АЛГЕБРА 2

Комутативни прстени са јединицом
Факторизација. Локализација

Зоран Петровић

28. април 2012.

Подсетимо се да је област целих (домен) комутативан прстен са јединицом у коме нема правих делитеља нуле, тј. у којима важи: за све $a, b \in A$ из $ab = 0$ следи $a = 0$, или $b = 0$. Сви прстени којима ћемо се бавити у овој лекцији биће домени.

Дефиниција 1 Два елемента $a, b \in A$ су придружена уколико постоји $u \in U(A)$ такав да је $a = ub$.

Јасно је да је придруженост елемената једна релација еквиваленције. Приметимо да ако је p нерастављив онда је то и сваки њему придружен елемент. Исто то важи и за просте елементе у домену.

Дефиниција 2 Домен A је домен за једнозначном факторизацијом уколико за сваки елемент из $a \in A \setminus (U(A) \cup \{0\})$ постоје нерастављиви елементи $p_1, \ldots, p_r$ такви да је $a = p_1 p_2 \cdots p_r$. Осим тога ако је за нерастављиве елемента p_i, q_j:

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

онда је $r = s$ и постоји пермутација $\sigma \in \mathbb{S}_r$ тако да је за све $i = \overline{1, r}$ елемент p_i придружен елементу $q_{\sigma(i)}$.

Другим речима у домену са једнозначном факторизацијом, сваки елемент може се на јединствен начин, до на придруженост и редослед фактора, приказати у облику производа нерастављивих елемената.

Став 3 Домен A је домен са једнозначном факторизацијом акко се сваки елемент $a \in A \setminus (U(A) \cup \{0\})$ може приказати у облику производа простих елемената. Посебно, то значи да је сваки нерастављив елемент прост.

Доказ. Претпоставимо да се сваки неинвертибилан, ненула елемент може приказати у облику производа простих. Како су прости нерастављиви, потребно је само доказати да је приказ у облику производа јединствен (у горенаведеном смислу). Докажимо најпре да је, у овом случају, сваки нерастављив елемент прост.

Нека је q нерастављив елемент. По претпоставци, он се може написати у облику производа простих елемената: $q = p_1 \cdots p_r$, где су p_i прости. Но, како је q нерастављив, мора бити $r = 1$, тј. и сам q је прост.

Докажимо сада јединственост разлагања у облику производа нерастављивих елемената. Нека је

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

Доказ изводимо индукцијом по r. Случај $r = 1$ је тривијалан (зашто?). Претпоставимо да је у горњој једнакости $r > 1$ и да су су p_i, q_j нерастављиви. Према доказаном, p_1 је прост, па постоји $j_1 \in \{1, \ldots, s\}$ тако да $p_1 \mid q_{j_1}$. Како је q_{j_1} нерастављив, добијамо да су p_1 и q_{j_1} придружени, тј. да постоји $u_1 \in U(A)$ за који је $q_{j_1} = u_1 p_1$. Горњу једнакост можемо поделити са p_1 и добијамо

$$p_2 \cdots p_r = q_2' q_3 \cdots q_s,$$

где је $q_2' = q_2 u_1$ и он је такође нерастављив. Индуктивна хипотеза завршава доказ.

Обратно, претпоставимо да је A домен за једнозначном факторизацијом. Довољно је показати да је сваки нерастављив елемент прост. Нека је p нерастављив и нека $p \mid ab$. Треба показати да $p \mid a$, или $p \mid b$. Претпоставимо да p не дели ни a ни b. Нека је $a = p_1 \cdots p_r$ факторизација a на нерастављиве елементе и $b = q_1 \cdots q_s$ факторизација b на нерастављиве. Тада је

$$ab = p_1 \cdots p_r q_1 \cdots q_s$$

факторизација ab на нерастављиве. Како p дели ab, то је $ab = pc$ за неко c. И c има факторизацију на нерастављиве елементе, па је $c = z_1 \cdots z_l$ за неке нерастављиве $z_1, \ldots, z_l$. Добијамо да је

$$p_1 \cdots p_r q_1 \cdots q_s = p z_1 \cdots z_l,$$

где су сви p_i, q_j, z_k и p нерастављиви. Како је, по претпоставци, A домен са једнозначном факторизацијом, то је p придружен неком од елемената из скупа $\{p_1, \ldots, p_r, q_1, \ldots, q_s\}$. Уколико је p придружен елементу p_i (за неко i), добијамо да $p \mid a$, а ако је p придружен неком q_j онда $p \mid b$. Наиме, лако се показује да важи следеће: ако је p придружен елементу q и ако $q \mid c$, онда и $p \mid c$ (докажите то!). Овим је доказ завршен. □

