АЛГЕБРА

Количнички прстени, Кинеска теорема, примитивни корени

Зоран Петровић

23. мај 2011.

У даљем ћемо претпоставити да су сви идеали са којима радимо прави, тј. да нису једнаки целом прстену.

Дефиниција 1 Нека је $I \triangleleft A$. На A дефинишемо релацију конгруенције по модулу I са:

$$a \equiv b \pmod{I} \quad \textbf{акко} \quad a - b \in I.$$

Проверимо да је ова релација заиста конгруенција.

Рефлексивност: Како је $a - a = 0 \in I$, то је заиста $a \equiv a \pmod{I}$ за све $a \in A$.

Симетричност: Нека је $a \equiv b \pmod{I}$. То значи да $a - b \in I$, но, множењем са (-1) добијамо да и $b - a = (-1)(a - b)$ припада I.

Транзитивност: Нека је $a \equiv b \pmod{I}$ и $b \equiv c \pmod{I}$. Дакле, $a - b \in I$ и $b - c \in I$. Но, тада је и

$$a - c = (a - b) + (b - c) \in I.$$

Слагање са $+$: Нека је $a \equiv a' \pmod{I}$ и $b \equiv b' \pmod{I}$. Дакле, $a - a' \in I$ и $b - b' \in I$. Добијамо да је

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I.$$

Слагање са $\cdot$: Нека је $a \equiv a' \pmod{I}$ и $b \equiv b' \pmod{I}$. Дакле, $a - a' \in I$ и $b - b' \in I$. Добијамо да је

$$a \cdot b - a' \cdot b' = (a \cdot b - a' \cdot b) + (a' \cdot b - a' \cdot b') = (a - a') \cdot b + a' \cdot (b - b') \in I.$$

Приметимо да је класа еквиваленције елемента a заправо скуп

$$a + I = \{a + x : x \in I\}.$$

Скуп класа еквиваленције означавамо са A/I. На основу претходног добијамо да је структура $(A/I, +, \cdot)$ један комутативан прстен са јединицом где су операције $+$ и $\cdot$ дефинисане са:

$$(a+I)+(b+I) := (a+b)+I, \quad (a+I)\cdot(b+I) := (a\cdot b)+I.$$

Наравно да неке од ових заграда нећемо увек записивати.

Као и у случају група, важе и теореме о изоморфизмима за прстене. Навешћемо само прву.

Теорема 2 *(*Теорема о изоморфизмима за прстене*)* Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Тада је $\tilde{f}\colon A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ задато са:

$$\tilde{f}(a+\mathrm{Ker}(f)) := f(a)$$

изоморфизам комутативних прстена са јединицом.

Доказ. Проверимо најпре да је $\tilde{f}$ добро дефинисано. У ту сврху, нека је $a+\mathrm{Ker}(f) = b+\mathrm{Ker}(f)$. То значи да $a-b \in \mathrm{Ker}(f)$, тј. да је $f(a) = f(b)$. Закључујемо да је $\tilde{f}$ заиста добро дефинисано.

Проверимо да је $\tilde{f}$ хомоморфизам.

$$\tilde{f}((a+\mathrm{Ker}(f))+(b+\mathrm{Ker}(f))) = \tilde{f}((a+b)+\mathrm{Ker}(f)) = f(a+b) =$$

$$= f(a)+f(b) = \tilde{f}(a+\mathrm{Ker}(f)) + \tilde{f}(b+\mathrm{Ker}(f)).$$

$$\tilde{f}((a+\mathrm{Ker}(f))\cdot(b+\mathrm{Ker}(f))) = \tilde{f}((a\cdot b)+\mathrm{Ker}(f)) = f(a\cdot b) =$$

$$= f(a)\cdot f(b) = \tilde{f}(a+\mathrm{Ker}(f)) \cdot \tilde{f}(b+\mathrm{Ker}(f)).$$

Јасно је да је $\tilde{f}$ „на“. Остаје да се провери да је $\tilde{f}$ „1–1“.

