Karel Rychlík

O kvadratických tělesech číselných. [I.]

Časopis pro pěstování mathematiky a fysiky, Vol. 50 (1921), No. 1, 49--59

Persistent URL: http://dml.cz/dmlcz/122274

Příloha k Časopisu pro pěstování mathematiky a fysiky.

O kvadratických tělesech číselných.

Dr. Karel Rychlík.

§ 1. Kvadratické těleso číselné.

Těleso číselné je soustava čísel, v níž možno prováděti čtyři základní početní úkony: sčítání, odčítání, násobení a dělení. Výsledek těchto operací, až na dělení nulou, provedeme-li je s libovolnými čísly oné soustavy, dá zase čísla z ní.

Tak na příklad čísla racionálná tvoří těleso: součet, rozdíl součin a podíl (je-li dělitel $\neq 0$) dvou čísel racionálných je zase číslo racionálné. Toto těleso označíme R. V pojednání tomto budeme se zabývati dalšími jednoduchými tělesy číselnými, totiž tělesy kvadratickými a budeme se snažiti definovati pro ně též pojem celistvosti a dělitelnosti.

Uvažujme všechna čísla, která možno vyjádřiti ve tvaru $a + b\sqrt{m}$, kdež m značí pevné číslo racionálné, však $\sqrt{m}$ je irracionálná, a, b pak libovolná čísla racionálná. Číslo takové $a + b\sqrt{m}$ je tehdy a jen tehdy $= 0$, když současně $a = b = 0$. Lze snadno dokázati, že souhrn čísel toho tvaru tvoří těleso. Jsou-li totiž $a_1 + b_1\sqrt{m}$ a $a_2 + b_2\sqrt{m}$ libovolná dvě taková čísla, tedy a_1, b_1, a_2, b_2 čísla racionálná, je součet $a_1 + a_2 + (b_1 + b_2)\sqrt{m}$, rozdíl $a_1 - a_2 + (b_1 - c_2)\sqrt{m}$ a součin jich $a_1 a_2 + m b_1 b_2 + (a_1 b_2 + a_2 b_1)\sqrt{m}$ zase číslo z onoho souhrnu. Platí to i pro podíl $(a_1 + b_1\sqrt{m}) / (a_2 + b_2\sqrt{m})$, kdež $a_2 + b_2\sqrt{m} \neq 0$ tak že není současně $a_2 = 0$, $b_2 = 0$, uvážíme-li, že lze jej uvésti na tvar

$$\frac{(a_1 + b_1\sqrt{m})(a_2 - b_2\sqrt{m})}{a_2^2 - b_2^2 m} = \frac{a_1 a_2 - m b_1 b_2}{a_2^2 - b_2^2 m} + \frac{a_2 b_1 - a_1 b_2}{a_2^2 - b_2^2 m}\sqrt{m}$$

Speciální těleso právě definované nazývá se *tělesem kvadratickým*. Je určeno číslem $\sqrt{m}$ a proto je označíme $R(\sqrt{m})$. Obsahuje v sobě všechna čísla z tělesa R. Racionálná funkce $\sqrt{m}$

s racionálnými koefficienty a obecněji racionálná funkce libovolného konečného počtu čísel z $R(\sqrt{m})$ s racionálnými koefficienty, nemá-li jmenovatele $= 0$, je zase číslo z $R(\sqrt{m})$. Je-li m kladné, je $\sqrt{m}$ číslo reálné; všechna čísla z tělesa $R(\sqrt{m})$ jsou reálná, *těleso* nazývá se *reálné*; je-li m záporné, tu jsou v tělese $R(\sqrt{m})$ všechna čísla, která nejsou racionálná, kompleksní, *těleso* nazývá se pak *imaginárné*.

Je ihned jasno, že, označíme-li k libovolné číslo racionálné, je $R(k\sqrt{m}) = R(\sqrt{m})$, Na základě toho lze nahraditi m číslem celým. Je-li totiž $m = m'/m''$, kdež m' a m'' jsou čísla celá, je $R(\sqrt{m}) = R(m''\sqrt{m}) = R(\sqrt{m'm''})$. Dokonce *lze* pak *nahraditi m číslem celým, které není dělitelno čtvercem žádného prvočísla* (od § 4. budeme o m předpokládati, že jest již tak zvoleno).

§ 2. Čísla sdružená, stopa, norma, diskriminant čísla a dvojice čísel.

Kořeny kvadratické rovnice $a_0 x^2 + a_1 x + a_2 = 0$ jsou patrně oba čísla z tělesa $R(\sqrt{a_1^2 - 4a_0 a_2})$, není-li $\sqrt{a_1^2 - 4a_0 a_2}$ číslo racionálné.