Подсетимо се да је прстен главноидеалски уколико је сваки идеал у њему главни. Раније смо закључили да су $\mathbb{Z}$ и $K[X]$, за произвољно поље K, главноидеалски домени. Показаћемо да је сваки главноидеалски домен уједно и домен са једнозначном факторизацијом.

Став 4 Доказати да у сваком главноидеалском домену за свака два елемента постоји њихов највећи заједнички делилац.

Доказ. Нека A један главноидеалски домен и $a, b \in A$. Посматрајмо идеал $\langle a, b\rangle$ генерисан елементима a и b. Како је у A сваки идеал главни, то је и $\langle a, b\rangle = \langle d\rangle$, за неки $d \in A$. Докажимо да је d један највећи заједнички делилац елемената a и b (највећи заједнички делилац није једнозначно одређен, али су свака два највећа заједничка делиоца придружени један другом).

Најпре, $a, b \in \langle d\rangle$. То значи да постоје a_1, b_1 за које је $a = da_1$ и $b = db_1$, тј. $d \mid a$ и $d \mid b$, те d јесте заједнички делилац од a и b.

Претпоставимо да $d_1 \mid a$ и $d_1 \mid b$, тј. да је d_1 неки заједнички делилац од a и b. Треба доказати да $d_1 \mid d$. Како $d_1 \mid a$ и $d_1 \mid b$, то постоје a_1 и b_1 тако да је $a = d_1a_1$ и $b = d_1b_1$. С обзиром да $d \in \langle a, b\rangle$, постоје p, q такви да је $d = ap + bq$. Добијамо да је $d = d_1a_1p + d_1b_1q = d_1(a_1p + b_1q)$, те следи да $d_1 \mid d$. □

Заправо је у овом ставу доказано не само да свака два елемента a и b имају највећи заједнички делилац d, но и да постоје p и q за које је $d = ap + bq$ (Безуова релација). Из ове релације се, на стандардан начин, изводи следеће својство: ако $a \mid bc$ и ако је $\mathrm{NZD}(a, b)$ придружен јединици, онда $a \mid c$ (наравно, уместо да пишемо да је $\mathrm{NZD}(a, b)$ придружен јединици, писаћемо да је $\mathrm{NZD}(a, b) = 1$, имајући на уму шта то значи). Нека читаоци ово сами докажу.

Теорема 5 Сваки главноидеалски домен је и домен са јединственом факторизацијом.

Доказ. Нека је A главноидеалски домен. Докажимо најпре да је сваки нерастављив елемент у A прост. Нека је q нерастављив и нека $q \mid ab$. Уколико q не дели a, мора бити $\mathrm{NZD}(q, a) = 1$. Наиме, ако је $d = \mathrm{NZD}(q, a)$, то значи да је $q = dz$ за неко z. Како је q нерастављив, мора бити $d \in U(A)$, или $z \in U(A)$. Но, ако је $z \in U(A)$, онда из чињенице да $d \mid a$ следи да и $q \mid a$ (зашто?), што противречи претпоставци. Закључујемо да $d \in U(A)$, тј. $\mathrm{NZD}(q, a) = 1$ (погледајте ранију напомену у загради). Но, тада из горенаведеног својства следи да $q \mid b$, те закључујемо да је q прост.

Да бисмо доказали да је A домен са јединственом факторизацијом, остаје само да покажемо да се сваки елемент из $A \setminus (U(A) \cup \{0\})$ може приказати у облику производа нерастављивих елемената (видети став 3).

