АЛГЕБРА 2

Комутативни прстени са јединицом

Прости и максимални идеали

Зоран Петровић

24. април 2012.

Започнимо ову лекцију следећим ставом

Став 1 Нека је A комутативан прстен са јединицом и $P \triangleleft A$ ($P \neq A$). Следећи услови су еквивалентни.

1. За $I, J \triangleleft A$ важи: ако је $I \cdot J \subseteq P$, онда $I \subseteq P$ или $J \subseteq P$.
2. За $a, b \in A$ важи: ако $ab \in P$, онда $a \in P$ или $b \in P$.
3. Прстен A/P је област целих.

Доказ. Подсетимо се најпре да се област целих дефинише као комутативан прстен са јединицом у коме нема правих делитеља нуле, тј. у коме важи: ако је $ab = 0$, онда је $a = 0$ или $b = 0$.

$1 \Longrightarrow 2$. Уочимо идеале $I = \langle a \rangle$, $J = \langle b \rangle$. Како је $I \cdot J = \langle ab \rangle$ и $ab \in P$, то $I \cdot J \subseteq P$. На основу 1. следи да $I \subseteq P$, или $J \subseteq P$, тј. $a \in P$, или $b \in P$.

$2 \Longrightarrow 3$. Претпоставимо да за елементе $x, y \in A/P$ важи: $xy = 0$. Како су то елементи из количничког прстена, то постоје $a, b \in A$ такви да је $x = a + P$ и $y = b + P$ и да важи: $(a + P)(b + P) = P$. Ова једнакост се своди на $ab + P = P$, тј. на $ab \in P$. На основу 2. добијамо да $a \in P$, или $b \in P$, односно $a + P = P$ или $b + P = P$, тј. $x = 0$, или $y = 0$.

$3 \Longrightarrow 1$. Нека су идеали I, J прстена A такви да је $I \cdot J \subseteq P$, а да $I \not\subseteq P$ и $J \not\subseteq P$. То значи да постоји $a \in I \setminus P$ и $b \in J \setminus P$. Но, $ab \in I \cdot J \subseteq P$, па је $(a + P)(b + P) = ab + P = P$. Како је A/P област целих, следи да $a \in P$, или $b \in P$. Ова контрадикција завршава доказ. □

Дефиниција 2 Идеал $P \triangleleft A$ је прост уколико испуњава неко од претходна три еквивалентна својства.

Приметимо да, уколико је P прост идеал, а $a_1, \ldots, a_n \in A$, онда из $a_1 \cdots a_n \in P$ следи да $a_i \in P$ за неко $i \in \{1, \ldots, n\}$ (што се лако доказује индукцијом по n).

У основној школи смо научили да је природан број прост уколико нема других делилаца сем 1 и њега самог (ово такође важи и за број 1, али се он не сматра простим бројем). Но, у произвољној области целих разликује се појам простог и нерастављивог елемента. Подсетимо се да са $U(A)$ означавамо скуп свих инвертибилних елемената у прстену A.

Дефиниција 3 Нека је A област целих. Елемент $p \in A \setminus (U(A) \cup \{0\})$ је

- прост, уколико за $a, b \in A$ важи: ако $p \mid ab$, онда $p \mid a$, или $p \mid b$;
- нерастављив уколико за $a, b \in A$ важи: ако је $p = ab$, онда је $a \in U(A)$, или $b \in U(A)$.

Веза између простих и нерастављивих елемената у произвољном прстену дата је следећим ставом.

Став 4 Сваки прост елемент је нерастављив.

Доказ. Претпоставимо да је p прост и да је $p = ab$. Посебно то значи да p дели производ ab. Како је p прост, то $p \mid a$, или $p \mid b$. Нека, на пример, $p \mid a$. То значи да постоји $c \in A$ за који је $a = pc$. Како је $p = ab$, то је $p = pcb$, тј. $p(1 - cb) = 0$, па мора бити $1 - cb = 0$, пошто је A област целих. Дакле, $cb = 1$, те је елемент b инвертибилан. □

У произвољној области целих, прости и нерастављиви елементи се разликују. Размотримо следећи пример.

Пример 5 У прстену $\mathbb{Z}\left[\sqrt{-5}\right]$ елемент 3 је нерастављив, али није прост.

Пре свега,

$$\mathbb{Z}\left[\sqrt{-5}\right] := \{p(\sqrt{-5}) : p \in \mathbb{Z}[X]\}.$$

Но, није тешко уверити се да из дефиниције следи да је

$$\mathbb{Z}\left[\sqrt{-5}\right] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Уверимо се најпре да је 3 нерастављив. Претпоставимо да је $3 = uv$. Уведимо ознаку $N(z) := z\overline{z}$, за $z \in \mathbb{Z}\left[\sqrt{-5}\right]$ (наравно да је $N(z)$ квадрат модула комплексног броја z). Јасно је да је $N(z_1 z_2) = N(z_1)N(z_2)$ за све z_1, z_2. Добијамо да је $N(3) = N(u)N(v)$, односно $9 = N(u)N(v)$. Ово је факторизација природног броја 9 у скупу природних бројева, то имамо две могућности:

1) један од $N(u)$, $N(v)$ једнак је 1, а други 9;

2) $N(u) = N(v) = 3$.

