n.$$

Přitom ale máme $p \nmid n$ – tedy spor.

θ je reducibilní, neboli platí $\theta = \theta_1\theta_2$ pro nějaké nejednotky $\theta_1, \theta_2 \in \mathbb{J}$. Zřejmě právě jedna z norem $N(\theta_1)$, $N(\theta_2)$ musí být násobkem p. Nechť je to bez újmy na obecnosti $N(\theta_1)$, tj. budiž $N(\theta_1) = n_1 p$ pro nějaké $n_1 \in \mathbb{N}$, $p \nmid n_1$. Pokud $n_1 = n$, pak nutně $N(\theta_2) = 1$, tudíž je θ_2 jednotkou, což je spor. Nutně tedy musí být $n_1 < n$. Přitom ale n_1 má tu vlastnost, že existuje $\theta_1 \in \mathbb{J}$ splňující $N(\theta_1) = n_1 p$ a zároveň $p \nmid n_1$ (n_1 dělí n). To je spor s tím, jak bylo zvoleno původní n, takže p nemůže být ireducibilní. □

Věta 10. *Pro libovolné $n \in \mathbb{N}$ existuje $\theta \in \mathbb{J}$ splňující $N(\theta) = n$.*

Důkaz. Začněme případem, kdy je n rovno nějakému prvočíslu p. Dle věty 9 je p reducibilní v $\mathbb{J}$, neboli existují nejednotková $\alpha, \beta \in \mathbb{J}$ splňující $p = \alpha\beta$. Z toho plyne na obou stranách

$$p^2 = N(p) = N(\alpha)N(\beta).$$

Vzhledem k $N(\alpha), N(\beta) > 1$ pak jistě $N(\alpha) = N(\beta) = p$, takže věta pro prvočísla vskutku platí.

Mějme nyní libovolné přirozené n. Pokud $n = 1$, máme $N(1) = 1$. Nadále tedy berme $n > 1$ a uvažujme rozklad

$$n = \prod_{s=1}^{m} p_s,$$

kde $m \geqq 1$ a všechna p_s jsou (ne nutně různá) prvočísla. Z platnosti věty pro prvočísla pro každé $s \in \{1, \ldots, m\}$ existuje $\theta_s \in \mathbb{J}$ splňující $N(\theta_s) = p_s$. Potom stačí vzít

$$\theta = \prod_{s=1}^{m} \theta_s,$$

čímž bude zaručeno

$$N(\theta) = N\left(\prod_{s=1}^{m} \theta_s\right) = \prod_{s=1}^{m} N(\theta_s) = \prod_{s=1}^{m} p_s = n.$$

□

Právě dokázaná věta je již pouhý krůček od Lagrangeovy věty o čtyřech čtvercích – víme již, že normy prvků $\mathbb{J}$ jsou právě všechna přirozená čísla, zbývá už jen ukázat, že totéž platí v $\mathbb{H}(\mathbb{Z})$. Než tak učiníme, dokažme ještě jednu větu o povaze ireducibilních prvků v $\mathbb{J}$.

Věta 11. *Kvaternion $\pi \in \mathbb{J}$ je ireducibilní, právě když je $N(\pi)$ prvočíslo.*

Důkaz. Pokud je $N(\pi) = p$ prvočíslo, pak pro libovolná $\alpha, \beta \in \mathbb{J}$ splňující $\pi = \alpha\beta$ platí $N(\alpha)N(\beta) = p$, tedy jedno z α, β musí být jednotkou, neboli je π vskutku ireducibilní.

Nyní nechť je π ireducibilní a uvažujme libovolné prvočíslo p, jež dělí $N(\pi)$. Dle věty 8 platí $p \in \mathbb{J}\pi$, neboli existuje $\theta \in \mathbb{J}$ takové, že $p = \theta\pi$. Položme $m = \frac{N(\pi)}{p} \in \mathbb{N}$ – potom máme

$$\begin{aligned} p^2 &= N(\theta) \cdot mp, \\ p &= N(\theta) \cdot m. \end{aligned}$$

Z toho plyne $m \in \{1, p\}$. Pokud $m = p$, musí θ být jednotkou, z čehož plyne $\pi = \overline{\theta}p$. Přitom p je ale dle věty 9 reducibilní, čímž je i π jakožto jeho násobek reducibilní. To je spor, tudíž jistě $m = 1$, neboli $N(\pi) = p$. □

Nyní již dokažme Lagrangeovu větu.