Je-li α číslo z tělesa kvadratického $R(\sqrt{m})$, $\alpha = a + b\sqrt{m}$ nazývá se $\alpha' = a - b\sqrt{m}$ *číslem* s ním *sdruženým* v tělese $R(\sqrt{m})$. Naopak je α číslem sdruženým s α'. Čísla spolu sdružená jsou si rovna jedině jsou-li to čísla racionálná.

Součet a součin obou čísel sdružených α, α' jsou čísla racionálná. Součet $S\alpha = \alpha + \alpha' = 2a$ nazývá se někdy *stopou*, součin $N\alpha = \alpha\alpha' = a^2 - b^2 m$ *normou*. Je patrně $S\alpha = S\alpha'$, $N\alpha = N\alpha'$, $N\alpha_1\alpha_2 = N\alpha_1 N\alpha_2$, $N\alpha_1/\alpha_2 = N\alpha_1/N\alpha_2$ pro $\alpha_2 \neq 0$. Jediné číslo z tělesa kvadratického, jehož norma $= 0$, je 0. Norma všech čísel $\neq 0$ z tělesa imagimárného je kladná.

Diskriminant čísla α, $D(\alpha)$ nazývá se výraz $D(\alpha) = (\alpha - \alpha')^2 = 4b^2 m$. Zase je $D(\alpha) = D(\alpha')$. Diskriminant je $= 0$ pouze pro čísla racionálná.

Čísla spolu sdružená α, α' jsou kořeny kvadratické rovnice $(x - \alpha)(x - \alpha') = x^2 - Sa\,x + Na = x^2 - 2a\,x + a^2 - b^2 m = 0$. Její diskriminant je diskriminantem α.

Diskriminantem soustavy dvou čísel $\alpha_1 = a_1 + b_1\sqrt{m}$, $\alpha_2 = a_2 + b_2\sqrt{m}$ nazývá se výraz $D(\alpha_1, \alpha_2) = \begin{vmatrix} \alpha_1 & \alpha_2 \\ \alpha'_1 & \alpha'_2 \end{vmatrix}^2 = 4(a_1 b_2 - a_2 b_1)^2 m$.*)

Je patrně $D(\alpha_1, \alpha_2) = D(\alpha_2, \alpha_1) = D(\alpha'_1, \alpha'_2)$.

Dále je $D(\alpha) = D(1, \alpha)$.

O diskriminantu dvojice čísel z $R(\sqrt{m})$ lze snadno dokázati větu:

Je-li $\beta_1 = c_{11}\alpha_1 + c_{12}\alpha_2$, $\beta_2 = c_{21}\alpha_1 + c_{22}\alpha_2$, platí

$$D(\beta_1, \beta_2) = \begin{vmatrix} c_{11}, & c_{22} \\ c_{21}, & c_{22} \end{vmatrix}^2 D(\alpha_1, \alpha_2).$$

Je totiž $\begin{vmatrix} \beta_1 & \beta_2 \\ \beta'_1 & \beta'_2 \end{vmatrix} = \begin{vmatrix} c_{11}\alpha_1 + c_{12}\alpha_2, & c_{21}\alpha_1 + c_{22}\alpha_2 \\ c_{11}\alpha'_1 + c_{12}\alpha'_2, & c_{21}\alpha'_1 + c_{22}\alpha'_2 \end{vmatrix} =$

$$\begin{vmatrix} c_{11} & c_{12} \\ c_{21} & c_{12} \end{vmatrix} \cdot \begin{vmatrix} \alpha_1 & \alpha_2 \\ \alpha'_1 & \alpha'_2 \end{vmatrix}$$

a utvořením čtverců dostaneme ihned větu uvedenou.

§ 3. Čísla lineárně neodvislá.

Čísla $\alpha_1, \alpha_2, \ldots \alpha_k$ z tělesa $R(\sqrt{m})$ nazveme *lineárně neodvislými*, jestliže rovnice $c_1\alpha_1 + \ldots + c_k\alpha_k$, kdež koeficienty $c_1, c_2, \ldots c_2$ jsou čísla racionálná, může platiti pouze tehdy, když všechny tyto koeficienty jsou $= 0$. V tělese $R(\sqrt{m})$ jsou jistě dvě čísla lineárně nezávislá, totiž 1 a $\sqrt{m}$.