1) Претпоставимо, на пример, да је $N(u) = 1$. Уколико је $u = a + b\sqrt{-5}$, добијамо да је $1 = N(u) = u\overline{u} = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$. С обзиром да $a, b \in \mathbb{Z}$, ово је могуће једино ако је $b = 0$ и $a \in \{-1, 1\}$, тј. $u \in \{-1, 1\}$, те следи да је u инвертибилан (било би добро да читаоци

сами покажу, за вежбу, да је $U(\mathbb{Z}\left[\sqrt{-5}\right] = \{-1, 1\}$ користећи функцију N).

2) Поступамо на сличан начин. Уколико је $u = a + b\sqrt{-5}$, добијамо да је $3 = N(u) = a^2 + 5b^2$. С обзиром да $a, b \in \mathbb{Z}$, мора бити $b = 0$ и добијамо да је $3 = a^2$, за неко $a \in \mathbb{Z}$. Ово наравно није могуће, те закључујемо да се слуцај 2) и не појављује.

Дакле, из чињенице да је $3 = uv$, добијамо да је један од фактора инвертибилан, а то заправо значи да је 3 нерастављив.

Остаје да покажемо да 3 није прост. посматрајмо факторизацију броја 9 у $\mathbb{Z}\left[\sqrt{-5}\right]$:

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Како је $9 = 3 \cdot 3$, то

$$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Покажимо да 3 не дели ниједан од ових фактора. Из те чињенице ће следити да 3 није прост.

Нека $3 \mid 2 + \sqrt{-5}$ (аналогно се разматра и други случај). Дакле, за неки елемент $u \in \mathbb{Z}\left[\sqrt{-5}\right]$:

$$3 \cdot u = 2 + \sqrt{-5}.$$

Применом функције N добијамо

$$9 \cdot N(u) = 9.$$

Добијамо да је $N(u) = 1$, те је $u \in \{-1, 1\}$, тј. $3 = 2 + \sqrt{-5}$, или $3 = -(2 + \sqrt{-5})$. Ова контрадикција нам показује да 3 не дели $2 + \sqrt{-5}$, тј. 3 заиста није прост. ♣

Напомена 6 Приметимо да једнакост $3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ даје две различите факторизације броја 9 у производ нерастављивих. То је нешто са чиме се нисмо срели у случају целих бројева. Више ћемо о овоме рећи у наредним предавањима.

Пример 7 У прстену тригонометријских полинома $A = \mathbb{R}[\sin x, \cos x]$ наћи пример неједнозначне факторизације на нерастављиве елементе.

Читаоци би требало да буду упознати са овим прстеном из курса Анализе 2 (Фуријеови редови и сл.). Заправо, није тешко показати да је сваки елемент из A облика $a_0 + \sum_{k=1}^{n}(a_k \cos kx + b_k \sin kx)$ (по дефиницији је $A = \{p(\sin x, \cos x) : p \in \mathbb{R}[X, Y]\}$). Познати идентитет $\sin^2 x + \cos^2 x = 1$ даје тражене факторизације:

$$\cos x \cdot \cos x = (1 - \sin x)(1 + \sin x).$$

Остављамо читаоцима за вежбу да покажу нерастављивост функција које се појављују у овој факторизацији (знање Анализе 2 може бити

корисно за ово, али није и неопходно – довољно је знање адиционих формула и једноставно рачунање интеграла функција облика $\sin kx$ и $\cos kx$) .

Следећи став је помало и очекиван.

Став 8 Елемент је прост ако и само ако је идеал генерисан тим елементом прост идеал.

Доказ. Нека је p прост елемент у прстену A и $\langle p\rangle$ идеал генерисан тим елементом. Уколико $ab \in \langle p\rangle$, онда је $ab = pc$ за неки $c \in A$, тј. $p \mid ab$. Како је елемент p прост, то $p \mid a$, или $p \mid b$, односно, $a \in \langle p\rangle$, или $b \in \langle p\rangle$, те закључујемо да је $\langle p\rangle$ прост идеал.

Обратно, претпоставимо да је $\langle p\rangle$ прост идеал и нека $p \mid ab$. То значи да $ab \in \langle p\rangle$, те следи да $a \in \langle p\rangle$, или $b \in \langle p\rangle$, односно $p \mid a$, или $p \mid b$. □

За крај ове приче о простим идеалима, наведимо једну интересантну теорему.

