

АЛГЕБРА

Комутативни прстени са јединицом

Зоран Петровић

16. мај 2011.

У овој лекцији прелазимо на изучавање алгебарских структура са две бинарне операције, које обично зовемо сабирање и множење. Пређимо на дефиницију основног објекта, који ћемо овде проучавати.

Дефиниција 1 Комутативан прстен са јединицом је структура $(A, +, \cdot)$ за коју важи

- $(A, +)$ је Абелова група;
- (A, \cdot) је комутативан моноид;
- За све $x, y, z \in A$ важи: $x \cdot (y + z) = x \cdot y + x \cdot z$.

Неутрал за сабирање (операцију $+$ у прстену) у комутативном прстену A означавамо са 0 (или понекад, због прецизности, са 0_A) и зовемо нуллом прстена A , док неутрал за множење (операцију \cdot у прстену) означавамо са 1 (или понекад, због прецизности, са 1_A) и зовемо јединицом прстена A .

У сваком прстену A , за сваки елемент $a \in A$, важи: $a \cdot 0 = 0$. Ево како то можемо показати:

$$a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0.$$

Коришћењем чињенице да је $(A, +)$ Абелова група, добијамо да је

$$0 = a \cdot 0.$$

Уколико би у прстену A важило: $0_A = 1_A$ (приметимо да нигде нисмо захтевали да је нула прстена различита од његове јединице), добили бисмо да за свако $a \in A$ важи:

$$a = a \cdot 1_A = a \cdot 0_A = 0_A,$$

па би било $A = \{0_A\}$. Такав прстен називамо нула прстен. У даљем ћемо увек претпоставити да је $0_A \neq 1_A$.

Приметимо још да је у сваком прстену испуњено: $-a = (-1) \cdot a$. Наиме,

$$a + (-1) \cdot a = 1 \cdot a + (-1) \cdot a = a \cdot 1 + a \cdot (-1) = a \cdot (1 + (-1)) = a \cdot 0 = 0,$$

те следи да је заиста $(-1) \cdot a = -a$. На сличан начин се доказују и други идентитети попут нпр. $(-a) \cdot b = -(a \cdot b)$, $(-a) \cdot (-b) = a \cdot b$ итд.

Структура (A, \cdot) је моноид, па у њој неки елементи могу имати инверз. Јасно је да то не може бити 0, пошто је $0 \cdot a = 0 \neq 1$ за сваки елемент $a \in A$. Стога је природно посматрати све оне елементе из $A \setminus \{0\}$ који имају инверз у односу на множење. Скуп свих таквих елемената означаваћемо са $U(A)$. Јасно је да је $(U(A), \cdot)$ једна комутативна група и зваћемо је групом инвертибилних елемената прстена. Дакле, када кажемо да је неки елемент прстена инвертибилан, мислимо на инвертибилност у односу на операцију множења, пошто у односу на сабирање сваки елемент сигурно има свој супротни елемент. Уколико је $U(A) = A \setminus \{0\}$, прстен A је поље.

Наведимо неке примере комутативних прстена са јединицом:

- \mathbb{Z} ;
- $\mathbb{Z}_n = (Z_n, +_n, \cdot_n)$;
- \mathbb{R} ;
- \mathbb{Q} ;
- \mathbb{C} .

Наравно да $+_n$ и \cdot_n означавају операције сабирања и множења по модулу n . Приметимо да су последња три прстена заправо поља, док први то сигурно није, а други за неке n јесте, а за неке n није. Заправо важи следеће.

$$U(\mathbb{Z}_n) = \Phi(n) \text{ (погледајте предавања бр. 2).}$$

Дакле,

\mathbb{Z}_n је поље ако и само ако је n прост број.

Важан пример прстена чини и прстен полинома са коефицијентима у неком комутативном прстену са јединицом A и неодређеном X , тј. прстен $A[X]$. Ми се нећемо детаљно бавити конструкцијом наведеног прстена, прихватићемо га као скуп свих формалних израза облика $a_0 + a_1X + \dots + a_nX^n$, при чему $a_i \in A$, за све i , а сабирање и множење се изводи као што изводимо сабирање и множење полинома са којима смо радили у средњој школи. Дакле,

$$A[X] = \{a_0 + a_1X + \dots + a_nX^n : n \in \mathbb{N}, a_i \in A\}.$$

Но, за разлику од полинома из средње школе, нека правила престају да важе. На пример, подсетимо се појма степена полинома. Уколико је $p = a_0 + a_1X + \dots + a_nX^n$, при чему је $a_n \neq 0$, онда је степен полинома p баш n . Тај полином p је моничан уколико је ту $a_n = 1$. У средњој школи смо навикли да је степен производа два полинома једнак збиру њихових степена:

$$\deg(ab) = \deg a + \deg b,$$

где је са $\deg a$ означен степен полинома a . Но, посматрајмо пример два полинома из $\mathbb{Z}_6[X]$. Нека је $a = 2 + 3X$, а $b = 1 + 2X$. Тада је

$$a \cdot b = (2 + 3X) \cdot (1 + 2X) = 2 + X.$$

Приметимо да су операције у прстену \mathbb{Z}_6 сабирање и множење по модулу 6, те како је $2 \cdot_6 3 = 0$ и сл. добијамо наведени резултат. Феномен, који се овде појавио састоји се у томе да производ два ненулта елемента ипак може бити једнак 0.

Дефиниција 2 За елемент $a \neq 0$, комутативног прстена са јединицом A , кажемо да је прави делитељ нуле у A уколико постоји $b \in A \setminus \{0\}$ такав да је $a \cdot b = 0$.

Став 3 У пољу нема правих делитеља нуле.