Aby čísla $\alpha_1 = a_1 + b_2\sqrt{m}$, $\alpha_2 = a_2 + b_2\sqrt{m}$, *byla lineárně nezávislá, je nutno a stačí, aby jich diskriminant byl různý od 0.*

Rovnice $c_1\alpha_1 + c_2\alpha_2 = 0$ je splněna racionálnými čísly pouze tehdy, když platí současně rovnice $c_1 a_1 + c_2 a_2 = 0$, $c_1 b_1 + c_2 b_2 = 0$. Těm lze však vyhověti čísly c_1, c_2, jež nejsou obě $= 0$ tehdy a pouze tehdy, když $a_1 b_2 - a_2 b_1 = 0$, t. j když

*) Determinant $\begin{vmatrix} \alpha_1 & \alpha_2 \\ \alpha'_1 & \alpha'_2 \end{vmatrix}$ je zkrácené označen výrazu $\alpha_1\alpha'_2 - \alpha'_1\alpha_2$ ať jsou $\alpha_1, \alpha_2, \alpha'_1, \alpha'_2$ čísla ja á oliv. Dá'e se vyskytující vzor o pro součin determinantů lze jednoduchým výpočtem verifikovati.

$D(\alpha_1, \alpha_2) = 0$. Je-li tedy $D(\alpha_1, \alpha_2) \neq 0$, jsou čísla α_1, α_2 jistě lineárně nezávislá.

Z výrazu pro diskriminant vidíme pak ihned, že *pro všechny dvojice lineárně neodvislých čísel z tělesa* $R(\sqrt{m})$ *má diskriminant totéž znamení a sice jako* m.

Jsou-li $\alpha_1 = a_1 + b_1\sqrt{m}$, $\alpha_2 = a_2 + b_2\sqrt{m}$ *libovolná dvě lineárně nezávislá čísla z* $R(\sqrt{m})$, *lze znázorniti libovolné číslo* $\alpha = a + b\sqrt{m}$ *z* $R(\sqrt{m})$ *ve tvaru* $\alpha = c_1\alpha_1 + c_2\alpha_2$ *s racionálnými koeficienty* c_1, c_2. *Toto znázornění je jednoznačné.*

Aby totiž $\alpha = c_1\alpha_1 + c_2\alpha_2$, je nutno a stačí, aby $a = c_1 a_1 + c_2 a_2$, $b = c_1 b_1 + c_2 b_2$. Rovnice ty lze splniti, je-li $a_1 b_2 - c_2 b_1 \neq 0$, t. j. $D(\alpha_1, \alpha_2) \neq 0$ a určují pak c_1 a c_2 jednoznačně.

Tři čísla α_1, α_2, α_3 *z tělesa* $R(\sqrt{m})$ *jsou vždy lineárně odvislá* (t. j. *nejsou lineárně nezávislá*).

Jsou-li čísla α_1, α_2 lineárně závislá, je rovnice $c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 = 0$ splněna pro $c_3 = 0$. Jsou-li však α_1, α_2 lineárně nezávislá, lze dle předešlé věty určiti c_1, c_2 tak, aby $\alpha_3 = c_1\alpha_1 + c_2\alpha_2$, tak že rovnice $c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 = 0$ je splněna pro $c_3 = -1$.

Jsou-li α_1, α_2 lineárně nezávislá čísla z $R(\sqrt{m})$, dají se libovolná dvě čísla β_1, β_2 znázorniti ve tvaru $\beta_1 = c_{11}\alpha_1 + c_{12}\alpha_2$, $\beta_2 = c_{21}\alpha_1 + c_{22}\alpha_2$ s racionálnými koeficienty c. Snadno lze rozhodnouti, kdy pak budou čísla β_1, β_2 lineárně neodvislá. Ježto $D(\beta_1, \beta_2) = \begin{vmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{vmatrix}^2 D(\alpha_1, \alpha_2)$, patrně tehdy a jen tehdy, když $\begin{vmatrix} c_{11} & c_{12} \\ c_{21} & c_{12} \end{vmatrix} \neq 0$.

§ 4. Čísla celá.

Číslo α z tělesa kvadratického $R(\sqrt{m})$ nazývá se *celé*, je-li kořenem rovnice druhého stupně $x^2 + a_1 x + a_2 = 0$ s racionálnými celými koeficienty a_1, a_2.

Ihned lze dokázati, že *libovolné číslo* β *z tělesa* $R(\sqrt{m})$ ***je podílem dvou čísel celých***, a dokonce, že ***lze za jmenovatele zvoliti číslo celé racionálné.***

Nechť β hoví rovnici $b_0 x^2 + b_1 x + b_2 = 0$, kdež b_0, b_1, b_2 jsou čísla celá racionálná. Rovnici té lze dáti, násobíme-li ji b_0, tvar $(b_0 x)^2 + b_0 b_1 (b_0 x) + b_0^2 b_2 = 0$, z čehož je viděti, že $b_0 \beta = \alpha$ je číslo celé, tak že skutečně $\beta = \alpha / b_0$.

