АЛГЕБРА 2

Комутативни прстени са јединицом
Идеали и хомоморфизми

Зоран Петровић

3. април 2012.

Као што у теорији група имамо појам подгрупе неке групе, тако и у теорији комутативних прстена са јединицом имамо појам потпрстена са јединицом.

Дефиниција 1 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ комутативни прстени са јединицом при чему је $B \subseteq A$. Уколико је за све $x, y \in B$ испуњено:

$$x + y = x +' y, \quad x \cdot y = x \cdot' y$$

и $1_A = 1_B$, онда је B један потпрстен са јединицом прстена A.

Приметимо да такође важи и $0_A = 0_B$, но та се чињеница може извести из преосталих, што није тачно за једнакост $1_A = 1_B$. На пример, нека је $A = \{(0,0), (0,1), (1,0), (1,1)\}$ и $B = \{(0,0), (1,0)\}$, где су операције дефинисане по координатама, а на свакој координати су сабирање, односно множење по модулу 2. Тада B јесте комутативан прстен са јединицом, но јединица у B је елемент $(1,0)$, а јединица у A је $(1,1)$. Стога B није потпрстен са јединицом прстена A.

Важнији од појма потпрстена је појам идеала.

Дефиниција 2 Нека је A комутативан прстен са јединицом и I непразан подскуп од A. Тада је I идеал у A уколико

1. за све $x, y \in I$: $x + y \in I$;
2. за све $a \in A$ и $x \in I$: $a \cdot x \in I$.

Приметимо да $0 \in I$ за сваки идеал I. Наиме, како је I непразан, то постоји $x \in I$. Но, тада је и $0 = 0 \cdot x \in I$. Ознака $I \lhd A$ означава да је I идеал у A.

Са идеалима се могу вршити операције сабирања и множења као и са елементима.

Дефиниција 3 Нека су I и J идеали прстена A.

1. $I + J := \{x + y : x \in I, y \in J\}$;
2. $I \cdot J := \{x_1y_1 + \cdots + x_ny_n : x_i \in I$ за све $i = \overline{1,n}, y_j \in J$ за све $j = \overline{1,n},$ и све $n \geq 1\}$.

Директна провера показује да су $I + J$ и $I \cdot J$ заиста идеали у прстену A. Идеал $I + J$ је најмањи идеал, који садржи (као своје подскупове) идеале I и J, док је $I \cdot J$ заправо најмањи идеал који садржи све могуће производе елемената из I са елементима из J.

Као и у случају подгрупа, пресек два идеала $I \cap J$ јесте идеал, док је њихова унија $I \cup J$ идеал ако и само ако је један од тих идеала садржан у другом. Заправо, ако посматрамо само операцију сабирања, приметимо да су идеали подгрупе групе $(A, +)$, а знамо да из чињенице да је унија две подгрупе подгрупа, следи да је једна од њих садржана у другој. Други смер се лако проверава.

Наведимо неке примере.

Пример 4 Ако је A комутативан прстен са јединицом и $a \in A$ произвољан елемент, онда је

$$\langle a \rangle := \{r \cdot a : r \in A\},$$

идеал. Овај идеал се назива главни идеал генерисан елементом a.

Како је $r \cdot a + s \cdot a = (r + s) \cdot a$, као и $s \cdot (r \cdot a) = (sr) \cdot a$, видимо да је $\langle a \rangle$ заиста идеал у прстену A. ♣

Пример 5 Сваки идеал у $\mathbb{Z}$ је облика $\langle m \rangle$ за неки природан број m.

Нека је $I \lhd \mathbb{Z}$. Како је $(I, +)$ подгрупа групе $(\mathbb{Z}, +)$, то на основу претходног знања о подгрупама групе $\mathbb{Z}$, добијамо да је $I = \langle m \rangle$. ♣

Напомена. Идеал $\langle m \rangle$ означава се и са $m\mathbb{Z}$ (скуп свих целобројних умножака броја m).

