АЛГЕБРА 2

Комутативни прстени са јединицом

Хомоморфизми и количнички прстени

Зоран Петровић

17. април 2012.

Од сада претпостављамо 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. □

Заправо, у произвољном прстену важи одговарајућа теорема, коју такође називамо Кинеском теоремом о остацима. Потребна нам је најпре једна дефиниција.

Дефиниција 8 Идеали I и J комутативног прстена са јединицом A су копрости уколико је $I + J = A$.

Теорема 9 (Кинеска теорема о остацима) Нека су идеали $I_1, \ldots, I_n$ комутативног прстена са јединицом A пар по пар узајамно прости. Тада важи изоморфизам:

$$A/(I_1 \cap \ldots \cap I_n) \cong A/I_1 \times \cdots \times A/I_n.$$

Доказ. Доказ је нешто тежи него у случају прстема целих бројева. Посматрамо хомоморфизам $f\colon A \to A_1 \times \cdots \times A_n$ дефинисан са:

$$f(x) = (x + I_1, \ldots, x + I_n).$$

Није тешко проверити да је ова функција заиста један хомоморфизам (проверите то).

Јасно је да је језгро овог хомоморфизма пресек свих идеала. Једино треба проверити да је f „на".

Приметимо да важи следећи резултат. Ако су I и J копрости, а такође и I и K, онда су и I и JK такође копрости. Наиме, како су I и J копрости следи да је $I + J = A$. Посебно, постоји $x_1 \in I$ и $y \in J$ такви да је $x_1 + y = 1$. Слично, постоји $x_2 \in I$ и $z \in K$ тако да је $x_2 + z = 1$. Множењем ове две једнакости добијамо

$$(x_1x_2 + x_1z + x_2y) + yz = 1.$$

Како $x_1x_2 + x_1z + x_2y \in I$, а $yz \in JK$ (зашто?), то $1 \in I + JK$, те мора бити $I + JK = A$ (зашто?), па су I и JK узајамно прости. Из овог резултата следи да је за свако $i = \overline{1,n}$ испуњено:

$$I_i \text{ и } \prod_{j \neq i} I_j \text{ су копрости.}$$

Наравно са $\prod_{j\neq i} I_j$ смо означили производ свих идеала I_j за $j \neq i$.

Дакле, за $i = \overline{1,n}$, постоје $a_i \in I_i$ и $b_i \in \prod_{j\neq i} I_j$ такви да је $a_i + b_i = 1$. То посебно значи да је $b_i \equiv 1 \pmod{I_i}$ и $b_i \equiv 0 \pmod{I_j}$, за све $j \neq i$ (зашто?).

Докажимо сада да је f „на". Нека је $(x_1 + I_1, \ldots, x_n + I_n)$ произвољни елемент из $A/I_1 \times \cdots \times A/I_n$. Уочимо елемент $x = b_1x_1 + \cdots + b_nx_n$, где су b_i претходно изабрани елементи. Тада је, за све i:

$$x = b_1x_1 + \cdots + b_ix_i + \cdots + b_nx_n \equiv 0 \cdot x_1 + \cdots + 1 \cdot x_i + \cdots + 0 \cdot x_n \pmod{I_i}.$$

Дакле, за све $i = \overline{1,n}$: $x \equiv x_i \pmod{I_i}$, а то управо значи да је

$$f(x) = (x_1 + I_1, \ldots, x_n + I_n).$$

Закључујемо да је f заиста „на". □

Напомена. Приметимо да за копросте идеале I и J важи следећа једнакост: $I \cdot J = I \cap J$.

Доказ. Увек је $I \cdot J \subseteq I \cap J$ (зашто?). Дакле, потребно је доказати само обратну инклузију. Како су I и J копрости, то постоје $x \in I$ и $y \in J$ тако да важи $x + y = 1$. Нека је $z \in I \cap J$ произвољан елемент. Тада је

$$z = z \cdot 1 = z \cdot (x + y) = z \cdot x + z \cdot y.$$

Како $x \in I$ и $z \in J$, то је $z \cdot x \in I \cdot J$ (радимо са комутативним прстенима, па је $z \cdot x = x \cdot z$. Такође и $z \cdot y \in I \cdot J$, па закључујемо да и z припада пресеку $I \cap J$. $\square$

Питање: Чему одговара резултат из напомене у случају целих бројева?

Јасно је да се претходни резултат генералише на произвољан коначан производ идеала. Размислите како се претходна Кинеска теорема за комутативне прстене може формулисати имајући у виду претходно доказано.