Celé číslo z kvadratického tělesa, které je racionálné, je racionálné celé číslo.

Budiž α celé číslo z tělesa hovící rovnici $x^2 + a_1 x + a_2 = 0$ s racionálnými celými koeficienty. Dejme tomu, že je α číslo racionálné. Vyjádřeme je ve tvaru $\alpha = a/b$, kdež a, b jsou celá čísla nesoudělná, Platí tedy rovnice $\frac{a^2}{b^2} + a_1 \frac{a}{b} + a_2 = 0$, $\frac{a^2}{b} = -(a_1 a + a_2 b)$, tak že musí býti a^2/b celým číslem. Ježto a, b jsou čísla nesoudělná, není to jinak možno než že $b = \pm 1$. Musí tedy býti α celé číslo racionálné.

Číslo α' sdružené s celým číslem α je zase celé, ježto α a α' jsou kořeny téže rovnice kvadratické.

Budeme se nyní zabývati otázkou, v jakém tvaru lze vyjádřiti celé číslo z tělesa $R(\sqrt{m})$. Za účelem zjednodušení dalších úvah budeme předpokládati, že m je celé číslo bez dělitelů kvadratických.

Každé číslo α z tělesa $R(\sqrt{m})$ lze psáti ve tvaru $\alpha = (a + b\sqrt{m})/c$, kdež a, b, c jsou čísla spolu nesoudělná a c kladné. α je kořenem rovnice druhého stupně $x^2 - \frac{2a}{c} x + \frac{a^2 - b^2 m}{c^2} = 0$. Aby bylo α celé číslo musí býti $2a/c$, $(a^2 - b^2 m)/c^2$ celá čísla. I budeme rozeznávati dva případy:

1. c liché. Pak musí býti a dělitelno c a aby bylo $a^2 - b^2 m$ dělitelno c^2, musí býti $b^2 m$ dělitelno c^2. Ježto není m dělitelno čtvercem žádného prvočísla, musí býti b dělitelno c. I je nutně, ježto čísla a, b, c mají býti nesoudělná a $c > 0$, $c = 1$. V tomto případě má celé číslo z tělesa $R(\sqrt{m})$ tvar $a + b\sqrt{m}$, kdež a, b jsou celá čísla racionálná. Naopak čísla tohoto tvaru jsou celá, ježto hoví rovnici s celými koeficienty $x^2 - 2ax + a^2 - mb^2 = 0$.

3. Je-li c sudé, $c = 2c_0$ pak musí býti a/c_0 celé číslo a též $(a^2 - m b^2)/c_0^2$ celé číslo, z čehož plyne nejprve, že musí býti mb^2/c_0^2 celé číslo a tedy jako dříve $c_0 = 1$, $c = 2$. Dále pak musí býti $(a^2 - mb^2)/c^2 = (a^2 - mb^2)/4$ celé číslo, t. j. $a^2 \equiv mb^2 \pmod 4$. Této kongruenci lze vyhověti při $m \equiv 2$ neb 3 jen tak, že a i b

je sudé, což není přípustno, ježto a, b, c jsou dle předpokladu čísla nesoudělná. V tom případě mají tedy všechna celá čísla z $R(\sqrt{m})$ tvar $a + b\sqrt{m}$. Je-li však $m \equiv 1 \pmod 4$, lze kongruenci $a^2 \equiv mb^2 \pmod 4$ splniti též tak, že a i b jsou čísla lichá a v tomto případě jsou v $R(\sqrt{m})$, vedle celých čísel tvaru $a + b\sqrt{m}$ též celá čísla tvaru $\frac{1}{2}(a + b\sqrt{m})$ s a i b lichým. Naopak lze tvrditi, že pro $m \equiv 1 \pmod 4$ jsou čísla tvaru $\frac{1}{2}(a + b\sqrt{m})$ celá, ať jsou a, b jakákoliv čísla lichá. Hoví totiž rovnici $x^2 - ax + \frac{a^2 - mb^2}{4} = 0$ v níž je i prostý člen celý. Možno tedy říci, že pro $m \equiv 1 \pmod 4$ celá čísla z $R(\sqrt{m})$ jsou tvaru $\frac{1}{2}(a + b\sqrt{m})$, kdež a, b jsou čísla celá současně sudá neb současně lichá, t. j. $a \equiv b \pmod 2$. Píšeme-li $b = a + 2\alpha$, vidíme, že pak jsou celá čísla z $R(\sqrt{m})$ tvaru $\alpha + b\frac{1 + \sqrt{m}}{2}$, značí-li, α, b čísla celá racionálná.