Доказ. Претпоставимо да у пољу F постоје прави делитељи нуле, тј. да постоје a и b такви да је $a \neq 0$ и $b \neq 0$, а да је $a \cdot b = 0$. Како је $a \neq 0$, а у пољу сваки елемент различит од нуле има инверз, постоји елемент a^{-1} за који важи $a^{-1} \cdot a = 1$. Тако добијамо да је

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1 \cdot b = b,$$

што противречи претпоставци $b \neq 0$. □

Дефиниција 4 Комутативан прстен са јединицом у коме нема правих делитеља нуле зове се област целих или домен.

Дакле, на основу претходног става, свако поље је домен, но има и домена који нису поља. На пример, \mathbb{Z} је домен који није поље. Занимљив је следећи резултат.

Став 5 Сваки коначан домен је поље.

Доказ. Претпоставимо да је A коначан домен и да је $a \in A \setminus \{0\}$. Треба показати да a има инверз. У ту сврху, посматрајмо функцију $L_a: A \rightarrow A$ дефинисану са $L_a(x) = a \cdot x$, за $x \in A$. Ова функција је „1–1“. Наиме, ако је $L_a(x) = L_a(y)$, онда је $a \cdot x = a \cdot y$, па је $a \cdot (x - y) = 0$. Како је A домен, а $a \in A \setminus \{0\}$, мора бити $x - y = 0$, тј. $x = y$. Но, свака „1–1“ функција која слика коначан скуп у њега самог мора бити бијекција. Закључујемо да је L_a бијекција, па постоји a' тако да је $L_a(a') = 1$, тј. постоји $a' \in A$ за који је $a \cdot a' = 1$, те a има инверз. □

Дефиниција 6 Елемент $a \in A$ је регуларан уколико из $a \cdot x = a \cdot y$ следи да је $x = y$.

Дакле, регуларни елементи су они елементи „са којима можемо скратити“ неке једнакости. Приметимо да су инвертибилни елементи сигурно регуларни, али да регуларни елементи не морају бити инвертибилни. Наиме, јасно је да у \mathbb{Z} сваки елемент различит од нуле регуларан, а да само 1 и -1 имају инверз у \mathbb{Z} . Но, Став 5 није тешко уопштити.

Став 7 У сваком коначном прстену сваки регуларан елемент је инвертибилан.

Упутство: Погледајте доказ Става 5. □

Дакле, сваки елемент у коначном прстену је или делитељ нуле или инвертибилан. Уколико скуп свих делитеља нуле у прстену A означимо са $Z(A)$, овај резултат можемо кратко записати и на следећи начин. Ако је A коначан комутативан прстен са јединицом онда је

$$A = Z(A) \sqcup U(A).$$

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

Дефиниција 8 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 9 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 $I \triangleleft A$ означава да је I идеал у A .

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

Дефиниција 10 Нека су I и J идеали прстена A .

1. $I + J := \{x + y : x \in I, y \in J\}$;
2. $I \cdot J := \{x_1 y_1 + \dots + x_n y_n : x_i \in I \text{ за све } i = \overline{1, n}, y_j \in J \text{ за све } j = \overline{1, n}, \text{ и све } n \geq 1\}$.

Директна провера показује да су $I + J$ и $I \cdot J$ заиста идеали у прстену A . Приметимо да 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 11 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 зове 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 12 Сваки идеал у \mathbb{Z} је облика $\langle m \rangle$ за неки природан број m .

Нека је $I \triangleleft \mathbb{Z}$. 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 13 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 $d = \text{NZD}(m, n)$. 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 $\langle m \rangle \cap \langle n \rangle = \langle \text{NZS}(m, n) \rangle$. ♣

Пример 14 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 $S = \{x_1, \dots, x_n\}$ пишемо $\langle x_1, \dots, x_n \rangle$, уместо $\langle \{x_1, \dots, x_n\} \rangle$). 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 15 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 ћемо само такве случајеве и разматрати).

Нека је $I \triangleleft K[X]$. 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 са 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 16 Нека је K поље и $I \triangleleft K$. 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 17 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 18 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ два комутативна прстена са јединицом. Функција $f: A \rightarrow B$ 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 19 Функција $\rho_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$ 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 20 Нека је $f: A \rightarrow B$ хомоморфизам комутативних прстена са јединицом. Језгро хомоморфизма f , у ознаци $\text{Ker}(f)$ дефинише се са:

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

Став 21 Нека је $f: A \rightarrow B$ хомоморфизам комутативних прстена са јединицом. Тада важи:

-
- а) $\text{Ker}(f) \triangleleft A$;
 б) ако је $J \triangleleft B$ онда је $f^{-1}[J] \triangleleft A$;
 в) ако је $I \triangleleft A$ и f „на“, онда је $f[I] \triangleleft B$.

Доказ.

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

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

па $x + y \in \text{Ker}(f)$.

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

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

те $a \cdot x \in \text{Ker}(f)$.

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 $f[I]$. \square

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

У општем случају директна слика идеала не мора бити идеал. На пример, јасно је да функција $i: \mathbb{Z} \rightarrow \mathbb{Q}$ 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 22 Нека је $n \geq 2$ цео број. Тада је сваки идеал у \mathbb{Z}_n главни.

Искористићемо хомоморфизам $\rho_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$, који је и „на“. Нека је $J \triangleleft \mathbb{Z}_n$. Тада је $\rho_n^{-1}[J] \triangleleft \mathbb{Z}$. 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 23 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 24 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 $m \in \mathbb{Z}_{12}$ 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 генерализовати). 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 $m \in \mathbb{Z}_{12}$ такав да је $2 = 4 \cdot_{12} m$. То би значило да постоји цео број q такав да је $2 = 4m + 12q$. Делењем 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:

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