Lemma 12. *Mějme $n \in \mathbb{N}$ a $\alpha \in \mathbb{J}$ takové, že $N(\alpha) = n$. Potom existuje $\beta \in \mathbb{H}(\mathbb{Z})$ splňující $N(\beta) = n$.*

Důkaz. Pokud $\alpha \in \mathbb{H}(\mathbb{Z})$, stačí vzít $\beta = \alpha$ – nadále tedy předpokládejme $\alpha \in \mathbb{J} \setminus \mathbb{H}(\mathbb{Z})$ neboli $\alpha = \frac{a+b\mathrm{i}+c\mathrm{j}+d\mathrm{k}}{2}$ pro nějaká lichá celá čísla a, b, c, d. Zvolme e, f, g, $h \in \{\pm 1\}$ tak, že

$$a - e, \quad b - f, \quad c - g, \quad d - h$$

jsou násobky čtyř. Položíme-li $\delta = \frac{e+f\mathrm{i}+g\mathrm{j}+h\mathrm{k}}{2}$, je $\delta \in \mathbb{J}$ a zároveň $N(\delta) = 1$, navíc platí

$$\alpha - \delta = \frac{(a-e) + (b-f)\mathrm{i} + (c-g)\mathrm{j} + (d-h)\mathrm{k}}{2} = 2\gamma$$

pro nějaké $\gamma \in \mathbb{H}(\mathbb{Z})$. Z toho ale

$$\begin{aligned} \overline{\delta} \cdot \alpha &= \overline{\delta}(2\gamma + \delta) = \overline{\delta} \cdot 2\gamma + \overline{\delta} \cdot \delta = (2\overline{\delta}) \cdot \gamma + 1, \\ N(\overline{\delta} \cdot \alpha) &= N(\overline{\delta}) \cdot N(\alpha) = n. \end{aligned}$$

Uvažme nyní, že pro libovolné $\theta \in \mathbb{J}$ platí $2\theta \in \mathbb{H}(\mathbb{Z})$, z čehož $(2\overline{\delta})\gamma + 1 \in \mathbb{H}(\mathbb{Z})$. K dokončení důkazu tak stačí vzít $\beta = \overline{\delta} \cdot \alpha$. □

Důsledek (Lagrangeova věta o čtyřech čtvercích). *Pro každé přirozené n existuje $\theta \in \mathbb{H}(\mathbb{Z})$ splňující $N(\theta) = n$.*

4. Konstrukce dalšího oboru

Povšimněme si ještě jednou, že všechna tvrzení předchozí sekce až po větu 10 jsme odvodili výhradně z vlastností (i)–(v). Toto umožňuje zobecnit Hurwitzův postup pro důkaz univerzálnosti dalších kvadratických forem: kdykoliv nalezneme takovou množinu H, která splní všechny podmínky (i)–(v) (píšeme-li v nich vždy H namísto $\mathbb{J}$), pak musí pro každé $n \in \mathbb{N}$ existovat $\theta \in H$ mající normu n. Pokud tedy kvadratické formě dovedeme přiřadit obor, jehož prvky mají normy rovné hodnotám dané kvadratické formy a který splňuje podmínky (i)–(v), plyne z toho, že daná kvadratická forma je univerzální.

Příklad 1. Dokažme univerzálnost formy $x^2 - xy + y^2 + z^2 - zw + w^2$. Označme $\omega = \frac{-1+\mathrm{i}\sqrt{3}}{2}$ a zaveďme

$$H_3 = \{x + y\omega + z\mathrm{j} + w\omega\mathrm{j} \colon x, y, z, w \in \mathbb{Z}\}.$$

Ověřme postupně, že H_3 splňuje podmínky (i)–(v). Splnění $\mathbb{Z} \subseteq H_3 \subseteq \mathbb{H}(\mathbb{R})$ je zcela zřejmé. Množina H_3 je uzavřená na sčítání, uzavřenost na násobení plyne z $\theta_1\theta_2 \in H_3$ pro libovolná $\theta_1, \theta_2 \in \{1, \omega, \mathrm{j}, \omega\mathrm{j}\}$ (toto lze ověřit přímými výpočty) – je tedy splněna podmínka (ii). Pro podmínku (iii) pak stačí pro $\theta = x + y\omega + z\mathrm{j} + w\omega\mathrm{j}$ vyjádřit

$$\begin{aligned} N(\theta) &= N\left(x + y \cdot \frac{1 - \mathrm{i}\sqrt{3}}{2} + z\mathrm{j} + w \cdot \frac{\mathrm{j} - \mathrm{k}\sqrt{3}}{2}\right) = \\ &= \left(x - \frac{y}{2}\right)^2 + \left(\frac{y\sqrt{3}}{2}\right)^2 + \left(z - \frac{w}{2}\right)^2 + \left(\frac{w\sqrt{3}}{2}\right)^2 = \\ &= x^2 - xy + y^2 + z^2 - zw + w^2 \in \mathbb{Z}. \end{aligned}$$