$$\begin{aligned} \tilde{f}(a+\mathrm{Ker}(f)) = \tilde{f}(b+\mathrm{Ker}(f)) &\implies f(a) = f(b) \\ &\implies f(a-b) = 0 \\ &\implies a-b \in \mathrm{Ker}(f) \\ &\implies a+\mathrm{Ker}(f) = b+\mathrm{Ker}(f). \end{aligned}$$

Проверимо још и да $\tilde{f}$ слика јединицу прстена у јединицу прстена:

$$\tilde{f}(1_A+\mathrm{Ker}(f) = f(1_A) = 1_B.$$

Закључујемо да је $\tilde{f}$ заиста један изоморфизам комутативних прстена са јединицом. □

Пример 3 Нека је $I \lhd A$. Тада је $p\colon A \to A/I$ један епиморфизам. ♣

Пример 4 За све $n \geq 1$ важи: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Хомоморфизам $\rho_n: \mathbb{Z} \to \mathbb{Z}_n$, дат раније, је „на“, а осим тога $\mathrm{Ker}(\rho_n) = n\mathbb{Z}$, те резултат следи. ♣

Већ смо у претходној лекцији навели појам директног производа два прстена, а и познат нам је општи појам директног производа алгебри, но ипак дајмо и ту дефиницију.

Дефиниција 5 Нека су $(A_1, +^1, \cdot^1), \ldots (A_n, +^n, \cdot^n)$ комутативни прстени са јединицом. На Декартовом производу

$$A = A_1 \times \cdots \times A_n,$$

задајемо структуру комутативног прстена са јединицом са:

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) := (a_1 +^1 b_1, \ldots, a_n +^n b_n)$$

$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) := (a_1 \cdot^1 b_1, \ldots, a_n \cdot^n b_n)$$

Приметимо да је $0_A = (0_1, \ldots, 0_n)$ и $1_A = (1_1, \ldots, 1_n)$.

Став 6 Нека су $m_1, \ldots, m_n$ позитивни цели бројеви за које важи: $\mathrm{NZD}(m_i, m_j) = 1$ за све $i \neq j$. Тада је

$$\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z}).$$

Доказ. Дефинишимо хомоморфизам

$$f: \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$$

са:

$$f(x) = (x + m_1\mathbb{Z}, \ldots, x + m_n\mathbb{Z}).$$

Остављамо читаоцима да провере да је f заиста хомоморфизам. Одредимо језгро овог хомоморфизма. Нека је $x \in \mathrm{Ker}(f)$. То значи да је $f(x) = (m_1\mathbb{Z}, \ldots, m_n\mathbb{Z})$, тј. то значи да $x \in m_1\mathbb{Z}$, $\ldots$, $x \in m_n\mathbb{Z}$. Дакле, у језгру се налазе они цели бројеви, који су дељиви свим бројевима $m_1, \ldots, m_n$. Како су m_i узајамно прости то језгро чине умношци од $m_1 \cdots m_n$, тј.

$$\mathrm{Ker}(f) = (m_1 \cdots m_n)\mathbb{Z}.$$

Добијамо да је

$$\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z} \cong \mathrm{Im}(f).$$

Но, како је $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$, то је

$$|\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z}| = m_1 \cdots m_n = |(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})|.$$

Закључујемо да f мора бити „на“. Тиме смо добили тражени изоморфизам. □

Последица 7 *(*Кинеска теорема о остацима*)* Нека су $m_1, \ldots, m_n$ позитивни цели бројеви који су пар по пар узајамно прости и $x_1, \ldots, x_n$ произвољни цели бројеви. Тада постоји цео број x такав да је

$$x \equiv x_1 \pmod{m_1}$$
$$x \equiv x_2 \pmod{m_2}$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$x \equiv x_n \pmod{m_n}$$

Ако је x' неки други цео број који задовољава наведени систем конгруенција, онда је

$$x \equiv x' \pmod{m_1 \cdots m_n}.$$

Доказ. Посматрајмо елемент

$$(x_1 + m_1\mathbb{Z}, \ldots, x_n + m_n\mathbb{Z}) \in (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z}).$$