Položíme-li $\omega = \sqrt{m}$ *pro* $m \equiv 2$ *neb* $3 \pmod 4$

$\omega = \frac{1}{2}(1 + \sqrt{m})$ *pro* $m \equiv 1 \pmod 4$,

vidíme, že všechna celá čísla z tělesa $R(\sqrt{m})$ *jsou zahrnuta ve tvaru* $a + b\sqrt{m}$, *značí-li* a *i* b *čísla celá racionálná.*

Nyní můžeme snadno dokázati větu:

Součet, rozdíl a součin dvou celých čísel z tělesa kvadratického je zase celé číslo téhož tělesa.

Součet a rozdíl celých čísel $\alpha_1 = a_1 + b_1\omega$ a $\alpha_2 = a_2 + b_2\omega$, $\alpha_1 \pm \alpha_2 = a_1 \pm a_2 + (b_1 \pm b_2)\omega$ hoví jistě podmínkám celistvosti. Abychom to dokázali v součinu $\alpha_1\,\alpha_2$, rozeznávejme případy

1. $m \equiv 2$ neb $3 \pmod 4$, $\omega = \sqrt{m}$;

$\alpha_1\,\alpha_2 = a_1\,a_2 + b_1\,b_2\,m + (a_1\,b_2 + c_2\,b_1)\,\omega$, z čehož vidno, že je to číslo celé.

2. $m \equiv 1 \pmod 4$, $\omega = \frac{1}{2}(1 + \sqrt{m})$, $\omega^2 = \frac{1}{4}(m - 1) + \omega$

$$\alpha_1\,\alpha_2 = a_1\,a_2 + (a_1\,b_2 + c_2\,b_1)\,\omega + b_1\,b_2\,\omega^2$$

$$= a_1\,a_2 - b_1\,b_2\frac{m-1}{4} + (a_1 b_2 + c_2 b_1 + 1)\,\omega$$

takže zase $\alpha_1\,\alpha_2$ je číslo celé.

Jako důsledek plyne ihned věta:

Racionální celá funkce s racionálovými celými koeficienty utvořená z celých čísel z tělesa je zase celé číslo z téhož tělesa kvadratického.

Dále je patrno, že *stopa, norma, diskriminant čísla celého z* $R(\sqrt{m})$ *je celé číslo racionálné. Stejně je tomu s diskriminantem dvou čísel celých.*

§ 5. Base tělesa kvadratického.

Čísla 1, ω mají diskriminant $d = (\omega' - \omega)^2$. I je pro $m \equiv 2$ neb 3 (mod 4) $d = 4m$ a pro $m \equiv 1$ (mod 4) $d = m$. Jsou tedy čísla 1, ω lineárně neodvislá.

Každá dvojice ω_1, ω_2 čísel lineárně neodvislých z tělesa $R(\sqrt{m})$ (pomocí této dvojice lze tedy znázorniti všechna čísla z tělesa jednoznačně ve tvaru $a\,\omega_1 + b\,a_2$, kdež a, b značí čísla racionálná), která nad to má tu vlastnost, že čísla celá jsou znázorněna ve tvaru $a\,\omega_1 + b\,\omega_2$ s racionálovými celými koeficienty a, b, nazývá se *basí tělesa*. Čísla 1, ω tvoří tedy basi tělesa $R(\sqrt{m})$.

Basí je v tělese kvadratickém nekonečně mnoho a lze z jedné z nich odvoditi každou jinou $\overline{\omega}_1$, $\overline{\omega}_2$.

Patrně *musí býti* $D(\omega_1, \omega_2) \neq 0$, $D(\overline{\omega}_1, \overline{\omega}_2) \neq 0$.

1.) $\overline{\omega}_1 = c_{11}\omega_1 + c_{12}\omega_2$, $\overline{\omega}_2 = c_{21}\omega_1 + c_{22}\omega_2$ a též naopak

$\omega_1 = \overline{c}_{11}\overline{\omega}_1 + \overline{c}_{22}\overline{\omega}_2$, $\omega_2 = \overline{c}_{21}\overline{\omega}_1 + \overline{c}_{22}\overline{\omega}_2$, kdež *koefficienty* c *i* $\overline{c}$ *jsou racionálné celé.*

Položíme-li

$$\begin{vmatrix} c_{11} c_{12} \\ c_{21} c_{22} \end{vmatrix} = C, \quad \begin{vmatrix} \overline{c}_{11}, \overline{c}_{12} \\ \overline{c}_{21}, \overline{c}_{22} \end{vmatrix} = \overline{C},$$

bude $D(\omega_1, \omega_2) = \overline{C}^2 D(\overline{\omega}_1, \overline{\omega}_2)$, $D(\overline{\omega}_1, \overline{\omega}_2) = C^2 D(\omega_1, \omega_2)$,

a tedy $C^2\overline{C}^2 = 1$, t. j. $C = \pm 1$, $\overline{C} = \pm 1$

Podmínka $C = \pm 1$ *je nejen nutná, nýbrž také dostačující.* Pak totiž z rovnice 1.)