Докажимо најпре да сваки непразан скуп идеала у A има максималан елемент. Претпоставимо да то није тако и нека је $\mathcal{I}$ неки непразан скуп идеала који не садржи максималан елемент. Нека је $I_1 \in \mathcal{I}$ произвољан идеал из $\mathcal{I}$. Како он није максималан у $\mathcal{I}$, то постоји $I_2 \in \mathcal{I}$ за који је $I_1 \subset I_2$. Слично, постоји и $I_3 \in \mathcal{I}$ такав да је $I_2 \subset I_3$. Заправо добијамо стриктно растући ланац идеала

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

из $\mathcal{I}$. Унија $J = \cup_{i=1}^{\infty} I_i$ је идеал као што се лако може проверити (проверите!). Но, с обзиром да је A главноидеалски, то је $J = \langle x \rangle$ за неки $x \in A$. Како је $x \in \cup_{i=1}^{\infty} I_i$, то $x \in I_{i_0}$ за неки i_0. Но, одавде следи да је $J = I_{i_0}$, па је и $I_i = I_{i_0}$ за све $i \geq i_0$, те бесконачан стриктно растући ланац идеала и не постоји. Закључујемо да у $\mathcal{I}$ постоји максималан елемент.

Претпоставимо да у $A \setminus (U(A) \cup \{0\})$ има елемената који немају факторизацију на нерастављиве елементе. Уочимо скуп идеала $\mathcal{J}$ задат са:

$$\mathcal{J} = \{\langle a \rangle : a \in A \setminus (U(A) \cup \{0\}) \text{ и } a \text{ нема факторизацију на нерастављиве}\}.$$

Према управо доказаном резултату, у $\mathcal{J}$ постоји максималан елемент $\langle x \rangle$. Како x нема факторизацију на нерастављиве, то он сам није нерастављив, па постоје a, b такви да је $x = ab$, при чему $a, b \in A \setminus (U(A) \cup \{0\})$. Стога је $\langle x \rangle \subset \langle a \rangle$ и $\langle x \rangle \subset \langle b \rangle$ (зашто?), па a и b имају факторизацију на нерастављиве ($\langle x \rangle$ је максималан елемент у $\mathcal{J}$). Но, ако су то факторизације $a = p_1 \cdots p_r$ и $b = q_1 \cdots q_s$, онда је $x = ab = p_1 \cdots p_r q_1 \cdots q_s$ једна факторизација x на нерастављиве, што противречи избору елемента x. Ова контрадикција завршава доказ. □

Може се показати (али ми то нећемо) да из чињенице да је A домен са једнозначном факторизацијом следи да је и $A[X]$ домен са једнозначном факторизацијом. Дакле, $\mathbb{Z}[X]$ је један пример домена са једнозначном факторизацијом, који није главноидеалски домен.

Дакле, домен са једнозначном факторизацијом се карактерише тиме да се у њему прости и нерастављиви елементи подударају и да се сваки ненула, неинвертибилан елемент a може представити у облику

$$a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}, \tag{1}$$

где је u инвертибилан елемент и p_i нерастављиви, при чему за $i \neq j$ елементи p_i и p_j нису придружени, док је $\alpha_i \in \mathbb{N}$. Осим тога, ако је

$$a = vq_1^{\beta_1} \cdots q_l^{\beta_l},$$

где је v инвертибилан, q_j нерастављиви и q_i, q_j нису придружени за $i \neq j$, онда је $k = l$ и за неку пермутацију $\sigma \in \mathbb{S}_k$ $\alpha_i = \beta_{\sigma(i)}$ и p_i је придружен елементу $q_{\sigma(i)}$.

Напомена 6 Читалац се можда пита зашто се појављује инвертибилан елемент u у представљању елемента a у облику производа, када се тако нешто не појављује у самој дефиницији домена са једнозначном факторизацијом. Разлог лежи у томе што нерастављиви елементи p_i нису међусобно придружени и онда је неопходно издвојити инвертибилан елемент u. На пример, елемент $-36 \in \mathbb{Z}$ се може записати у облику $-36 = (-1)2^2 3^2$, или у облику $-36 = (-1)2^2(-3)^2$, али се (-1) мора појавити у овим записима. Презентација $-36 = 2(-2)3^2$ не задовољава услов да за различите индексе прости елементи нису придружени.