Dokažme nyní splnění podmínky (iv) pomocí podobného postupu jako v lemmatu 2. Uvažujme libovolné prvočíslo p a dokažme, že lze zvolit x, z tak, že $x^2 - x + 1 + z^2$ je násobkem p, ale nikoliv p^2. Zaprvé pokud $p = 2$, stačí zvolit $x = 0$, $z = 1$. Nadále nechť je p liché (tedy $p \geqq 3$). Zaveďme $S_1 = \{1, \ldots, \frac{p+1}{2}\}$, $S_2 = \{0, \ldots, \frac{p-1}{2}\}$. Tak jako v důkazu lemmatu 2 nabývá $z^2 \pmod p$ pro $z \in S_2$ přesně $\frac{p+1}{2}$ různých hodnot. Dále pro $x_1, x_2 \in S_1 \setminus \{\frac{p+1}{2}\}$ díky $2 \leqq x_1 + x_2 \leqq p - 1$ (tedy $p \nmid (x_1 + x_2 - 1)$) platí $x_1^2 - x_1 + 1 \equiv x_2^2 - x_2 + 1 \pmod p$, právě když

$$x_1^2 - x_2^2 - x_1 + x_2 \equiv 0 \pmod p,$$

$$\begin{aligned}(x_1 - x_2)(x_1 + x_2 - 1) &\equiv 0 \pmod p,\\ x_1 - x_2 &\equiv 0 \pmod p,\\ x_1 &\equiv x_2 \pmod p,\end{aligned}$$

zatímco pro $x_1 = \frac{p+1}{2}$ nastává $p \mid (x_1 + x_2 - 1)$ právě tehdy, když i $x_2 \equiv \frac{p+1}{2} \pmod p$. Pro $x \in S_1$ tak výraz $x^2 - x + 1 \pmod p$ musí nabývat $\frac{p+1}{2}$ různých hodnot. Označíme-li tedy

$$U = \{x^2 - x + 1 \pmod p \colon x \in S_1\}, \qquad V = \{-z^2 \pmod p \colon z \in S_2\},$$

platí $|U| + |V| = p + 1 > p = |\mathbb{Z}_p|$ a zároveň $U, V \subseteq \mathbb{Z}_p$, čímž z Dirichletova principu nejsou U, V disjunktní. Existují tedy $x, z \in S$ taková, že

$$\begin{aligned}x^2 - x + 1 &\equiv -z^2 \pmod p,\\ x^2 - x + 1 + z^2 &\equiv 0 \pmod p.\end{aligned}$$

Platí pak $N(x + \omega + z\mathrm{j}) = mp$ pro

$$\begin{aligned}m &= \frac{x^2 - x + 1 + z^2}{p} \leqq \frac{\left(\frac{p+1}{2}\right)^2 - \frac{p+1}{2} + 1 + \left(\frac{p-1}{2}\right)^2}{p} =\\ &= \frac{(p^2 + 2p + 1) - 2(p+1) + 4 + (p^2 - 2p + 1)}{4p} = \frac{2p^2 - 2p + 4}{4p} < \frac{2p^2 + 4}{4p} <\\ &< \frac{3p^2}{4p} = \frac{3}{4}p < p\end{aligned}$$

(využíváme $p^2 \geqq 3^2 = 9 > 4$), zároveň ale jistě $x^2 - x + 1 + z^2 > 0$ (díky $x \geqq 1$ je $x^2 - x \geqq 0$). Z toho dohromady určitě plyne $p \nmid m$, čímž je podmínka (iv) jistě splněna.

Zbývá tak dokázat splnění podmínky (v). Podobně jako v případě oboru Hurwitzových kvaternionů dokážeme, že H_3 je (levým) oborem hlavních ideálů, skrze jeho eukleidovskost zleva. Za eukleidovkou funkci poslouží opět norma – chceme tedy dokázat, že pro nenulová $\alpha, \beta \in H_3$ existuje $\gamma \in H_3$ splňující $N(\alpha - \gamma\beta) < N(\beta)$. Zavedeme-li $\varphi = \frac{\alpha\overline{\beta}}{N(\beta)}$ (to je obecně prvek $\mathbb{H}(\mathbb{R})$), pak $\alpha = \varphi\beta$ a předchozí nerovnost lze ekvivalentně upravit do tvaru

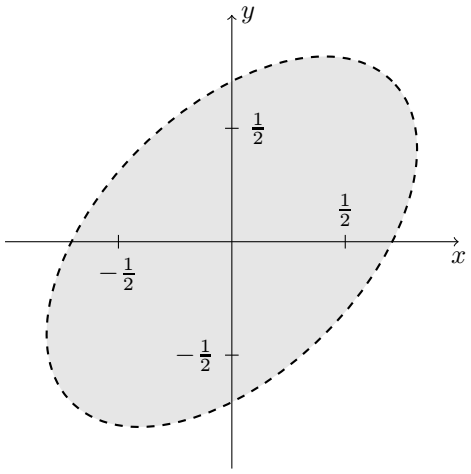
$$\begin{aligned}N(\varphi - \gamma)N(\beta) = N(\varphi\beta - \gamma\beta) = N(\alpha - \gamma\beta) &< N(\beta),\\ N(\varphi - \gamma) &< N(1).\end{aligned} \tag{2}$$