plyne $\pm\omega_1 = c_{22}\overline{\omega}_1 - c_{12}\overline{\omega}_2$, $\pm\omega_2 = -c_{21}\overline{\omega}_1 + c_{11}\overline{\omega}_2$, zase s celými koefficienty. Celé číslo $\alpha = a\omega_1 + b\omega_2$, kdež a, b jsou

celá čísla racionálná, jest znázorněno pak ve tvaru

$$\alpha = \pm (ac_{22} - bc_{21})\,\overline{\omega_1} \pm (-ac_{12} + bc_{22})\,\overline{\omega_2},$$

při čemž koefficienty u $\overline{\omega_1}$ a ω_2 jsou opět čísla celá racionálná.

Zároveň je patrno, že *pro všecky base má diskriminant tutéž hodnotu d*, která nazývá se *diskriminantem* (*základním číslem*) *tělesa*.

Lze dokázati snadno, že za basi tělesa lze vždy zvoliti dvojici 1, $\frac{1}{2}(d + \sqrt{d})$.

Dvě celá čísla α_1, α_2 z tělesa $R(\sqrt{m})$ lze vyjádřiti ve tvaru $\alpha_1 = a_{11}\omega_1 + a_{12}\omega_2$, $\alpha_2 = a_{21}\omega_1 + a_{22}\omega_2$ s celými racionálnými koefficienty a. Jsou-li α_1, α_2 čísla lineárně neodvislá, netvoří li však basi, je determinant $\begin{vmatrix} a_{11} a_{12} \\ a_{21} a_{22} \end{vmatrix}$ celé číslo $\neq \pm 1$. Z toho plyne, že pak $|D(\alpha_1, \alpha_2)| > |D(\omega_1, \omega_2)|$. Uvažujeme li tedy všechny dvojice lineárně nezávislých čísel z tělesa kvadratického, má diskriminant pro base nejmenší absolutní hodnotu.

§ 6. Dělitelnost, jednotky, čísla associovaná v kvadratickém tělese.

Jsou-li α, β dvě celá čísla z kvadratického tělesa $R(\sqrt{m})$, $\beta \neq 0$, řekneme, že α je *dělitelno* β, je-li α/β číslo celé. Pak lze snadno nahlédnouti platnost vět: *Je-li celé číslo α dělitelno celým číslem $\beta \neq 0$, β dělitelno celým číslem $\gamma \neq 0$, je α dělitelno γ. Jsou-li α, $\varkappa$, β celá čísla, $\beta \neq 0$ a α dělitelno β, je též $\alpha\varkappa$ dělitelno β. Jsou-li čísla celá α, β dělitelna celým číslem $\delta \neq 0$, je $\alpha \pm \beta$ dělitelno δ a obecněji $\lambda\alpha + \mu\beta$ dělitelno δ, značí-li λ, μ libovolná čísla celá.*

Číslo celé ε z $R(\sqrt{m})$ nazývá se *jednotkou*, je-li $1/\varepsilon$ též celé číslo. Z čísel racionálných jsou jednotkami pouze ± 1. *Převratná hodnota jednotky je zase jednotka. Součin a podíl dvou jednotek je zase jednotka. Každé číslo celé je pak dělitelno všemi jednotkami.*

Číslo celé ε z $R(\sqrt{m})$ je jednotkou tehdy a jen tehdy, je-li jeho norma ± 1.

Z $N\varepsilon = \pm 1$ plyne totiž $\varepsilon\varepsilon' = \pm 1$, $1/\varepsilon = \pm\varepsilon'$. Ježto zároveň s ε je ε' celé, je $1/\varepsilon$ celé, tak že je ε skutečně jednotka.

Naopak, je-li ε jednotka, t. j. ε i $1/\varepsilon = \eta$ celé, pak $1 = \varepsilon\eta$ a utvoříme li normy $1 = N\varepsilon N\eta$, kdež $N\varepsilon$ a $N\eta$ jsou celá čísla racionálná. Z toho plyne $N\varepsilon = \pm 1$.

V tělesech kvadratických imaginárných lze snadno jednotky ustanoviti. Dokážeme platnost věty:

V tělese $R(\sqrt{-1})$ *jsou 4 jednotky* ± 1, $\pm i$, *v tělese* $R(\sqrt{-3})$ *je 6 jednotek* ± 1, $\frac{1}{2}(\pm 1 \pm \sqrt{-3})$, *v ostatních tělesech kvadratických imaginárních pouze dvě jednotky* ± 1.

