Математичка гимназија у Београду
Додатна настава за трећи и четврти разред
09.10.2005.

Раширења поља $\mathbb{Q}$

Миливоје Лукић

1. Теоријски увод

Нека је K поље. *Валуација* поља K је свако пресликавање $|\ |: K \to [0, +\infty)$ такво да:
(i) $|x| = 0 \Leftrightarrow x = 0$,
(ii) $|xy| = |x| \cdot |y|$ за све $x, y \in K$,
(iii) $|x + y| \leq \max\{|x|, |y|\}$

Ако је $|\ |_1$ валуација поља K, онда је валуација и $|\ |_2 = |\ |_1^c$, за било који позитиван реалан број c. Ако једну валуацију можемо добити од друге на овај начин, тада кажемо да су те две валуације еквивалентне.
Пример: за сваки прост број p, дефинишимо валуацију $|\ |_p$ поља $\mathbb{Q}$ са $|0|_p = 0$ и

$$\left|p^a \frac{u}{v}\right|_p = \frac{1}{p^a}\ , \qquad \text{за } \gcd(u,p) = \gcd(v,p) = 1. \tag{1}$$

Напоменимо да је према теореми Островског свака валуација поља $\mathbb{Q}$ еквивалентна некој од валуација $|\ |_p$.

Приметимо да је

$$\mathbb{Z} = \left\{x \in \mathbb{Q} \;\middle|\; |x|_p \leq 1 \text{ за све } p\right\}. \tag{2}$$

Мотивисани формулом (2), за коначно раширење K поља $\mathbb{Q}$, дефинишимо прстен "целих" бројева у пољу K као

$$O_K = \left\{x \in K \;\middle|\; |x| \leq 1 \text{ за све валуације } |\ | \text{ поља } K\right\}. \tag{3}$$

Непосредно се проверава да је O_K заиста потпрстен од K.

Осврнимо се на још један могућ приступ дефинисању прстена O_K: Како је K коначно раширење од $\mathbb{Q}$, K је и алгебарско раширење над $\mathbb{Q}$. Дакле, за сваки $\alpha \in K$ постоји полином $p(x) \in \mathbb{Q}[x]$ такав да $p(\alpha) = 0$. Другим речима, постоје $a_0, a_1, \ldots, a_n \in \mathbb{Q}$ такви да

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0. \tag{4}$$

Алтернативно се O_K може дефинисати као скуп свих $\alpha \in K$ таквих да постоје $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ такви да

$$a_0 + a_1\alpha + \cdots + \alpha^n = 0. \tag{5}$$

Ова дефиниција је еквивалентна са дефиницијом датом једначином (3).

2. Квадратна раширења поља $\mathbb{Q}$

Свако квадратно раширење поља $\mathbb{Q}$ је облика

$$\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} | a, b \in \mathbb{Q}\}, \tag{6}$$

где је d цео број различит од 0 и 1 који није дељив квадратом ниједног простог броја. Као специјални случај ранијег разматрања,

$$\alpha \in O_{\mathbb{Q}[\sqrt{d}]} \iff (\exists a_0, a_1 \in \mathbb{Z}) a_0 + a_1\alpha + \alpha^2 = 0. \tag{7}$$

Из претходне формуле се непосредно изводи

$$O_{\mathbb{Q}[\sqrt{d}]} = \begin{cases} \mathbb{Z} + \mathbb{Z}\sqrt{d} & \text{за} \quad d \equiv 2,3 \pmod 4 \\ \mathbb{Z} + \mathbb{Z}\dfrac{1+\sqrt{d}}{2} & \text{за} \quad d \equiv 1 \pmod 4 \end{cases} \tag{8}$$

Дакле, супротно "очигледном" избору да за целе бројеве раширења $\mathbb{Q}[\sqrt{d}]$ одаберемо бројеве облика $a + b\sqrt{d}$, где су $a, b \in \mathbb{Z}$, за $d \equiv 1 \pmod 4$ скуп целих бројева је нешто шири и садржи и бројеве облика $a + b\sqrt{d} + \frac{1+\sqrt{d}}{2}$, $a, b \in \mathbb{Z}$.

3. Норма у квадратним раширењима поља $\mathbb{Q}$

У $\mathbb{Q}[\sqrt{d}]$, дефинишимо норму $N : \mathbb{Q}[\sqrt{d}] \to \mathbb{Q}$ са

$$N(a + b\sqrt{d}) = a^2 - db^2. \tag{9}$$

Приметимо да важи

$$(\forall x, y \in \mathbb{Q}[\sqrt{d}])\ N(xy) = N(x)N(y), \tag{10}$$

$$N(x) = 0 \iff x = 0. \tag{11}$$

У даљем тексту прстен целих бројева $O_{\mathbb{Q}[\sqrt{d}]}$ краће ћемо означавати са R. Непосредно се проверава да важи

$$x \in R \ \Rightarrow\ N(x) \in \mathbb{Z}, \tag{12}$$

па норму можемо посматрати и као пресликавање из R у $\mathbb{Z}$.