Пример 6 Нека су m и n позитивни цели бројеви. Одредити:

$$\langle m \rangle \cdot \langle n \rangle, \quad \langle m \rangle + \langle n \rangle, \quad \langle m \rangle \cap \langle n \rangle.$$

Пре свега, $\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle$ важи у сваком прстену и за све елементе a и b (проверите!). Стога је $\langle m \rangle \cdot \langle n \rangle = \langle mn \rangle$. На основу дефиниције:

$$\langle m \rangle + \langle n \rangle = \{mx + ny : x, y \in \mathbb{Z}\}.$$

Како ми знамо да је $\langle m \rangle + \langle n \rangle$ сигурно главни идеал, потребно је само одредити који је његов генератор. Но, није потребно много размишљати о томе. Из горње једнакости се просто намеће да је

$$\langle m \rangle + \langle n \rangle = \langle d \rangle,$$

где је $d = \mathrm{NZD}(m, n)$. Пре свега, добро нам је познато да увек постоје $p, q \in \mathbb{Z}$ за које је $mp + nq = d$. Стога, $d \in \langle m \rangle + \langle n \rangle$, па мора бити и

$\langle d\rangle \subseteq \langle m\rangle + \langle n\rangle$. Но, како $d \mid m$ и $d \mid n$, то постоје m_1 и n_1 такви да је $m = dm_1$ и $n = dn_1$. Уколико је $mx+ny$ произвољан елемент из $\langle m\rangle+\langle n\rangle$ добијамо:

$$mx + ny = dm_1x + dn_1y = d(m_1x + n_1y),$$

те закључујемо да $mx + ny \in \langle d\rangle$

Одредимо још и $\langle m\rangle \cap \langle n\rangle$. Приметимо да $x \in \langle m\rangle \cap \langle n\rangle$ ако и само ако $m \mid x$ и $n \mid x$. Но, то управо значи да је $\langle m\rangle \cap \langle n\rangle = \langle \mathrm{NZS}(m, n)\rangle$. ♣

Пример 7 У прстену $\mathbb{Z}[X]$ постоји идеал који није главни.

Посматрајмо идеал I генерисан са два елемента 2 и X, $I = \langle 2, X\rangle$ (ознака $\langle S\rangle$ означава најмањи идеал (који увек постоји јер је пресек ма које колекције идеала идеал) који садржи скуп S; у случају да је $S = \{x_1, \ldots, x_n\}$ пишемо $\langle x_1, \ldots, x_n\rangle$, уместо $\langle\{x_1, \ldots, x_n\}\rangle$). Овај идеал сигурно није главни. Наиме, претпоставимо да је

$$\langle 2, X\rangle = \langle a(X)\rangle,$$

за неки полином $a(X)$. Како је $2 \in \langle a(X)\rangle$, то мора бити $2 = a(X) \cdot b(X)$ за неки полином $b(X)$. То значи да је $a(X)$ константан полином. Но, из чињенице да $X \in \langle a(X)\rangle$, следи да $a(X) \mid X$, па мора бити $a(X) = 1$, или $a(X) = -1$. То би значило да је $1 = 2p(X) + Xq(X)$ за неке полиноме $p(X), q(X) \in \mathbb{Z}[X]$. Но, заменом 0 уместо X добијамо да је тада $1 = 2p(0)$, те би следило да $\frac{1}{2} \in \mathbb{Z}$. Закључујемо да наведени идеал није главни. ♣

Пример 8 Нека је K ма које поље. Тада је сваки идеал у прстену $K[X]$ главни.

У доказу ћемо користити чињеницу да за полиноме $a(X)$ и $b(X)$ из $K[X]$ за које је $b(X) \neq 0$ постоје и једнозначно су одређени полиноми, $q(X)$ и $r(X)$ такви да је

$$a(X) = q(X)b(X) + r(X), \quad r(X) = 0 \text{ или } \deg r(X) < \deg b(X).$$

Ово је познато еуклидско дељење полинома, или дељење са остатком, са којим смо упознати у средњој школи (додуше само за реалне, односно комплексне полиноме, али лако се види да се овакво дељење може извести у ма ком пољу).

Нека је $I \lhd K[X]$. Уколико је $I = \{0\}$, јасно је да је I главни идеал генерисан елементом 0. Претпоставимо стога да је $I \neq \{0\}$. Нека је μ моничан полином најмањег степена који се налази у I. Тај полином сигурно постоји пошто је I идеал. Докажимо да је $I = \langle\mu\rangle$. Посматрајмо произвољни елемент $a \in I$. На основу резултата наведеног горе, постоје полиноми q и r (читалац сигурно примећује да понекад полиноме означавамо са $a(X)$, а понекад и само са a, као и да производ два елемента у прстену понекад пишемо без ознаке операције множења)

такви да је $a = q\mu + r$, при чему је степен полинома r мањи од степена полинома μ, или је $r = 0$. Како $a, \mu \in I$, добијамо да је $r = a - q\mu$ такође из I. Но, уколико је $r \neq 0$, множењем инверзом водећег коефицијента од r добили бисмо да се у I налази моничан полином степена мањег од степена полинома μ што противречи избору полинома μ. Закључујемо да мора бити $r = 0$, тј. да $\mu \mid a$, те да $a \in \langle \mu \rangle$, чиме је доказ завршен.♣

Пример 9 Нека је K поље и $I \lhd K$. Тада је $I = \{0\}$, или је $I = K$.