Nechť je $\varphi = x_0 + y_0\omega + z_0\mathrm{j} + w_0\omega\mathrm{j}$ pro reálná x_0, y_0, z_0, w_0. Uvažujme reálná x, y, z, w taková, že $x_0 - x$ atp. jsou celá čísla, a označme $\gamma = \varphi - (x + y\omega + z\mathrm{j} + w\omega\mathrm{j})$. Pro splnění podmínky (v) je třeba ukázat, že x, y, z, w lze zvolit tak, aby bylo splněno $x_0 - x \in \mathbb{Z}$ atp., a zároveň

$$1 > N(\varphi - \gamma) = N(x + y\omega + z\mathrm{j} + w\omega\mathrm{j}) = (x^2 - xy + y^2) + (z^2 - zw + w^2). \tag{3}$$

K tomu postačí ukázat, že lze zvolit x, y tak, aby $x^2 - xy + y^2 < \frac{1}{2}$ (analogicky pak totéž provedeme pro z, w, což dohromady dá (3)). Na to už lze nahlížet geometricky –

řešení nerovnice $x^2 - xy + y^2 < \frac{1}{2}$ představují v $\mathbb{R}^2$ vnitřek jisté elipsy se středem v počátku (viz obrázek 1) a má se dokázat, že libovolný bod (x_0, y_0) roviny lze posunout o vektor (a, b) s celočíselnými složkami tak, aby jeho obraz ležel uvnitř této elipsy. To je ekvivalentní tvrzení, že všechna posunutí této elipsy o všechny možné vektory (a, b) s celočíselnými složkami dohromady pokrývají celou rovinu.



Obr. 1. Řešení nerovnice $x^2 - xy + y^2 < \frac{1}{2}$

Stačí ukázat, že takovéto pokrytí vytvoří už nějaká podmnožina vnitřku elipsy. Označme A_0, B_0 průsečíky elipsy $x^2 - xy + y^2 = \frac{1}{2}$ s přímkou $y = \frac{1}{2}$. Dosazením do rovnice elipsy máme

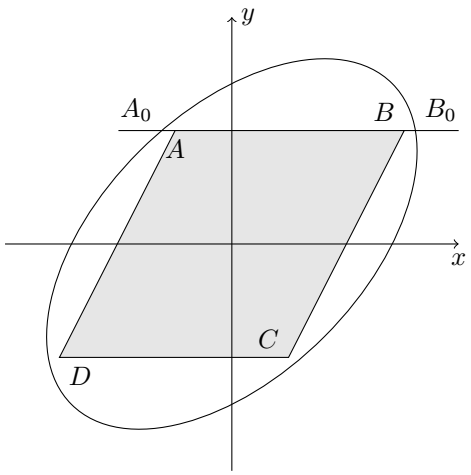
$$x^2 - \frac{x}{2} - \frac{1}{4} = 0,$$

$$x_{1,2} = \frac{\frac{1}{2} \pm \sqrt{\frac{1}{4} + 4 \cdot \frac{1}{4}}}{2},$$

takže

$$|A_0B_0| = x_1 - x_2 = \sqrt{\frac{1}{4} + 4 \cdot \frac{1}{4}} = \frac{\sqrt{5}}{2} > 1.$$

Určitě tedy lze zvolit body A, B tak, že oba jsou vnitřními body úsečky A_0B_0 a zároveň $|AB| > 1$. Označme C, D obrazy A, B v souměrnosti dle počátku. Pak je celý rovnoběžník $ABCD$ obsažen uvnitř uvažované elipsy (vnitřní oblast elipsy je konvexní množina souměrná dle počátku), zároveň má ale stranu délky $|AB| > 1$ a výšku na ni kolmou délky přesně 1 (viz obrázek 2). Posouváním tohoto rovnoběžníku o vektory s celočíselnými složkami tak určitě pokryjeme celou rovinu. Pro daná reálná x_0, y_0 tedy lze zvolit x, y splňující $x - x_0 \in \mathbb{Z}$, $y - y_0 \in \mathbb{Z}$ a taková, že bod $[x, y]$ náleží rovnoběžníku $ABCD$. Např. lze nejprve zvolit y tak, že $-\frac{1}{2} \leqq y \leqq \frac{1}{2}$ (to určitě lze), a následně vhodně zvolit x – to lze, neboť průnikem $ABCD$ s libovolnou přímkou $y = t$, kde $-\frac{1}{2} \leqq t \leqq \frac{1}{2}$, je úsečka délky $|AB| > 1$.



Obr. 2. Příklad rovnoběžníku $ABCD$ uvnitř elipsy

Tímto je dokázáno, že H_3 splňuje podmínku (v). To už značí, že kvadratická forma

$$x^2 - xy + y^2 + z^2 - zw + w^2$$

je univerzální.