Јединица у прстену R је сваки број $\epsilon \in R$ за који постоји $\delta \in R$ такво да $\epsilon\delta = 1$. Нормирањем обе стране закључујемо да је ϵ јединица у R ако и само ако је $N(\epsilon) = 1$. На пример, у прстену $\mathbb{Z}$ једине јединице су бројеви 1 и -1. Затим, ако је $N(\pi) = p$, где је p прост број у прстену $\mathbb{Z}$, онда је π прост број у прстену R.

Релација дељивости се уводи на уобичајени начин: за $\alpha, \beta \in R$, $\alpha \neq 0$,

$$\alpha | \beta \iff (\exists \gamma \in R)\beta = \alpha\gamma. \tag{13}$$

Бројеви α и β су *асоцирани* ако $\alpha|\beta$ и $\beta|\alpha$, односно ако постоји јединица ϵ таква да $\alpha = \epsilon\beta$.

Напоменимо да прстени $O_{\mathbb{Q}[\sqrt{d}]}$ немају увек својство јединствене факторизације: на пример, за $d = -13$,

$$49 = 7^2 = (6 + \sqrt{-13})(6 - \sqrt{-13}),$$

при чему су 7, $6 + \sqrt{-13}$, $6 - \sqrt{-13}$ нерастављиви у $O_{\mathbb{Q}[\sqrt{-13}]}$.

Теорема: Свако Еуклидско раширење има својство јединствене факторизације.

Теорема: За $d = -11, -7, -3, -2, -1, 2, 3, 5$, поље $\mathbb{Q}[\sqrt{d}]$ је Еуклидско. (Важи и општије тврђење: поље $\mathbb{Q}[\sqrt{d}]$ је Еуклидско ако и само ако је d један од бројева -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57 и 73.)

4. Прости бројеви у квадратним раширењима поља $\mathbb{Q}$

Опишимо сада просте бројеве у квадратним раширењима поља Q: нека је $R = O_{\mathbb{Q}[\sqrt{d}]}$ Еуклидски прстен. Користићемо ознаку p за просте бројеве прстена $\mathbb{Z}$ и ознаку π за просте бројеве прстена R. Од значаја ће бити *дискриминанта* раширења δ, при чему је $\delta = 4d$ за $d \equiv 2,3 \pmod 4$ и $\delta = d$ за $d \equiv 1 \pmod 4$. Разматрањем факторизације броја p у прстену R, испоставља се да су могућа три случаја:

1. $p|\delta$: У овом случају $p = \epsilon\pi^2$, где је ϵ јединица, а π прост број у R.
2. $p \nmid \delta$ и $\left(\frac{d}{p}\right) = -1$ за $p > 2$, односно $d \equiv 5 \pmod 8$ за $p = 2$: У овом случају $p = \pi$, то јест p остаје прост број у R.

3. $p \nmid \delta$ и $\left(\frac{d}{p}\right) = 1$ за $p > 2$, односно $d \equiv 1 \pmod 8$ за $p = 2$: У овом случају $p = \pi_1\pi_2$, при чему је $\pi_2 = \bar{\pi}_1$ и π_1 и π_2 нису асоцирани.

Обратно, сваки прост број π прстена R добија се у факторизацији тачно једног p.

5. Задаци

1. Описати јединице и просте бројеве прстена $\mathbb{Z}[i]$.
2. Који прости бројеви p се могу представити у облику $p = x^2 + 2y^2$?
3. Због чега идентитети $6^2 = (5+\sqrt{-11})(5-\sqrt{-11})$ и $3^2 = (2+\sqrt{-5})(2-\sqrt{-5})$ не показују да прстени $O_{\mathbb{Q}[\sqrt{-11}]}$ и $O_{\mathbb{Q}[\sqrt{-5}]}$ немају јединствену факторизацију?
4. Наћи потребан и довољан услов за $x, y \in \mathbb{Z}$ да у $\mathbb{Z}[i]$ важи $\gcd(2, x+yi) = 1$.
5. Решити једначину $x^2 + 2 = y^3$ у скупу целих бројева.
6. Решити једначину $x^2 + 4 = y^3$ у скупу целих бројева.
7. Решити једначину $x^2 + 11 = y^3$ у скупу целих бројева.
8. Нека су a, b, c природни бројеви такви да $ab = c^2+1$. Доказати да постоје $m, n, p, q \in \mathbb{N}$ такви да $a = m^2 + n^2$, $b = p^2 + q^2$, $c = mp + nq$.
9. Доказати: Ако су x, y, z цели бројеви такви да $x^2 + 3y^2 = z^3$, $\gcd(x, y) = 1$, $3 \nmid x$, онда постоје цели бројеви a и b такви да је $a^2 + 3b^2 = z$.
10. Решити једначину $x^2 = y^5 - 1$ у скупу целих бројева.
11. (БМО1998.4) Доказати да једначина $y^2 = x^5 - 4$ нема решења у скупу целих бројева.
12. (Велика Фермаова теорема, случај $n = 3$) Решити једначину $x^3 + y^3 + z^3 = 0$ у скупу целих бројева.