АЛГЕБРА

Комутативни прстени са јединицом

Зоран Петровић

Девето предавање

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 нулом 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.

Сви прстени, са којима у даљем будемо радили, биће комутативни прстени са јединицом и кратко ћемо их звати прстени. У сваком прстену A, за сваки елемент $a \in A$, важи: $a \cdot 0_A = 0_A$. Ево како то можемо показати:

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

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

$$0_A = a \cdot 0_A.$$

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: $-a = (-1_A) \cdot a$. Наиме,

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

те следи да је заиста $(-1_A) \cdot a = -a$. На сличан начин се доказују и други идентитети попут, на пример, $(-a) \cdot b = -(a \cdot b)$, $(-a) \cdot (-b) = a \cdot b$ 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 <u>поље</u>.

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.

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

Дакле,

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

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 $a_0 + a_1X + \cdots + a_nX^n$, 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,

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

Но, за разлику од полинома из средње школе, нека правила престају да важе. На пример, подсетимо се појма степена полинома. Уколико је $p = a_0 + a_1 X + \cdots + a_n X^n$, 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 зовемо 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 $L_a \colon A \to A$ 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 обавезно и 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 $I \lhd A$ 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. $I \cdot J := \{x_1y_1 + \cdots + x_ny_n : x_i \in I$ 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. 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 назива се 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 $I \lhd \mathbb{Z}$. 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 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 $d = \mathrm{NZD}(m, n)$. 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 $mx + ny \in \langle d\rangle$, те је заиста $\langle m\rangle + \langle n\rangle = \langle d\rangle$.

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 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 $S = \{x_1, \ldots, x_n\}$ 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 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 у применама 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 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 $f\colon A \to B$ 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 19 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 20 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 21 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. Закључујемо да $a \cdot x \in f^{-1}[J]$.

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, $\mathrm{Ker}(f) = \{0_A\}$ ако и само ако је хомоморфизам f 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 22 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 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 $m \in Z_{12}$ 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:

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

У даљем ћемо претпоставити да су сви идеали са којима радимо прави, тј. да нису једнаки целом прстену.

Дефиниција 25 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 $b - a = (-1)(a - b)$ припада I, па је $b \equiv a \pmod{I}$.

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

$$a - c = (a - b) + (b - c) \in I,$$

те је $a \equiv c \pmod{I}$.

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 26 *(*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 27 Нека је $I \lhd A$. Тада је $p\colon A \to A/I$ један епиморфизам. ♣

Пример 28 За све $n \geq 1$ важи: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Хомоморфизам $\rho_n\colon \mathbb{Z} \to \mathbb{Z}_n$, 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 29 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 $0_A = (0_{A_1}, \ldots, 0_{A_n})$ и $1_A = (1_{A_1}, \ldots, 1_{A_n})$.

Став 30 Нека су $m_1, \ldots, m_n$ позитивни цели бројеви за које је: $\mathrm{NZD}(m_i, m_j) = 1$ 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

$$f\colon \mathbb{Z} \to (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$$

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 31 *(*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. □

Став 32 Ако су прстени A и B изоморфни, онда је $(U(A), \cdot) \cong (U(B), \cdot)$

Доказ. Јасно је да се инвертибилни елементи при сваком хомоморфизму сликају у инвертибилне елементе. Наиме, ако је $a \in U(A)$, то значи да постоји a' такав да је $a \cdot a' = 1_A$. Но, тада је $f(a) \cdot f(a') = f(a \cdot a') = f(1_A) = 1_B$, па и $f(a)$ има инверз.

Према томе, $f[U(A)] \subseteq U(B)$ за сваки хомоморфизам $f\colon A \to B$. Уколико је f изоморфизам и $b \in U(B)$, то постоји $a \in A$ такав да је $f(a) = b$. Но, елемент b има инверз, па је $b \cdot b' = 1_B$ за неки $b' \in B$. Елемент b' је слика неког елемента a': $f(a') = b'$. Но, тада је $f(a \cdot a') = f(a) \cdot f(a') = b \cdot b' = 1_B$, те како је f „1–1", мора бити $a \cdot a' = 1_A$ те a има инверз. Закључујемо да f успоставља бијекцију између $U(A)$ и $U(B)$. Како је f хомоморфизам, добијамо тражени изоморфизам. □

Став 33 Важи једнакост: $U(A_1 \times \cdots \times A_n) = U(A_1) \times \cdots \times U(A_n)$.

Доказ. Нека је $a = (a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$. Тада

$$\begin{aligned}
a \in U(A_1 \times \cdots \times A_n) &\iff \text{постоји } b \in A : a \cdot b = 1 \\
&\iff \text{постоје } b_i \in A_i \text{ т. д. } a_i \cdot b_i = 1 \text{ за све } i \\
&\iff a_1 \in U(A_1), \ldots, a_n \in U(A_n) \\
&\iff a \in U(A_1) \times \cdots \times U(A_n).
\end{aligned}$$

□

Теорема 34 Ако су $m_1, \ldots, m_n$ пар по пар узајамно прости позитивни цели бројеви, онда је

$$\mathbb{Z}_{m_1 \cdots m_n} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$$

и

$$\varphi(m_1 \cdots m_n) = \varphi(m_1) \cdots \varphi(m_n),$$

где је φ Ојлерова функција.