Теорема 9 (Теорема о избегавању простих идеала) Нека су $P_1, \ldots, P_n$ прости идеали прстена A и $I \triangleleft A$. Ако је $I \subseteq P_1 \cup \ldots \cup P_n$, онда је $I \subseteq P_i$ за неко $i \in \{1, \ldots, n\}$.

Доказ. Изводимо доказ индукцијом по n. Случај $n = 1$ је тривијалан. Претпоставимо да је $n > 1$ и да је тврђење тачно уколико је I садржан у унији мање од n простих идеала. Нека је $I \subseteq P_1 \cup \ldots \cup P_n$, при чему су сви ови прости. Уколико је I садржано у некој од унија $\cup_{j\neq i} P_j$ (за неко i), онда резултат следи на основу индуктивне хипотезе. Претпоставимо, стога, да $I \not\subseteq \cup_{j\neq i} P_j$ за све $i = \overline{1,n}$. Дакле, постоје елементи $x_i \in I \setminus \cup_{j\neq i} P_j$. Посматрамо елемент $x = x_1 + x_2 \cdots x_n$. Како је $x_i \in I \setminus \cup_{j\neq i} P_j$, а $I \subseteq P_1 \cup \ldots \cup P_n$, то $x_i \in P_i$. Поставља се питање где се налази елемент x. Уколико $x \in P_1$, онда $x_2 \cdots x_n \in P_1$ (јер $x_1 \in P_1$), те из чињенице да је P_1 прост, следи да $x_j \in P_1$ за неко $j \neq i$, што није тачно. Дакле, $x \notin P_1$. Следи да $x \in P_j$ за неко $j \neq 1$. Како и $x_j \in P_j$, то и производ $x_2 \cdots x_n$ припада P_j, те следи да и $x_1 = x - x_2 \cdots x_n \in P_j$. Ова контрадикција завршава доказ. □

Пређимо сада на појам максималног идеала.

Дефиниција 10 Идеал M прстена A је максималан, уколико не постоји идеал I прстена A за који важи: $M \subset I \subset A$.

Дакле, максималан идеал је прави идеал за који не постоји прави идеал, различит од њега, који га садржи као свој подскуп.

Став 11 Нека је M прави идеал прстена A. Тада је M максималан идеал ако и само ако је A/M поље.

Доказ. Претпоставимо да је M максималан идеал и $a + M \neq M$. Треба показати да $a + M$ има инверз у прстену A/M. Посматрамо идеал

$\langle a\rangle + M$. Како $a \notin M$, то је M прави подскуп од $\langle a\rangle + M$. Но, с обзиром да је M максималан идеал, мора бити $\langle a\rangle + M = A$. То значи да постоје $b \in A$ и $m \in M$ за које је $ab + m = 1$. Дакле, $ab - 1 = m \in M$, па је $ab + M = 1 + M$, те је $b + M$ тражени инверз елемента $a + M \in M$.

Обратно, претпоставимо да је A/M поље. Нека је M прави подскуп идеала I. Дакле, постоји $a \in I \setminus M$. Стога је $a + M \neq M$ у количничком прстену A/M. Како је овај прстен по претпоставци поље, то постоји $b \in M$ тако да је $(a + M)(b + M) = 1 + M$, односно, $ab - 1 \in M$. Дакле, за неко $m \in M$ важи: $ab - 1 = m$, тј. $1 \in ab - m$. Како и a и m припадају идеалу I, то и $1 \in I$, па мора бити $I = A$. Закључујемо да је M заиста максималан идеал у A. □

Напомена 12 Видимо да из овог става следи да је сваки максималан идеал уједно и прост идеал, пошто у пољу нема правих делитеља нуле.

Веза између нерастављивих елемената и максималних идеала дата је следећим ставом.

Став 13 Елемент $a \in A$ је нерастављив ако и само ако је идеал $\langle a\rangle$ максималан у скупу свих главних идеала прстена A.

Доказ. Претпоставимо да је $a \in A$ нерастављив и нека је $\langle a\rangle \subseteq \langle b\rangle$. Треба да покажемо да је $\langle a\rangle = \langle b\rangle$ или $\langle b\rangle = A$. Како је $\langle a\rangle \subseteq \langle b\rangle$, то $a \in \langle b\rangle$, па постоји $c \in A$ тако да је $a = bc$. Како је a нерастављив, то $b \in U(A)$, или $c \in U(A)$. Уколико $b \in U(A)$, онда је $\langle b\rangle = A$, а ако $c \in U(A)$, онда је $\langle a\rangle = \langle b\rangle$.