5. Využití nadoboru

Postup použitý v předchozí sekci spoléhá na to, že obor, jehož prvky mají normy určené danou kvadratickou formou, je oborem hlavních ideálů. Toto není vždy splněno. V mnoha případech lze však uvažovat nějaký nadobor tohoto oboru, který už oborem hlavních ideálů je, a následně už pouze dokázat, že každý prvek nadoboru má k sobě prvek oboru se stejnou normou. To je přesně postup, který jsme užili k důkazu Lagrangeovy věty – namísto abychom pracovali přímo s oborem $\mathbb{H}(\mathbb{Z})$, využili jsme jeho nadobor $\mathbb{J}$. Poznamenejme, že pro některé formy uvedené v tabulce 1 může být tento postup mírně výpočetně náročný – nalezení a ověření všech použitých konstant se v takových případech vyplatí provést počítačem.

Příklad 2. Ukažme, že kvadratická forma

$$x^2 + xy + 2y^2 + yz - xw + z^2 + zw + 2w^2 \tag{4}$$

je univerzální. Položme

$$\alpha = \frac{1 + \mathrm{i}\sqrt{7}}{2}, \qquad \beta = \frac{\mathrm{i} + \mathrm{j}\sqrt{6}}{\sqrt{7}}, \qquad \zeta = \frac{1 + \alpha + \beta + \alpha\beta}{2}$$

a zaveďme množiny

$$\begin{aligned} H_6 &= \{x + y\alpha + z\beta + w\alpha\beta \colon x, y, z, w \in \mathbb{Z}\}\,, \\ G_3 &= \{x + y\alpha + z\beta + w\zeta \colon x, y, z, w \in \mathbb{Z}\}\,. \end{aligned}$$

Obě množiny H_6, G_3 tvoří obory – uzavřenost na sčítání je v obou případech zřejmá, pro uzavřenost na násobení stačí ověřit $\theta_1\theta_2 \in H_6$ pro θ_1, $\theta_2 \in \{1, \alpha, \beta, \alpha\beta\}$, resp. $\theta_1\theta_2 \in G_3$ pro θ_1, $\theta_2 \in \{1, \alpha, \beta, \zeta\}$ (to lze učinit přímými výpočty). Pro báze H_6 dostáváme multiplikační tabulku 2.

	1	α	β	$\alpha\beta$
1	1	α	β	$\alpha\beta$
α	α	$\alpha - 2$	$\alpha\beta$	$\alpha\beta - 2\beta$
β	β	$-1 - \alpha\beta + \beta$	-1	$-\beta + \alpha - 1$
$\alpha\beta$	$\alpha\beta$	$-\alpha + 2\beta$	$-\alpha$	$-\alpha\beta - 2$

Tab. 2. Multiplikační tabulka bází oboru H_6

Dále platí

$$\alpha\beta = \left(\frac{1+\mathrm{i}\sqrt{7}}{2}\right)\cdot\left(\frac{\mathrm{i}+\mathrm{j}\sqrt{6}}{\sqrt{7}}\right) = -\frac{1}{2} + \frac{\mathrm{i}}{2\sqrt{7}} + \frac{\mathrm{j}\sqrt{6}}{2\sqrt{7}} + \frac{\mathrm{k}\sqrt{6}}{2},$$

což už pro $\theta = x + y\alpha + z\beta + w\alpha\beta$ implikuje

$$\begin{aligned} N(\theta) &= N\left(x + y\cdot\frac{1+\mathrm{i}\sqrt{7}}{2} + z\cdot\frac{\mathrm{i}+\mathrm{j}\sqrt{6}}{\sqrt{7}} + w\cdot\left(-\frac{1}{2} + \frac{\mathrm{i}}{2\sqrt{7}} + \frac{\mathrm{j}\sqrt{6}}{2\sqrt{7}} + \frac{\mathrm{k}\sqrt{6}}{2}\right)\right) = \\ &= \left(x + \frac{y}{2} - \frac{w}{2}\right)^2 + \left(\frac{y\sqrt{7}}{2} + \frac{z}{\sqrt{7}} + \frac{w}{2\sqrt{7}}\right)^2 + \left(\frac{z\sqrt{6}}{\sqrt{7}} + \frac{w\sqrt{6}}{2\sqrt{7}}\right)^2 + \left(\frac{w\sqrt{6}}{2}\right)^2 = \\ &= x^2 + xy + 2y^2 + yz - xw + z^2 + zw + 2w^2. \end{aligned}$$