Како је хомоморфизам f, из доказа претходне теореме, „на“, то постоји $x \in \mathbb{Z}$ који се слика у наведени елемент, тј. постоји $x \in \mathbb{Z}$ за који је

$$x + m_1\mathbb{Z} = x_1 + m_1\mathbb{Z}, \quad \ldots \quad , x + m_n\mathbb{Z} = x_n + m_n\mathbb{Z},$$

но, то управо значи да је

$$x \equiv x_1 \pmod{m_1}, \quad \ldots \quad , x \equiv x_n \pmod{m_n}.$$

Уколико је x' други цео број који задовољава наведене конгруенције, то значи да је $f(x) = f(x')$, тј.

$$x - x' \in \mathrm{Ker}(f) = (m_1 \cdots m_n)\mathbb{Z},$$

као што је и тврђено. □

Став 8 Ако су прстени A и B изоморфни, онда је $(U(A), \cdot) \cong (U(B), \cdot)$

Доказ. Јасно је да се инвертибилни елементи при сваком хомоморфизму сликају у инвертибилне елементе. Наиме, ако је $a \in U(A)$, то значи да постоји a' такав да је $a \cdot a' = 1_A$. Но, тада је $f(a) \cdot f(a') = f(a \cdot a') = f(1_A) = 1_B$, па и $f(a)$ има инверз.

Према томе, $f[U(A)] \subseteq U(B)$ за сваки хомоморфизам $f\colon A \to B$. Уколико је f изоморфизам и $b \in U(B)$, то постоји $a \in A$ такав да је $f(a) = b$. Но, елемент b има инверз, па је $b \cdot b' = 1_B$ за неки $b' \in B$. Елемент b' је слика неког елемента a': $f(a') = b'$. Но, тада је $f(a \cdot a') = f(a) \cdot f(a') = b \cdot b' = 1_B$, те како је f „1–1“, мора бити $a \cdot a' = 1_A$ те a има инверз. Закључујемо да f успоставља бијекцију између $U(A)$ и $U(B)$. Како је f хомоморфизам, добијамо тражени изоморфизам. □

Став 9 Важи једнакост: $U(A_1 \times \cdots \times A_n) = U(A_1) \times \cdots \times U(A_n)$.

Доказ. Нека је $a = (a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$. Тада

$$\begin{aligned} a \in U(A_1 \times \cdots \times A_n) &\iff \text{постоји } b \in A : a \cdot b = 1 \\ &\iff \text{постоје } b_i \in A_i \text{ т. д. } a_i \cdot b_i = 1 \text{ за све } i \\ &\iff a_1 \in U(A_1), \ldots, a_n \in U(A_n) \\ &\iff a \in U(A_1) \times \cdots \times U(A_n). \end{aligned}$$

□

Теорема 10 Ако су $m_1, \ldots, m_n$ пар по пар узајамно прости позитивни цели бројеви, онда је

$$\mathbb{Z}_{m_1 \cdots m_n} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$$

и

$$\varphi(m_1 \cdots m_n) = \varphi(m_1) \cdots \varphi(m_n),$$

где је φ Ојлерова функција.

Доказ. Како је $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$, то први резултат следи из Става 6. Осим тога, $\varphi(m) = |U(\mathbb{Z}_m)|$, те резултат за Ојлерову функцију следи из Става 8 и Става 9. □

Групе $U(\mathbb{Z}_n)$ имају занимљиву структуру, но ми се њима нећемо детаљно бавити. Но, ипак ћемо, због примена, доказати да је за сваки прост број p група $U(\mathbb{Z}_p)$ циклична. Заправо, доказаћемо општији резултат, али пре тога морамо да докажемо нешто у вези Абелових група.

Став 11 Нека је A Абелова група реда m и нека за свако d, које дели m постоји највише d елемената $a \in A$ за које је $da = 0$. Тада је група A циклична.

Доказ. Докажимо најпре следећи резултат, који је и сам по себи занимљив:

$$\sum_{d|m} \varphi(d) = m.$$

Посматрајмо цикличну групу G реда m. Као што знамо она има тачно једну подгрупу реда d за сваки d који је делилац броја m. Осим тога, циклична група реда d има тачно $\varphi(d)$ генератора. Следи да у цикличној групи реда m има тачно $\varphi(d)$ елемената реда d (сваки елемент реда d генеришу исту подгрупу групе G) за свако d које дели m. Стога једнакост следи.