Обратно, претпоставимо да је $\langle a\rangle$ максималан у скупу свих главних идеала прстена A. Нека је $a = bc$ и претпоставимо да $c \notin U(A)$. То значи да је $a \in \langle b\rangle$, али да $b \notin \langle a\rangle$ (зашто?), тј. да је $\langle a\rangle$ прави подскуп идеала $\langle b\rangle$. Како је $\langle a\rangle$ максималан у скупу свих главних идеала, то мора бити $\langle b\rangle = A$, тј. постоји $c \in A$ тако да је $bc = 1$, те закључујемо да је b инвертибилан. □

Максималан идеал у сваком комутативном прстену са јединицом постоји. Заправо, важи следећа теорема, коју нећемо доказивати.

Теорема 14 Нека је I прави идеал у комутативном прстену са јединицом A. Тада постоји максималан идеал M за који је $I \subseteq M$.

Посебно је занимљив случај прстена у којима постоји тачно један максимални идеал.

Став 15 У комутативном прстену са јединицом A постоји тачно један максималан идеал ако и само ако је $A \setminus U(A)$ идеал.

Доказ. Претпоставимо да је прстену постоји тачно један максималан идеал M. Доказаћемо да је заправо $M = A \setminus U(A)$. Пре свега, ниједан елемент у M не може бити инвертибилан пошто је M прави идеал (идеал генерисан инвертибилним елементом једнак је целом прстену).

Дакле, $M \subseteq A \setminus U(A)$. Обратно, нека је $a \in A \setminus U(A)$. Како a није инвертибилан, то је идеал $\langle a \rangle$ прави идеал, па је по претходној теореми садржан у неком максималном идеалу. Но, како је M једини максималан идеал, то $a \in M$. Добили смо да је $A \setminus U(A) = M$, па је $A \setminus U(A)$ заиста идеал.

Обратно, нека у прстену A сви неинвертибилни елементи чине идеал M. Јасно је да тај идеал мора бити максималан. Наиме, ако је M прави подскуп идеала I у I постоји неки елемент који није у M. Тај елемент је нужно инвертибилан (пошто су у M сви неинвертибилни), те генерише цео прстен и следи да је и $I = A$. Дакле, M је максималан идеал. Претпоставимо да је M' неки други максималан идеал и нека је $M \neq M'$. Како је M' максималан то $M' \not\subseteq M$, па постоји елемент $x \in M' \setminus M$. Но, то значи да је x инвертибилан, па је $M' = A$ и M' није прави идеал, а то противречи претпоставци да је он максималан. Закључујемо да је M једини максималан идеал у A. □

Следећи пример је само специјалан случај важне конструкције, коју ћемо подробније анализирати када се будемо бавили пољима.

Пример 16 Показати да је $\mathbb{R}[X]/\langle X^2+1\rangle \cong \mathbb{C}$.

Користићемо теорему о изоморфизмима за прстене. Нека је $f\colon \mathbb{R}[X] \to \mathbb{C}$ дефинисана са: $f(p) = p(i)$ (i је наравно имагинарна јединица). Јасно је да је f хомоморфизам: $f(pq) = (pq)(i) = p(i)q(i)$, $f(p+q) = (p+q(i) = p(i)+q(i)$. Осим, тога, f је „на": $f(a+bX) = a+bi$ за $a, b \in \mathbb{R}$. Потребно је само да одредимо језгро хомоморфизма f. Јасно је да је $X^2+1 \in \mathrm{Ker}(f)$, пошто је $i^2 + 1 = 0$. Стога је $\langle X^2+1\rangle \subseteq \mathrm{Ker}(f)$. Претпоставимо да $p(X) \in \mathrm{Ker}(f)$. То значи да је $p(i) = 0$. Поделимо $p(X)$ полиномом X^2+1. Добијамо да је, за неке $a, b \in \mathbb{R}$

$$p(X) = q(X)(X^2+1) + a + bX.$$

Како је $p(i) = 0$, добијамо да је $0 = a+bi$. Како су a и b реални бројеви, то је могуће једино ако је $a = b = 0$, те закључујемо да $(X^2+1) \mid p(X)$. Стога је заиста $\mathrm{Ker}(f) = \langle X^2+1\rangle$. Теорема о изоморфизмима за прстене даје нам тражени резултат. ♣

На потпуно аналогни начин доказује се да је

$$\mathbb{Q}[X]/\langle X^2-2\rangle \cong \mathbb{Q}[\sqrt{2}],$$

при чему је $\mathbb{Q}[\sqrt{2}] := \{p(\sqrt{2}) : p \in \mathbb{Q}[X]\}$. Како је полином $X^2-2 \in \mathbb{Q}[X]$ нерастављив, добијамо да је заправо $\mathbb{Q}[\sqrt{2}]$ поље. О примерима овог типа биће више речи када будемо изучавали поља.