Označme $\gamma = \frac{-1-\alpha+\beta-\alpha\beta}{2} = \beta - \zeta$. Potom také $\gamma\beta = \frac{-1+\alpha-\beta-\alpha\beta}{2} = \alpha - \zeta$. Určitě tedy γ, $\gamma\beta \in G_3$, díky vztahům

$$\zeta = \beta - \gamma, \qquad \alpha = \zeta + \gamma\beta = \beta - \gamma + \gamma\beta$$

tak lze G_3 ekvivalentně zapsat ve tvaru $G_3 = \{x + y\gamma + z\beta + w\gamma\beta\colon x, y, z, w \in \mathbb{Z}\}$. Potom normu libovolného $\theta = x + y\gamma + z\beta + w\gamma\beta \in G_3$ vyjádříme jako

$$\begin{aligned} N(\theta) &= N(x + y\gamma + z\beta + w\gamma\beta) = N\left(\left(x - \frac{y}{2} - \frac{w}{2}\right) + \left(\frac{w-y}{2}\right)\alpha + \right. \\ &\quad \left. + \left(z + \frac{y}{2} - \frac{w}{2}\right)\beta + \left(\frac{-y-w}{2}\right)\alpha\beta\right) = \left(x - \frac{y}{2} - \frac{w}{2}\right)^2 + \\ &\quad + \left(x - \frac{y}{2} - \frac{w}{2}\right)\left(\frac{w-y}{2}\right) + 2\left(\frac{w-y}{2}\right)^2 + \left(\frac{w-y}{2}\right)\left(z + \frac{y}{2} - \frac{w}{2}\right) - \\ &\quad - \left(x - \frac{y}{2} - \frac{w}{2}\right)\left(\frac{-y-w}{2}\right) + \left(z + \frac{y}{2} - \frac{w}{2}\right)^2 + \left(z + \frac{y}{2} - \frac{w}{2}\right)\left(\frac{-y-w}{2}\right) + \\ &\quad + 2\left(\frac{-y-w}{2}\right)^2 = x^2 - xy + y^2 + z^2 - zw + w^2. \end{aligned}$$

Přitom už víme, že kvadratická forma $x^2 - xy + y^2 + z^2 - zw + w^2$ je univerzální, takže určitě pro každé $n \in \mathbb{N}$ existuje $\theta \in G_3$ takové, že $N(\theta) = n$.

Zbývá už jen ukázat, že každé takové θ lze vynásobit jednotkou (z G_3) tak, aby součin byl prvkem H_6. Pokud $\theta \in H_6$, je to triviální, nadále tedy předpokládejme $\theta \in G_3 \setminus H_6$. Povšimněme si, že $2\zeta \in H_6$, a dále

$$\begin{aligned} \gamma \cdot 2 &= -1 - \alpha + \beta - \alpha\beta \in H_6, & \gamma \cdot (\alpha - 1) &= 1 - \beta \in H_6, \\ \gamma \cdot (\beta - 1) &= \alpha - \beta \in H_6, & \gamma \cdot (\alpha\beta - 1) &= 1 + \alpha \in H_6. \end{aligned}$$

Libovolné $\theta \in G_3 \setminus H_6$ tak lze zapsat jako

$$\theta = m + \gamma + 2x + y(\alpha - 1) + z(\beta - 1) + w(\alpha\beta - 1)$$

pro $m \in \{0, 1\}$; konečně pak $\overline{\gamma} = \frac{-1+\alpha-\beta+\alpha\beta}{2} = -1 - \gamma$, z čehož $\gamma(1+\gamma) = \gamma \cdot (-\overline{\gamma}) = -N(\gamma) = -1$. Rozlišíme dva případy: pokud $m = 1$, vezmeme

$$\gamma \cdot \theta = -1 + \gamma \cdot (2x + y(\alpha - 1) + z(\beta - 1) + w(\alpha\beta - 1)) \in H_6,$$

zatímco pokud $m = 0$, vezmeme

$$(\gamma + 1) \cdot \theta = -1 + (\gamma + 1) \cdot (2x + y(\alpha - 1) + z(\beta - 1) + w(\alpha\beta - 1)) \in H_6.$$

Platí $N(\gamma) = N(\gamma + 1) = 1$, takže jsou oba tyto kvaterniony jednotkami a univerzálnost kvadratické formy (4) je dokázána.

Příklad 3. Ukažme, že kvadratická forma

$$x^2 + xy + 3y^2 + yz - xw + z^2 + zw + 3w^2 \tag{5}$$

je univerzální. Položme

$$\alpha = \frac{1 + \mathrm{i}\sqrt{11}}{2}, \qquad \beta = \frac{\mathrm{i} + \mathrm{j}\sqrt{10}}{\sqrt{11}}, \qquad \gamma = \frac{1 + 2\alpha + 2\beta - \alpha\beta}{5}$$

a zaveďme množiny

$$\begin{aligned} H_{10} &= \{x + y\alpha + z\beta + w\alpha\beta \colon x, y, z, w \in \mathbb{Z}\}\,, \\ G_2 &= \{x + y\alpha + z\beta + w\gamma \colon x, y, z, w \in \mathbb{Z}\}\,. \end{aligned}$$

Stejně jako v předchozím případě tvoří H_{10} i G_2 obory – pro báze H_{10} dostáváme multiplikační tabulku 3.

