Werk

Label: Article

Jahr: 1933

PURL: https://resolver.sub.uni-goettingen.de/purl?31311028X_0062|log107

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

ROZHLEDY
MATEMATICKO-PŘÍRODOVĚDECKÉ.

ROČNÍK 12 (1932/33). ČÍSLO 3.

Čísla Gaussova.

Vlad. Knichal.

V novějších směrech matematického badání (hlavně v algebře) jeví se snaha vybudovati na jednotném základě různé obory, které na prvý pohled nemají nic společného. Místo s čísly pracujeme v moderní algebře s elementy, o jejichž interpretaci se předem nestaráme. Předpokládáme, že máme definovány jisté početní operace s těmito elementy (které nazveme sčítáním, násobením atd.), a že pro tyto početní operace platí jistá početní pravidla (analogická početním pravidlům pro sčítání, násobení a t. p. čísel). Z těchto základních pravidel vyvozujeme důsledky, zavádíme nové pojmy, mezi nimiž pak hledáme vztahy. Je pak patrno, že takto vybudovanou teorii můžeme aplikovati na jakoukoliv interpretaci daných elementů, jsou-li jen splněny základní předpoklady o operacích s těmito elementy. Tím vlastně do jisté míry sjednotíme všechny obory, na které lze tuto obecnou teorii aplikovati a získáváme na jejich přehlednosti.

Ukážeme si na příkladě Gaussových čísel, že platí pro ně analogické věty jako pro čísla celá. Můžeme pak tušiti, že pojem čísla celého lze zobecniti (tak, aby se základní vlastnosti těchto čísel zachovaly). Jak se to děje, a do jaké míry, je možno viděti v teorii okruhů a ideálů. To však se již vymyká rámci tohoto článku.

Čísly Gaussovými budeme nazývati taková čísla komplexní[1]) $\alpha = a + bi$, kde a, b jsou čísla celá; na př. $2 + 3i = \alpha$ je takovým číslem. Je patrno, že součet, rozdíl a součin dvou čísel Gaussových je opět číslem Gaussovým. Neplatí to obecně o podílu. Jsou-li dána dvě čísla Gaussova α, β ($\beta \neq 0$) a jestliže $\frac{\alpha}{\beta}$ je opět číslo Gaussovo, budeme říkati, že α je dělitelno číslem β aneb, že β je dělitelem čísla α aneb, že α je násobkem β. Tuto okolnost budeme značiti: β/α. Není-li β/α, budeme psáti $\beta \times \alpha$.[2]) *Normou* $N(\alpha)$ komplex-

[1]) i značí imaginární jednotku; komplexní čísla budeme zásadně značiti písmeny řeckými, reálná čísla písmeny latinskými.

[2]) Čísla celá jsou ovšem zároveň čísly Gaussovými. V oboru čísel celých máme již však pojem dělitelnosti zaveden. Jestliže však a jest dělitelno

ního čísla $\alpha = a + bi$ budeme nazývati číslo $N(\alpha) = a^2 + b^2$. (Zřejmě $N(0) = 0$ a naopak, jestliže $N(\alpha) = 0$, je $\alpha = 0$.) Gaussovo číslo α budeme nazývati Gaussovou jednotkou, jestliže $N(\alpha) = 1$. Okamžitě je patrno, že pouze čísla $1, i, -1, -i$ jsou Gaussovými jednotkami. Dvě Gaussova čísla α, β budeme nazývati asociovanými, jestliže $\alpha = \varepsilon\beta$, kde ε je Gaussova jednotka.[3])

Buď $\alpha = a + bi, \quad \beta = c + di.$ Pak

$$\alpha\beta = (ac - bd) + i\,(ad + bc)$$

a dále

$$N(\alpha\beta) = (ac - bd)^2 + (ad + bc)^2 = (a^2 + b^2)\,(c^2 + d^2) = \\ = N(\alpha)\,.\,N(\beta).$$

Jestliže $\beta \neq 0$, klaďme $\frac{\alpha}{\beta} = \gamma$. Pak je

$$N(\alpha) = N(\beta\gamma) = N(\beta)\,.\,N(\gamma)$$

a tudíž

$$N\left(\frac{\alpha}{\beta}\right) = N(\gamma) = \frac{N(\alpha)}{N(\beta)}.$$

Platí tedy

$$N(\alpha\beta) = N(\alpha)\,N(\beta)$$

vždy a

$$N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)} \text{ pro } \beta \neq 0. \tag{1}$$

Jestliže je α číslo Gaussovo, je zřejmě $N(\alpha)$ číslo celé, nezáporné. Jsou-li tedy α, β $(\beta \neq 0)$ dvě čísla Gaussova a jestliže je α dělitelno číslem β, pak $N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}$ je číslo celé, t. zn. norma čísla α je dělitelná[2]) normou čísla β.