На основу једнакости (1), лако се показује да свака два елемента из домена са једнозначном факторизацијом имају највећи заједнички делилац (како се то показује?), но Безуова релација ипак не мора важити. Довољно је посматрати пример прстена $\mathbb{Z}[X]$ и елемената 2 и X, који јесу узајамно прости, али за које не постоје полиноми $p(X)$ и $q(X)$ тако да је $2p(X) + Xq(X) = 1$ (зашто?).

Пређимо сада на важан метод локализације којим се од датог домена прелази на нови домен, а у коме су неки изабрани елементи из почетног домена инвертибилни у новом домену. Почнимо следећом дефиницијом.

Дефиниција 7 Нека је A домен и $S \subseteq A \setminus \{0\}$. За S кажемо да је мултипликативан ако $1 \in S$ и ако из $s, t \in S$ следи да $st \in S$.

Пример 8 Следећи подскупови од $A \setminus \{0\}$ су мултипликативни:

1. $A \setminus \{0\}$;
2. $\{f^n : n \in \mathbb{N}\}$, за ма који елемент $f \in A \setminus \{0\}$;
3. $A \setminus P$ за ма који прост идеал $P \triangleleft A$.

1. Ово је јасно.

2. Подсетимо се да $0 \in \mathbb{N}$, па $1 \in S$. Осим тога, како је $f^m f^n = f^{m+n}$ и други услов је испуњен.

3. Јасно је да $1 \in A \setminus P$. Осим тога, ако $a \notin P$ и $b \notin P$, онда и $ab \notin P$, пошто је P прост идеал (појасните себи ово!). ♣

Нека је A домен и S ма који мултипликативан подскуп од A. На скупу $A \times S$ дефинишемо релацију $\sim$ са:

$$(a, s) \sim (b, t) \overset{\text{def}}{\iff} ta = sb.$$

Докажимо да је $\sim$ једна релација еквиваленције.

Рефлексивност. Ово је јасно пошто је $sa = sa$, па је $(a, s) \sim (a, s)$.

Симетричност. И ово је јасно, јер из $(a, s) \sim (b, t)$, следи да је $ta = sb$, тј, $sb = ta$, а то управо значи да је $(b, t) \sim (a, s)$.

Транзитивност. Нека је $(a, s) \sim (b, t)$ и $(b, t) \sim (c, r)$. То значи да је $ta = sb$ и $rb = tc$. Добијамо да је

$$rta = rsb = stc.$$

Како је A домен, то је $ra = sc$, па је $(a, s) \sim (c, r)$.

Са $S^{-1}A$ означавамо скуп свих класа еквиваленције, а са $\frac{a}{s}$ класу еквиваленције елемента (a, s). Дефинишемо операције $+$ и $\cdot$ на $S^{-1}A$ са:

$$\frac{a}{s} + \frac{b}{t} := \frac{ta + sb}{st};$$

$$\frac{a}{s}\cdot\frac{b}{t}:=\frac{ab}{st}.$$

Како је скуп S мултипликативан, то за $s,t\in S$ и $st\in S$, па ови записи имају смисла. Треба још да проверимо да су ове операције добро дефинисане.

Нека је $\frac{a}{s}=\frac{a'}{s'}$ и $\frac{b}{t}=\frac{b'}{t'}$. То заправо значи да је $(a,s)\sim(a',s')$ и $(b,t)\sim(b',t')$. Треба проверити да је $(ta+sb,st)\sim(t'a'+s'b',s't')$ и $(ab,st)\sim(a'b',s't')$. Рачунамо:

$$s't'(ta+sb)=s't'ta+s't'sb=t'tsa'+s'stb'=st(t'a'+s'b'),$$

па је заиста $(ta+sb,st)\sim(t'a'+s'b',s't')$. На сличан начин се проверава и добра дефинисаност операције множења.