	1	α	β	$\alpha\beta$
1	1	α	β	$\alpha\beta$
α	α	$\alpha - 3$	$\alpha\beta$	$\alpha\beta - 3\beta$
β	β	$-1 - \alpha\beta + \beta$	-1	$-\beta + \alpha - 1$
$\alpha\beta$	$\alpha\beta$	$-\alpha + 3\beta$	$-\alpha$	$-\alpha\beta - 3$

Tab. 3. Multiplikační tabulka bází oboru H_6

Roznásobením $\alpha \cdot \beta$ a přímým výpočtem z definice normy získáme

$$N(x + y\alpha + z\beta + w\alpha\beta) = x^2 + xy + 3y^2 + yz - xw + z^2 + zw + 3w^2.$$

Dále platí $\gamma\beta = \frac{-2+\alpha+\beta+2\alpha\beta}{5} = -2\gamma + \alpha + \beta$, z čehož určitě $\gamma\beta \in G_2$ a zároveň $\alpha = 2\gamma - \beta + \gamma\beta$. Obor G_2 tak lze ekvivalentně zapsat jako $G_2 = \{x + y\gamma + z\beta + w\gamma\beta : x, y, z, w \in \mathbb{Z}\}$. Přímým výpočtem pak můžeme normu libovolného $\theta = x + y\gamma + z\beta + w\gamma\beta \in G_2$ vyjádřit jako

$$\begin{aligned} N(\theta) &= N\left(\left(x + \frac{y}{5} - \frac{2w}{5}\right) + \left(\frac{2y+w}{5}\right)\alpha + \left(z + \frac{2y}{5} + \frac{w}{5}\right)\beta + \left(\frac{2w-y}{5}\right)\alpha\beta\right) = \\ &= x^2 + xy + y^2 + yz - xw + z^2 + zw + w^2 = \\ &= \left(x + \frac{y}{2} - \frac{w}{2}\right)^2 + \left(\frac{y-w}{2}\right)^2 + \left(z + \frac{y}{2} + \frac{w}{2}\right)^2 + \left(\frac{y+w}{2}\right)^2 = \\ &= N\left(x + y \cdot \frac{1+\mathrm{i}+\mathrm{j}+\mathrm{k}}{2} + z\mathrm{j} + w \cdot \frac{-1-\mathrm{i}+\mathrm{j}+\mathrm{k}}{2}\right). \end{aligned} \tag{6}$$

Přitom ale

$$\begin{aligned} \mathbb{J} &= \left\{x + y \cdot \frac{1+\mathrm{i}+\mathrm{j}+\mathrm{k}}{2} + z\mathrm{j} + w\mathrm{k}\colon x, y, z, w \in \mathbb{Z}\right\} = \\ &= \left\{x + y \cdot \frac{1+\mathrm{i}+\mathrm{j}+\mathrm{k}}{2} + zj + w \cdot \frac{-1-\mathrm{i}+\mathrm{j}+\mathrm{k}}{2}\colon x, y, z, w \in \mathbb{Z}\right\}, \end{aligned}$$

takže výrazem (6) lze dle věty 10 vyjádřit libovolné přirozené číslo. Pro každé $n \in \mathbb{N}$ tak existuje $\theta \in G_2$ takové, že $N(\theta) = n$.

Zbývá už jen ukázat, že každé takové θ lze vynásobit jednotkou (z G_2) tak, aby součin byl prvkem H_{10}. Pokud $\theta \in H_{10}$, je to triviální, nadále tedy předpokládejme $\theta \in G_2 \setminus H_{10}$. Povšimněme si, že platí

$$\begin{aligned} \gamma \cdot 5 &= 1 + 2\alpha + 2\beta - \alpha\beta \in H_{10}, & \gamma \cdot (\alpha - 2) &= -2 - \beta \in H_{10}, \\ \gamma \cdot (\beta + 2) &= \alpha + \beta \in H_{10}, & \gamma \cdot (\alpha\beta - 1) &= -2\beta + \alpha\beta \in H_{10}. \end{aligned}$$

Z toho pro libovolné θ_0 tvaru

$$\theta_0 = 5x + y(\alpha - 2) + z(\beta + 2) + w(\alpha\beta - 1) \tag{7}$$

plyne $\gamma\theta_0 \in H_{10}$, resp. dokonce $(\rho\gamma + \tau)\theta_0 \in H_{10}$ pro libovolná $\rho, \tau \in H_{10}$. Tvarem $\rho\gamma + \tau$ však lze popsat libovolný prvek G_2, tedy v souhrnu pro každé θ_0 tvaru (7) platí $\lambda\theta_0 \in H_{10}$ pro libovolné $\lambda \in G_2$.