Ježto v imaginárných tělesech jsou normy všech čísel $\neq 0$ kladné, mají všechny jednotky normu $+1$.

Uvažujme nejprvé $R(\sqrt{-1})$. Poněvadž base je zde 1, i, $(i = \sqrt{-1})$, musí býti jednotky tvaru $x + iy$, kdež x, y jsou racionálná celá čísla a $N(x + iy) = x^2 + x^2 = 1$. Tomu lze vyhověti jen tak, že $x = \pm 1$, $y = 0$; $x = 0$, $y = \pm 1$, čemuž odpovídají jednotky $+1$, $\pm i$.

Pro těleso $R(\sqrt{-3})$ je base 1, $\frac{1}{2}(1+\sqrt{-3})$, tak že lze jednotky vyjádřiti ve tvaru $x + \frac{1}{2}(1 + \sqrt{-3})y$ a $N(x + \frac{1}{2}(1 + \sqrt{-3})y) = (x + \frac{1}{2}y)^2 + \frac{3}{4}y^2 = 1$, t. j. $x^2 + xy + y^2 = 1$. Řešení této rovnice jsou $x = \pm 1$, $y = 0$; $x = 1$, $y = -1$; $x = -1$, $y = 1$; $x = 0$, $y = \pm 1$. I dostáváme jako jednotky skutečně ± 1, $\frac{1}{2}(\pm 1 \pm \sqrt{-3})$; jsou mezi nimi třetí kořeny z jednotky 1, $\frac{1}{2}(-1 \pm \sqrt{-3})$.

Pro každé jiné těleso imaginárné $R(\sqrt{m})$ bude celé číslo tvaru $x + \sqrt{m}\,y$ pro $m \equiv 2, 3 \pmod 4$ neb $x + \frac{1}{2}(1 + \sqrt{m})y$ pro $m \equiv 1 \pmod 4$, tak že bude jednotkou, jestliže $x^2 - my^2 = 1$ resp. $(x + \frac{1}{2}y)^2 - \frac{1}{4}my^2 = 1$, t. j. poněvadž $m = -|m|$, jestliže $x^2 + |m|y^2 = 1$, resp. $x^2 + my + \frac{1}{4}(1 + |m|)y^2 = 1$. Při tom je v prvém případě $|m| \geqq 2$, v druhém $|m| \geqq 7$. I musí býti nutně $y = 0$. Neboť kdyby $|y| \geqq 1$, byl by v prvém případě člen $|m|y^2 > 1$, v druhém člen $\frac{1}{4}(1 + |m|)y^2 > 1$.

Pak $x^2 = 1$, tak že jediné jednotky dostáváme pro $x = \pm 1$, $y = 0$, a jsou to ± 1.

Později dokážeme, že v tělesech kvadratických reálných je jednotek nekonečně mnoho a udáme způsob, jak je lze pomocí jedné z nich vyjádřiti.

Dvě čísla α, β z tělesa $R(\sqrt{m})$, jichž podíl je jednotka z tělesa $R(\sqrt{m})$, nazveme spolu *associovanými*, což označíme $\alpha \sim \beta$. I platí vztahy $\alpha \sim \beta$; *z* $\alpha \sim \beta$ *plyne* $\beta \sim \alpha$; *z* $\alpha \sim \beta$,

$\beta \sim \gamma$ *plyne* $\alpha \sim \gamma$; *z* $\alpha_1 \sim \beta_1$, $\alpha_2 \sim \beta_2$ *plyne* $\alpha_1\alpha_2 \sim \beta_1\beta_2$, $\alpha_1/\alpha_2 \sim \beta_1/\beta_2$. Poněvadž čísla associovaná s čísly celými jsou zase celá, *plyne z té okolnosti, že* α_1 *je dělitelno* α_2, $\alpha_1 \sim \beta_1$, $\alpha_2 \sim \beta_2$ *též že* β_1 *je dělitelno* β_2.

§ 7. Čísla nerozložitelná v kvadratickém tělese; v $R(\sqrt{-5})$ neplatí věta o podstatně jednoznačné rozložitelnosti.

Budiž π číslo celé z kvadratického tělesa $R(\sqrt{m})$, které není jednotkou a je dělitelno pouze samo sebou a jednotkami. Takové číslo nazveme *nerozložitelným*.