Претпоставимо да је I идеал у K и да је $I \neq \{0\}$. То значи да идеал I садржи неки елемент $x \neq 0$. Уколико је a ма који елемент из K, добијамо да и a припада идеалу I. Наиме, како је I идеал, а $x \neq 0$, то постоји x^{-1} и елемент $(ax^{-1}) \cdot x$ мора припадати идеалу I, а јасно је да је тај елемент једнак елементу a. ♣

Пример 10 Нека је A ма који комутативан прстен са јединицом и $u \in U(A)$. Тада је $\langle u \rangle = A$.

Доказ се изводи на исти начин као у претходном примеру. ♣

Пређимо сада на појам хомоморфизма прстена.

Дефиниција 11 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ два комутативна прстена са јединицом. Функција $f\colon A \to B$ је хомоморфизам прстена уколико је $f(1_A) = 1_B$ и уколико за све $x, y \in A$ важи:

$$f(x + y) = f(x) +' f(y) \quad \text{и} \quad f(x \cdot y) = f(x) \cdot' f(y).$$

Пример 12 Функција $\rho_n\colon \mathbb{Z} \to \mathbb{Z}_n$ задата са $\rho_n(x) := \rho(x, n)$, где је са $\rho(x, n)$ означен остатак при дељењу x са n, је један хомоморфизам прстена.

Овај хомоморфизам ћемо искористити да опишемо идеале у прстенима $\mathbb{Z}_n$, но пре тога ћемо навести неке опште резултате о хомоморфизмима.

Дефиниција 13 Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Језгро хомоморфизма f, у ознаци $\mathrm{Ker}(f)$ дефинише се са:

$$\mathrm{Ker}(f) := \{x \in A : f(x) = 0_B\}.$$

Став 14 Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Тада важи:

а) $\mathrm{Ker}(f) \lhd A$;

б) ако је $J \lhd B$ онда је $f^{-1}[J] \lhd A$;

в) ако је $I \lhd A$ и f „на“, онда је $f[I] \lhd B$.

Доказ.

а) Нека $x, y \in \mathrm{Ker}(f)$. Тада је

$$f(x+y) = f(x) +' f(y) = 0_B +' 0_B = 0_B,$$

па $x + y \in \mathrm{Ker}(f)$.

Уколико је $x \in \mathrm{Ker}(f)$ и $a \in A$:

$$f(a \cdot x) = f(a) \cdot' f(x) = f(a) \cdot' 0_B = 0_B,$$

те $a \cdot x \in \mathrm{Ker}(f)$.

б) Нека је J идеал у B и $x, y \in f^{-1}[J]$. То значи да је $f(x) \in J$ и $f(y) \in J$. Како је J идеал, закључујемо да и $f(x+y) = f(x) +' f(y) \in J$. Дакле, $x + y \in f^{-1}[J]$.

Такође, уколико је $x \in f^{-1}[J]$ и $a \in A$, добијамо да је $f(a \cdot x) = f(a) \cdot' f(x) \in J$, пошто $f(x) \in J$, а J је идеал.

в) Нека су $u, v \in f[I]$. То значи да је $u = f(x)$ и $v = f(y)$ за неке $x, y \in I$. Како је I идеал, то је $x + y \in I$, а како је $u +' v = f(x) +' f(y) = f(x+y)$, закључујемо да је $u +' v \in f[I]$.

Уколико је $u \in f[I]$, а $b \in B$, с обзиром да је по претпоставци f „на“, добијамо да постоји $a \in A$ тако да је $b = f(a)$. Осим тога је $u = f(x)$ за неко $x \in I$. Како је I идеал, $a \cdot x$ припада I, па је $b \cdot' u = f(a) \cdot f(x) = f(a \cdot x)$ из $f[I]$. □

Приметимо да је, као и у случају хомоморфизма група, $\mathrm{Ker}(f) = \{0\}$ ако и само ако је хомоморфизам инјективан.

У општем случају директна слика идеала не мора бити идеал. На пример, јасно је да функција $i\colon \mathbb{Z} \to \mathbb{Q}$ дефинисана са $i(x) = x$ за све $x \in \mathbb{Z}$, јесте хомоморфизам (то је инклузија прстена целих бројева у поље рационалних бројева). Но,

$$i[\langle 2 \rangle] = \{2m : m \in \mathbb{Z}\},$$

а то очигледно није идеал у $\mathbb{Q}$, пошто су, на основу раније доказаног, једини идеали у $\mathbb{Q}$: $\{0\}$ и $\mathbb{Q}$.