Није тешко проверити да је структура $(S^{-1}A,+,\cdot)$ један комутативан прстен са јединицом (урадите то за вежбу: $0_{S^{-1}A}=\frac{0}{1}$, $1_{S^{-1}A}=\frac{1}{1}$). Овај прстен назива се локализација домена A у односу на мултипликативан скуп S. Основно својство локализације дато је следећим ставом.

Став 9 Нека је A домен и S неки мултипликативан подскуп од A.

а) Са $i(a)=\frac{a}{1}$ задат је један мономорфизам $i\colon A\to S^{-1}A$,

б) Ако је B ма који комутативан прстен и $f\colon A\to B$ хомоморфизам такав да за све $s\in S$ важи: $f(s)\in U(B)$, онда постоји тачно један хомоморфизам $\widetilde{f}\colon S^{-1}A\to B$ за који је $\widetilde{f}\circ i=f$.

Доказ.

а) Како је $i(a+b)=\frac{a+b}{1}=\frac{a}{1}+\frac{b}{1}=i(a)+i(b)$ и $i(ab)=\frac{ab}{1}=\frac{a}{1}\frac{b}{1}$, то је i заиста хомоморфизам. Но, $a\in\mathrm{Ker}(i)$ ако и само ако је $\frac{a}{1}=\frac{0}{1}$, што је еквивалентно са $a=0$, па је i мономорфизам.

б) Тражени хоморфизам $\widetilde{f}$ дефинишемо са: $\widetilde{f}(\frac{a}{s})=f(a)f(s)^{-1}$. Како је, за све $s\in S$, $f(s)$ инвертибилан, ова дефиниција има смисла. Остављамо читаоцима да провере да је ово заиста један добро дефинисан хомоморфизам и да важи: $\widetilde{f}\circ i=f$. □

Уколико је $S=A\backslash P$ за неки прост идеал P, онда се уместо $(A\backslash P)^{-1}A$ краће пише: A_P. Важи следећа теорема.

Теорема 10 За сваки прост идеал $P\lhd A$, прстен A_P је локални прстен.

Доказ. Доказаћемо да је скуп свих неинвертибилних елемената идеал. Одредимо најпре $U(A_P)$:

$$\frac{a}{s}\in U(A_P)\text{ акко постоје }b\in A\text{ и }t\in A\setminus P\text{ тако да је }\frac{a}{s}\cdot\frac{b}{t}=\frac{1}{1}.$$

Другим речима, $\frac{a}{s}$ је инвертибилан акко постоји $b\in A$ и $t\notin P$ за које је $ab=st$. Уколико $a\in P$, онда и $st=ab\in P$, па како је P прост идеал,

следи да $s \in P$, или $t \in P$, што није могуће на основу избора s и t. А уколико $a \notin P$, онда је $\frac{s}{a} (\in A_P)$ инверз елемента $\frac{a}{s}$. Дакле,

$$A_P \setminus U(A_P) = \left\{ \frac{a}{s} \in A_P : a \in p \right\}.$$

Уверимо се да је ово заиста идеал у A_P.

Нека су x, y неинвертибилни елементи из A_P. То значи да постоје елементи $a, b \in p$ и $s, t \notin P$ за које је $x = \frac{a}{s}$ и $y = \frac{b}{t}$. Тада је $x + y = \frac{a}{s} + \frac{b}{t} = \frac{ta+sb}{st}$, но, како је P идеал, $ta + sb \in P$, па је заиста и елемент $x + y$ неинвертибилан. На сличан начин се показује да ако $x \in A_P$ нема инверз и ако је $z \in A_P$ произвољан, ни елемент zx нема инверз. Закључујемо да је $A_P \setminus U(A_P)$ заиста идеал, па је и прстен A_P локални прстен. □

За крај напоменимо да, уколико је $S = A \setminus \{0\}$, у прстену $S^{-1}A$ је сваки елемент различит од нуле инвертибилан, те је, у овом случају, $S^{-1}A$ једно поље. Ово поље се назива поље разломака домена A и означава са $Q(A)$. На овај начин смо показали да се сваки домен може утопити у неко поље. Као што видимо, ова је конструкција у потпуности аналогна конструкцији рационалних бројева као разломака над целим бројевима.