Jsou-li α, β dvě asociovaná Gaussova čísla, je $\alpha = \varepsilon\beta$, kde ε je Gaussova jednotka a tudíž

$$N(\alpha) = N(\varepsilon)\,.\,N(\beta) = N(\beta). \tag{2}$$

Každé číslo Gaussovo $\alpha \neq 0$ je dělitelno Gaussovými jednotkami a všemi čísly asociovanými k α. Jestliže kromě těchto dělitelů

číslem $b \neq 0$ v oboru čísel Gaussových, t. zn. jestliže $\frac{a}{b} = \alpha$ je číslo Gaussovo, je α číslo celé, neboť je rovno číslu reálnému $\frac{a}{b}$. Je tedy a dělitelno číslem b také v oboru čísel celých. Opak je samozřejmý.

[3]) Pak $\beta = \frac{1}{\varepsilon}\,\alpha$, kde zřejmě $\frac{1}{\varepsilon}$ je rovněž Gaussova jednotka.

není žádné jiné Gaussovo číslo dělitelem čísla α a jestliže $N(\alpha) \neq 1$, nazýváme α Gaussovým prvočíslem.

Prvým naším úkolem bude rozhodnouti o daném Gaussově čísle, zdali je prvočíslem. Dalším úkolem bude pak dokázati větu o rozkladu Gaussových čísel v součin Gaussových prvočísel.

Věta 1. Buďte dána dvě Gaussova čísla α, β ($\alpha \neq 0$, $\beta \neq 0$). Jestliže součin $\alpha\beta$ je dělitelný jistým Gaussovým prvočíslem ϱ, pak jistě alespoň jedno z čísel α, β je dělitelno číslem ϱ.

Důkaz.

1. Nechť ϱ / α. Věta 1. je pak zřejmě správná.
2. Nechť $\varrho \nmid \alpha$. Utvořme systém S čísel

$$\lambda\varrho + \mu\alpha, \tag{3}$$

při čemž λ, μ probíhají nezávisle na sobě všechna možná Gaussova čísla. (Klademe-li jednou $\lambda = 1$, $\mu = 0$ a po druhé $\lambda = 0$, $\mu = 1$, vidíme, že čísla ϱ, α jsou obsažena v systému S.) Tento systém má následující vlastnosti: Jestliže čísla $\sigma_1 = \lambda_1\varrho + \mu_1\alpha$, $\sigma_2 = \lambda_2\varrho + \mu_2\alpha$ náleží do systému S ($\lambda_1, \mu_1, \lambda_2, \mu_2$ jsou Gaussova čísla), pak v systému S jsou také čísla

$$\sigma_1 \pm \sigma_2 = (\lambda_1 \pm \lambda_2)\,\varrho + (\mu_1 \pm \mu_2)\,\alpha, \quad \tau\sigma_1 = (\tau\lambda_1)\,\varrho + (\tau\mu_1)\,\alpha,$$

při čemž τ je libovolné Gaussovo číslo. Tedy s čísly σ_1, σ_2 vyskytuje se v systému S současně jejich součet, rozdíl a všechny jejich násobky. Poněvadž normy Gaussových čísel jsou čísla celá, existuje v systému S číslo $\omega \neq 0$, jehož norma $N(\omega)$ je nejmenší,[4]) to zn., že pro každé číslo $\sigma \neq 0$ z S platí:

$$0 < N(\omega) \leqq N(\sigma). \tag{4}$$

Dokážeme si nejdříve, že každé číslo σ z S dá se pak vyjádřiti takto: $\sigma = \tau\omega$, při čemž τ je Gaussovo číslo. Utvořme podíl

$$\frac{\sigma}{\omega} = \bar{\tau} = \bar{a} + \bar{b}i. \tag{5}$$

Buď a, resp. b celé číslo, které se nejvíce přibližuje k číslu $\bar{a}$, resp. $\bar{b}$; tedy, klademe-li $\bar{a} = a + a'$, $\bar{b} = b + b'$, je $|a'| \leqq \frac{1}{2}$, $|b'| \leqq \frac{1}{2}$ a norma čísla $\tau' = a' + b'i$ je $N(\tau') = a'^2 + b'^2 \leqq \frac{1}{2}$. Avšak číslo (klademe $\tau = a + bi$, tedy $\bar{\tau} = \tau + \tau'$)

$$\sigma - \tau\omega$$

je obsaženo v systému S (podle nahoře vytčených vlastností tohoto systému) a tedy, poněvadž $\sigma - \tau\omega = \tau'\omega$, je $N(\tau'\omega)$ číslo celé, nezáporné. Podle (1) je však $N(\tau'\omega) = N(\tau').N(\omega) \leqq \frac{1}{2}N(\omega) < N(\omega)$. Kdyby $\tau'\omega \neq 0$, bylo by podle (4): $N(\tau'\omega) \geqq N(\omega)$. Tedy $\tau'\omega = 0$, čili ($\omega \neq 0$) $\tau' = 0$. Tudíž $\sigma = \bar{\tau}\omega = \tau\omega$.

[4]) V systému S existují čísla od nuly různá, na př. ϱ, α.