Вратимо се нашој групи A. Означимо са $\psi(d)$ број елемената реда d у A. Сваки елемент $x \in A$ је неког реда d, где $d \mid m$. То значи да је

$$\sum_{d|m} \psi(d) = m.$$

С друге стране, ако је $\psi(d) > 0$, онда у групи A постоји елемент a, који је реда d. Посматрајмо подгрупу A' генерисану тим елементом. У њој има d елемената и за свако $z \in A'$ важи $dz = 0$. То значи да су сви елементи $x \in A$ за које је $dx = 0$ садржани у подгрупи A'. Дакле, сваки елемент реда d у A је садржан у цикличној подгрупи A', која је реда d. Но, ми знамо да у цикличној групи реда d има тачно $\varphi(d)$ генератора, тј. елемената реда d. Закључујемо да важи следеће: ако је за неко d, које дели m, $\psi(d) > 0$, онда је за то d: $\psi(d) = \varphi(d)$. С обзиром да је

$$\sum_{d|m} \varphi(d) = m = \sum_{d|m} \psi(d),$$

закључујемо да је за све d, који деле m испуњено $\psi(d) = \varphi(d)$. То посебно значи да је и $\psi(m) = \varphi(m) > 0$, па у A има елемената реда m, те је група A заиста циклична. □

Теорема 12 Нека је F поље и G коначна подгрупа групе $(F \setminus \{0\}, \cdot)$. Тада је G циклична група.

Доказ. Покажимо најпре да сваки полином $p(X)$ из $F[X]$ степена n има највише n нула у пољу F. Доказ се изводи индукцијом по степену полинома $p(X)$.

$n = 1$: Овде нема шта да се доказује, јасно је да полином има тачно једну нулу у F.

Претпоставимо да је $n > 1$ и да је тврђење тачно за све полиноме степена мањег од n. Ако полином $p(X)$ нема ниједну нулу у пољу F, онда је тврђење испуњено. Претпоставимо да $p(X)$ има неку нулу $a \in F$. Еуклидско дељење полинома $p(X)$ полиномом $X - a$ даје:

$$p(X) = (X - a)q(X) + r,$$

где је $r = 0$, или је то константан не-нула полином. Но, с обзиром да је $p(a) = 0$, добијамо да је $r = 0$. Стога је $p(X) = (X - a)q(X)$. Полином $q(X)$ је степена $n-1$ и по индукцијској хипотези има највише $n-1$ нулу у F. Како је свака нула полинома $p(X)$ или једнака a или је нека нула полинома $q(X)$ закључујемо да $p(X)$ има највише n нула у F.

Пређимо сада на доказ наше теореме. Теорему ћемо доказати тако што ћемо се уверити да група G испуњава услове претходног става (јасно је да је G комутативна група). С обзиром да овде користимо мултипликативну нотацију, треба да покажемо да за сваки d који дели ред групе G, у групи G има највише d елемената a за које је $a^d = 1$. Но, $G \subset F$ и елемент $a \in G$ за који је $a^d = 1$ у G(тј. у F) је заправо нула полинома $X^d - 1$ из $F[X]$. Ово је полином степена d и према претходно доказаном, он има највише d нула у F. Закључујемо да су услови за примену претходног става испуњени те добијамо да је G циклична група. □

Дакле, доказали смо да је свака коначна подгрупа мултипликативне групе поља циклична. Истакнимо још једном да се ради о коначним подгрупама. Наравно да мултипликативна група произвољног поља F, тј. група $(F \setminus \{0\}, \cdot)$ не мора бити циклична! Нпр. $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ сигурно нису цикличне (ти скупови су непребројиви!).

Погледајмо како можемо искористити чињеницу да је $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ циклична група. Пре свега, уведимо терминологију.

Дефиниција 13 Ма који генератор групе $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ зове се примитивни корен модуло p.