Dále lze každé $\theta \in G_2 \setminus H_{10}$ zapsat jako

$$\theta = m(\gamma + \ell) + \theta_0,$$

kde θ_0 je tvaru (7), $m \in \{1, 2, 3, 4\}$ a $\ell \in \{0, 1, 2, 3, 4\}$. Nyní tedy stačí ukázat, že pro každé z těchto ℓ existuje jednotka $\zeta_\ell \in G_2$ splňující $\zeta_\ell(\gamma + \ell) \in H_{10}$. Takovéto jednotky existují, vyhovují např.

$$\begin{aligned} \zeta_0 &= \overline{\gamma} = 1 - \gamma, & \zeta_1 &= \gamma - \beta, & \zeta_2 &= \gamma\beta = \alpha + \beta - 2\gamma, \\ \zeta_3 &= \gamma - \alpha, & \zeta_4 &= \gamma. \end{aligned}$$

Tímto je dokázáno, že kvadratická forma (5) je univerzální.

6. Jacobiho věta

Závěrem článku uveďme bez důkazu, jak lze Lagrangeovu větu podstatně zesílit.

Věta (Jacobiho o čtyřech čtvercích). *Pro $n \in \mathbb{N}$ je počet celočíselných řešení rovnice $n = x^2 + y^2 + z^2 + w^2$ přesně*

$$8 \sum_{4\nmid d \mid n} d,$$

tedy osminásobek součtu těch dělitelů n, které nejsou samy násobky čtyř.

Tuto větu poprvé dokázal roku 1834 Carl Gustav Jakob Jacobi pomocí analytických metod. Později byl Adolfem Hurwitzem podán důkaz vycházející z podrobnějšího zkoumání faktorizace v oboru $\mathbb{J}$ a izomorfizmů mezi některými okruhy zbytkových tříd mod p oboru $\mathbb{H}(\mathbb{Z})$ a maticovými okruhy nad $\mathbb{Z}_p$ (pro prvočíslo p).

Zobecněním Hurwitzovy metody lze podobné explicitní vzorce pro počet vyjádření daného čísla danou kvadratickou formou nalézt i pro mnohé další (ne však všechny) kvadratické formy uvedené v tabulce 1 v úvodu článku – viz tabulku 4.

$(x^2 + xy + y^2) + (yz - xw) + (z^2 + zw + w^2)$	$24 \sum_{2\nmid d \mid n} d$
$(x^2 + xy + y^2) + (z^2 + zw + w^2)$	$12 \sum_{3\nmid d \mid n} d$
$x^2 + y^2 + z^2 + w^2$	$8 \sum_{4\nmid d \mid n} d$
$(x^2 + xy + y^2) + (yz - xw) + 2(z^2 + zw + w^2)$	$6 \sum_{5\nmid d \mid n} d$
$(x^2 + xy + 2y^2) + (z^2 + zw + 2w^2)$	$4 \sum_{7\nmid d \mid n} d$
$(x^2 + xy + 3y^2) + 3(yz - xw) + 2(z^2 + zw + 3w^2)$	$2 \sum_{13\nmid d \mid n} d$
$(x^2 + xy + 2y^2) + (yz - xw) + (z^2 + zw + 2w^2)$	$8 \sum_{3\nmid d \mid n} d - 4 \sum_{2,3\nmid d \mid n} d$
$(x^2 + xy + y^2) + 2(z^2 + zw + w^2)$	$12 \sum_{2\nmid d \mid n} d - 6 \sum_{2,3\nmid d \mid n} d$
$(x^2 + xy + 2y^2) + 2(yz - xw) + 2(z^2 + zw + 2w^2)$	$4 \sum_{5\nmid d \mid n} d - 2 \sum_{2,5\nmid d \mid n} d$
$(x^2 + xy + 3y^2) + (yz - xw) + (z^2 + zw + 3w^2)$	$8 \sum_{2\nmid d \mid n} d - 4 \sum_{2,5\nmid d \mid n} d$
$(x^2 + xy + 3y^2) + 2(z^2 + zw + 3w^2)$	$4 \sum_{2\nmid d \mid n} d - 2 \sum_{2,11\nmid d \mid n} d$

Tab. 4. Vzorce analogické Jacobiho větě pro vybrané kvadratické formy

Poděkování. Autor děkuje Mgr. Vítězslavu Kalovi, Ph.D., za cenné rady a ochotnou pomoc při psaní tohoto článku, jakož i práce SOČ, z níž tento článek vychází.

L i t e r a t u r a

[1] Coan, B., Perng, C.: *Factorization of Hurwitz quaternions*. International Mathematical Forum (2012) [online], [cit. 27. 3. 2019]. Dostupné z: `http://www.m-hikari.com/imf/imf-2012/41-44-2012/perngIMF41-44-2012.pdf`

[2] Heath, T.: *Diophantus of Alexandria; a study in the history of Greek algebra*. Cambridge University Press, Cambridge, 1910.

[3] Hurwitz, A.: *Ueber die Zahlentheorie der Quaternionen*. Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Matematisch-physikalische Klasse (1896), 313–340.