Доказ. Како је $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$, то први резултат следи из става 6. Осим тога, $\varphi(m) = |U(\mathbb{Z}_m)|$, те резултат за Ојлерову функцију следи из става 8 и става 9. □

Групе $U(\mathbb{Z}_n)$ имају занимљиву структуру, но ми се њима нећемо детаљно бавити. Но, ипак ћемо, због примена, доказати да је за сваки прост број p група $U(\mathbb{Z}_p)$ циклична. Заправо, доказаћемо општији резултат, али пре тога морамо да докажемо нешто у вези Абелових група.

Став 35 Нека је A Абелова група реда m и нека за свако d, које дели m, постоји највише d елемената $a \in A$ за које је $da = 0$. Тада је група A циклична.

Доказ. Докажимо најпре следећи резултат, који је и сам по себи занимљив:

$$\sum_{d|m} \varphi(d) = m.$$

Посматрајмо цикличну групу G реда m. Као што знамо, она има тачно једну подгрупу реда d за сваки d који је делилац броја m. Осим тога, циклична група реда d има тачно $\varphi(d)$ генератора. Следи да у цикличној групи реда m има тачно $\varphi(d)$ елемената реда d (сваки елемент реда d генеришу исту подгрупу групе G) за свако d које дели m. Стога једнакост следи.

Вратимо се нашој групи A. Означимо са $\psi_A(d)$ број елемената реда d у A. Сваки елемент $x \in A$ је неког реда d, где $d \mid m$. То значи да је

$$\sum_{d|m} \psi_A(d) = m.$$

С друге стране, ако је $\psi_A(d) > 0$, онда у групи A постоји елемент a, који је реда d. Посматрајмо подгрупу A' генерисану тим елементом. У њој има d елемената и за свако $z \in A'$ важи $dz = 0$. То значи да су сви елементи $x \in A$ за које је $dx = 0$ садржани у подгрупи A'. Дакле, сваки елемент реда d у A је садржан у цикличној подгрупи A', која је реда d. Но, ми знамо да у цикличној групи реда d има тачно $\varphi(d)$ генератора, тј. елемената реда d. Закључујемо да важи следеће: ако је за неко d, које дели m, $\psi_A(d) > 0$, онда је за то d: $\psi_A(d) = \varphi(d)$. С обзиром да је

$$\sum_{d|m} \varphi(d) = m = \sum_{d|m} \psi_A(d),$$

закључујемо да је за све d, који деле m испуњено $\psi_A(d) = \varphi(d)$. То посебно значи да је и $\psi_A(m) = \varphi(m) > 0$, па у A има елемената реда m, те је група A заиста циклична. □

Теорема 36 Нека је F поље и G коначна подгрупа групе $(F \setminus \{0\}, \cdot)$. Тада је G циклична група.

Доказ. Покажимо најпре да сваки полином $p(X)$ из $F[X]$ степена n има највише n нула у пољу F. Доказ се изводи индукцијом по степену полинома $p(X)$.

За $n = 1$ нема шта да се доказује, јасно је да полином има тачно једну нулу у F.

Претпоставимо да је $n > 1$ и да је тврђење тачно за све полиноме степена мањег од n. Ако полином $p(X)$ нема ниједну нулу у пољу F, онда је тврђење испуњено. Претпоставимо да $p(X)$ има неку нулу $a \in F$. Еуклидско дељење полинома $p(X)$ полиномом $X - a$ даје:

$$p(X) = (X - a)q(X) + r,$$

где је $r = 0$, или је то константан не-нула полином. Но, с обзиром да је $p(a) = 0$, добијамо да је $r = 0$. Стога је $p(X) = (X - a)q(X)$. Полином $q(X)$ је степена $n-1$ и по индукцијској хипотези има највише $n-1$ нулу у F. Како је свака нула полинома $p(X)$ или једнака a или је нека нула полинома $q(X)$ закључујемо да $p(X)$ има највише n нула у F.

Пређимо сада на доказ наше теореме. Теорему ћемо доказати тако што ћемо се уверити да група G испуњава услове претходног става (јасно је да је G комутативна група). С обзиром да овде користимо мултипликативну нотацију, треба да покажемо да за сваки d који дели ред групе G, у групи G има највише d елемената a за које је $a^d = 1$. Но, $G \subset F$ и елемент $a \in G$ за који је $a^d = 1$ у G(тј. у F) је заправо нула полинома $X^d - 1$ из $F[X]$. Ово је полином степена d и према претходно доказаном, он има највише d нула у F. Закључујемо да су услови за примену претходног става испуњени те добијамо да је G циклична група. □

Дакле, доказали смо да је свака коначна подгрупа мултипликативне групе поља циклична. Истакнимо још једном да се ради о коначним подгрупама. Наравно да мултипликативна група произвољног поља F, тј. група $(F \setminus \{0\}, \cdot)$ не мора бити циклична! Нпр. $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ сигурно нису цикличне (ти скупови су непребројиви!).