Став 14 Нека је r ма који примитивни корен модуло p. Тада је са:

$$\mathrm{ind}_r(a) = x \textbf{ акко } r^x = a,$$

дефинисан изоморфизам $\mathrm{ind}_r \colon (\mathbb{Z}_p \setminus \{0\}, \cdot_p) \to (\mathbb{Z}_{p-1}, +_{p-1})$.

Доказ. Овај став је заправо само преформулација и прецизирање тврђења да је група $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ циклична.

Како је r примитивни корен модуло p, то за свако $a \in \mathbb{Z}_p \setminus \{0\}$ постоји тачно једно $x \in \mathbb{Z}_{p-1}$ за које је $r^x = a$. Наиме, r је генератор наведене групе, па је сваки елемент у тој групи неки степен од r. Како та група има $p-1$ елемената, то $x \in \mathbb{Z}_{p-1}$. Ми треба да проверимо да ли је ind_r хомоморфизам, тј. да ли је

$$\mathrm{ind}_r(a \cdot_p b) = \mathrm{ind}_r(a) +_{p-1} \mathrm{ind}_r(b),$$

за све $a, b \in \mathbb{Z}_p \setminus \{0\}$. Нека је $x = \mathrm{ind}_r(a)$ и $y = \mathrm{ind}_r(b)$. Дакле, $r^x = a$ и $r^y = b$. Тада је

$$a \cdot_p b = r^x \cdot_p r^y = r^{x+y}.$$

С обзиром на чињеницу да је $\omega(r) = p - 1$, то је

$$r^{x+y} = r^{x +_{p-1} y},$$

па добијамо да је

$$a \cdot_p b = r^{x +_{p-1} y},$$

те је

$$\mathrm{ind}_r(a \cdot_p b) = x +_{p-1} y = \mathrm{ind}_r(a) +_{p-1} \mathrm{ind}_r(b).$$

Дакле, ind_r је заиста хомоморфизам, а да је бијекција следи из чињенице да је $\omega(r) = p - 1$. □

Пример 15 Наћи све примитивне корене модуло 13.

За почетак потражимо бар један примитивни корен. Почнимо од 2:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 3, \quad 2^5 = 6, \quad 2^6 = 12, \quad 2^7 = 11, \quad 2^8 = 9$$

$$2^9 = 5, \quad 2^{10} = 10, \quad 2^{11} = 7, \quad 2^{12} = 1.$$

Дакле, заиста је $\langle 2 \rangle = \mathbb{Z}_{13} \setminus \{0\}$. Да бисмо нашли све примитивне корене модуло 13, направимо таблицу за ind_2.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2(a)$	12	1	4	2	9	5	11	3	8	10	7	6

С обзиром да је $2^{\mathrm{ind}_2(a)} = a$, није тешко извршити проверу.

Ова таблица нам омогућава да нађемо и све остале примитивне корене модуло 13. Наиме, подсетимо се да важи следеће:

Ако је $\omega(r) = n$ онда је $\omega(r^m) = n$ ако и само ако је $\mathrm{NZD}(n, m) = 1$.

Пошто је у нашем случају $\omega(2) = 12$, то је $\omega(2^m) = 12$ ако и само ако је $\mathrm{NZD}(m, 12) = 1$, тј. ако и само ако је $m \in \{1, 5, 7, 11\}$. Дакле, остали примитивни корени по модулу 13 су: $6 (= 2^5)$, $11 (= 2^7)$ и $7 (= 2^{11})$. ♣

Пример 16 Решити конгруенцију

$$x^5 \equiv 7 \pmod{13}.$$

Већ знамо да је 2 примитивни корен по модулу 13. Применом $\beth\ltimes_2$ на дату конгруенцију добијамо да је

$$5y \equiv 11 \pmod{12},$$

где смо са y означили $\mathrm{ind}_2(x) \in \mathbb{Z}_{12}$. Тако смо применом ind_2 једну конгруенцију петог степена свели на линеарну, која се лако може решити. С обзиром да је $5 \cdot_{12} 5 = 1$, добијамо да је

$$y \equiv 7 \pmod{12}.$$

Дакле, како је $y = \mathrm{ind}_2(x)$, добијамо да је

$$x \equiv 11 \pmod{13}.$$

♣