Пример 15 Нека је $n \geq 2$ цео број. Тада је сваки идеал у $\mathbb{Z}_n$ главни.

Искористићемо хомоморфизам $\rho_n\colon \mathbb{Z} \to \mathbb{Z}_n$, који је и „на“. Нека је $J \lhd \mathbb{Z}_n$. Тада је $\rho_n^{-1}[J] \lhd \mathbb{Z}$. На основу структуре идеала прстена $\mathbb{Z}$, знамо да постоји $m \geq 0$ такав да је $\rho_n^{-1}[J] = \langle m \rangle$. Но, тада је

$$J = \rho_n[\rho_n^{-1}[J]] = \rho_n[\langle m \rangle] = \langle \rho_n(m) \rangle.$$

Приметимо да једнакост $J = \rho_n[\rho_n^{-1}[J]]$ следи из чињенице да је ρ_n „на“, док је јасно да је $f[\langle a \rangle] = \langle f(a) \rangle$ за сваки епиморфизам (хомоморфизам који је „на“) f и сваки елемент a (покажите да је ово тачно!). ♣

Напомена. Можда је читалац приметио да смо овај резултат могли да докажемо као и у случају прстена целих бројева. Наиме, сваки идеал у $\mathbb{Z}_n$ је и подгрупа цикличне групе, па је тиме и сама циклична. А знамо како изгледају цикличне подгрупе групе $\mathbb{Z}_n$. У овом доказу само треба обратити пажњу на чињеницу да је свака подгрупа од $\mathbb{Z}_n$ заиста идеал (у случају прстена $\mathbb{Z}$, то је тривијално испуњено, пошто се множење елементима из $\mathbb{Z}$ заправо своди на сабирање (уз евентуално множење са -1 које одговара тражењу супротног елемента). Чињеница да је то испуњено и за $\mathbb{Z}_n$ захтева мали доказ. Размислите мало о томе.

Пример 16 Навести пример комутативног прстена са јединицом и подгрупе адитивне групе тог прстена, која није идеал.

Посматрамо прстен $A = \mathbb{Z}_2 \times \mathbb{Z}_2$. Овде су операције дефинисане по координатама и заправо је A директан производ прстена $\mathbb{Z}_2$ и $\mathbb{Z}_2$ (поновите појам директног производа алгебри). Скуп $\{(0,0),(1,1)\}$ је подгрупа адитивне групе тог прстена, али није идеал пошто елемент $(1,0)\cdot(1,1) = (1,0)$ не припада том скупу, а $(1,1)$ му припада. ♣

Пример 17 Наћи све идеале у прстену $\mathbb{Z}_{12}$.

Знамо да су сви идеали у овом прстену главни. Такође знамо да је сваки елемент у $\mathbb{Z}_{12}$ или делитељ нуле или инвертибилан. Како сваки инвертибилан елемент генерише, према једном од раније наведених примера, цео прстен, остаје да се види које идеале генеришу делитељи нуле. Приметимо да је $m \in Z_{12}$ делитељ нуле ако и само ако $2 \mid m$ или $3 \mid m$ (зашто?). Стога је

$$Z(\mathbb{Z}_{12}) = \{0, 2, 3, 4, 6, 8, 9, 10\}.$$

Приметимо да, пошто је $5 \in U(\mathbb{Z}_{12})$ и $10 = 5 \cdot_{12} 2$ имамо да је $\langle 10\rangle = \langle 2\rangle$ (размислите како се ово може генерализати). Такође је $9 = -3 = (-1)\cdot 3$, па је и $\langle 9\rangle = \langle 3\rangle$. Добијамо да је и $\langle 8\rangle = \langle 4\rangle$.

С друге стране, $\langle 2\rangle \neq \langle 4\rangle$. Наиме, претпоставимо да $2 \in \langle 4\rangle$. Тада би постојао $m \in Z_{12}$ такав да је $2 = 4 \cdot_{12} m$. То би значило да постоји цео број q такав да је $2 = 4m + 12q$. Дељењем са 2 добили бисмо да је $1 = 2m + 6q$ за неке целе бројеве m и q што свакако није могуће. Како је очигледно $4 \in \langle 2\rangle$, то добијамо да је $\langle 4\rangle \subset \langle 2\rangle$ (идеал генерисан са 4 је прави подскуп идеала генерисаног са 2). На сличан начин се добија да је $\langle 6\rangle \subset \langle 3\rangle$. Читаоцима остављамо да се увере да су сви различити идеали прстена $\mathbb{Z}_{12}$ следећи:

$$\langle 0\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle, \mathbb{Z}_{12}.$$