Погледајмо како можемо искористити чињеницу да је $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ циклична група. Пре свега, уведимо терминологију.

Дефиниција 37 Ма који генератор групе $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ зове се примитивни корен модуло p.

Став 38 Нека је r ма који примитивни корен модуло p. Тада је са:

$$\mathrm{ind}_r(a) = x \textbf{ акко } r^x = a,$$

дефинисан изоморфизам $\mathrm{ind}_r \colon (\mathbb{Z}_p \setminus \{0\}, \cdot_p) \to (\mathbb{Z}_{p-1}, +_{p-1})$.

Доказ. Овај став је заправо само преформулација и прецизирање тврђења да је група $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ циклична.

Како је r примитивни корен модуло p, то за свако $a \in \mathbb{Z}_p \setminus \{0\}$ постоји тачно једно $x \in \mathbb{Z}_{p-1}$ за које је $r^x = a$. Наиме, r је генератор наведене групе, па је сваки елемент у тој групи неки степен од r. Како та група има $p-1$ елемената, то $x \in \mathbb{Z}_{p-1}$. Ми треба да проверимо да ли је ind_r хомоморфизам, тј. да ли је

$$\mathrm{ind}_r(a \cdot_p b) = \mathrm{ind}_r(a) +_{p-1} \mathrm{ind}_r(b),$$

за све $a, b \in \mathbb{Z}_p \setminus \{0\}$. Нека је $x = \mathrm{ind}_r(a)$ и $y = \mathrm{ind}_r(b)$. Дакле, $r^x = a$ и $r^y = b$. Тада је

$$a \cdot_p b = r^x \cdot_p r^y = r^{x+y}.$$

С обзиром на чињеницу да је $\omega(r) = p-1$, то је

$$r^{x+y} = r^{x+_{p-1}y},$$

па добијамо да је

$$a \cdot_p b = r^{x+_{p-1}y},$$

те је

$$\mathrm{ind}_r(a \cdot_p b) = x +_{p-1} y = \mathrm{ind}_r(a) +_{p-1} \mathrm{ind}_r(b).$$

Дакле, ind_r је заиста хомоморфизам, а да је бијекција следи из чињенице да је $\omega(r) = p-1$. □

Пример 39 Наћи све примитивне корене модуло 13.

За почетак потражимо бар један примитивни корен. Почнимо од 2:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 3, \quad 2^5 = 6, \quad 2^6 = 12, \quad 2^7 = 11, \quad 2^8 = 9$$

$$2^9 = 5, \quad 2^{10} = 10, \quad 2^{11} = 7,$$

док је, наравно, $2^0 = 1$. Дакле, заиста је $\langle 2 \rangle = \mathbb{Z}_{13} \setminus \{0\}$. Да бисмо нашли све примитивне корене модуло 13, направимо таблицу за ind_2.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2(a)$	0	1	4	2	9	5	11	3	8	10	7	6

С обзиром да је $2^{\mathrm{ind}_2(a)} = a$, није тешко извршити проверу.

Ова таблица нам омогућава да нађемо и све остале примитивне корене модуло 13. Наиме, подсетимо се да важи следеће:

Ако је $\omega(r) = n$ онда је $\omega(r^m) = n$ ако и само ако је $\mathrm{NZD}(n, m) = 1$.

Пошто је у нашем случају $\omega(2) = 12$, то је $\omega(2^m) = 12$ ако и само ако је $\mathrm{NZD}(m, 12) = 1$, тј. ако и само ако је $m \in \{1, 5, 7, 11\}$. Дакле, остали примитивни корени по модулу 13 су: $6 (= 2^5)$, $11 (= 2^7)$ и $7 (= 2^{11})$. ♣

Пример 40 Решити конгруенцију

$$x^5 \equiv 7 \pmod{13}.$$

Већ знамо да је 2 примитивни корен по модулу 13. Применом ind_2 на дату конгруенцију добијамо да је

$$5y \equiv 11 \pmod{12},$$

где смо са y означили $\mathrm{ind}_2(x) \in \mathbb{Z}_{12}$. Тако смо применом ind_2 једну конгруенцију петог степена свели на линеарну, која се лако може решити. С обзиром да је $5 \cdot_{12} 5 = 1$, добијамо да је

$$y \equiv 7 \pmod{12}.$$

Дакле, како је $y = \mathrm{ind}_2(x)$, добијамо да је

$$x \equiv 11 \pmod{13}.$$

♣