Mysleme si, že jsme celé číslo α z $R(\sqrt{m})$ rozložili na nerozložitelné činitele. I můžeme si položiti otázku: Je ten rozklad možný v podstatě jediným způsobem? Rozklad je možný v podstatě jediným způsobem, znamená pak, že eksistuje-li vedle rozkladu $\alpha = \pi_1\pi_2 \ldots \pi_k$ v nerozložitelné činitele ještě podobný rozklad $\alpha = \varkappa_1\varkappa_2 \ldots \varkappa_l$, je nutně každý činitel $\varkappa$ associován s jistým činitelem π, tak že pak nutně $l = k$.

Ukážeme, že tomu tak není pro každé těleso kvadratické na tělese $R(\sqrt{-5})$.

$R(\sqrt{-5})$ má basi 1, $\sqrt{-5}$. Je to těleso imaginárné, tak že jednotky jsou pouze ± 1.

Pro číslo 6 platí rozklady $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Čísla celá 2, 3, $1+\sqrt{-5}$, $1-\sqrt{-5}$ jsou *a*) nerozložitelná, *b*) žádná dvě nejsou spolu associována.

a) Dejme tomu, že by bylo $2 = \alpha\beta$, kdež α, β jsou čísla celá nejednotková. Pak by pro normy musilo platiti $4 = N\alpha N\beta$, $N\alpha > 1$, $N\beta > 1$, a tedy $N\alpha = N\beta = 2$. Kdyby $\alpha = a + b\sqrt{-5}$, kdež a, b jsou čísla racionálná celá, musilo by býti $a^2 + 5b^2 = 2$ čemuž nelze vyhověti. Je tedy 2 skutečně číslo nerozložitelné. Podobně by se to dokázalo o 3.

Kdyby bylo $1+\sqrt{-5} = \alpha\beta$, pak by pro normy musilo platiti $6 = N\alpha N\beta$, $N\alpha \neq 1$, $N\beta \neq 1$ a tedy $N\alpha = 2$, $N\beta = 3$ neb naopak. To však není možno. Podobně při $1-\sqrt{-5}$.

b) Že není 2 associováno ani se 3, ani s $1+\sqrt{-5}$, ani s $1-\sqrt{-5}$, plyne z toho, že by pak musilo býti $N2 = N3$ resp. $= N(1+\sqrt{-5})$, $= N(1-\sqrt{-5})$, jest však $N2 = 4$, $N3 = 9$, $N(1+\sqrt{-5}) = N(1-\sqrt{-5}) = 6$. Podobně se do-

káže o 3, že není associováno ani s $1+\sqrt{-5}$ ani s $1-\sqrt{-5}$. Čísla $1+\sqrt{-5}$, $1-\sqrt{-5}$ mají sice stejnou normu 6, nejsou však spolu associována: jich podíl $\frac{1+\sqrt{-5}}{1-\sqrt{-5}} = 1+\frac{1}{3}\sqrt{-5}$ není celé číslo.

Uveďme další příklady rozkladu téhož čísla v nerozložitelné činitele podstatně různé:

$$9 = 3.3 = (2+\sqrt{-5})(2-\sqrt{-5})$$
$$21 = 3.7 = (4+\sqrt{-5})(4-\sqrt{-5}) =$$
$$= (1+2\sqrt{-5})(1-2\sqrt{-5}).$$

Abychom pravidla dělitelnosti mohli v kvadratických tělesech pohodlně vyjádřiti, zavedeme pojem divisorů. Za tím účelem budeme nejprvé definovati pojem dělitelnosti vzhledem k prvočíslu v tělesech racionálných a pak kvadratických.

(Dokončení.)

Geometrické sestrojování stereoskopických obrazců.

Dr. **Klíma Josef.**

Při vyučování deskriptivní geometrii v sedmé třídě reálky možno jako vhodnou a žáky zajímající aplikaci perspektivního zobrazování sestrojovati stereoskopické obrazce, čehož lze na př. na ryse použíti.

Perspektivné obrazy, jež sestrojují se z jediného centra S, bylo by třeba pozorovati též jediným okem, které je nad hlavním bodem ve vzdálenosti příslušné distance. K tomuto správnému dívání se na perspektivní obraz buď sestrojený geometricky neb pořízený fotografickou cestou slouží přístroj mající jen jedinou čočku.

Ježto však obyčejně předmět pozorujeme oběma očima současně dostáváme pro každé oko jiný zorný kužel t. j. jiný obrys na tělese a tudíž pro každé oko jiný perspektivní obraz. Rozdíly jsou tu tím patrnější, čím předmět je bližší. Nejjasněji se o tom přesvědčíme pozorujeme-li současně s tělesem předměty za ním jsoucí t. zv. pozadí; tu pokaždé jiná část pozadí je zakryta