

Глава 3

Комутативни прстени са јединицом

3.1 Дефиниција и основна својства

У овом делу 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 3.1 Алгебарска структура $(A, +, \cdot)$ је КОМУТАТИВАН ПРСТЕН СА ЈЕДИНИЦОМ ако и само ако важи:

1. $(A, +)$ је Абелова група;
2. операција \cdot је асоцијативна и комутативна на A ;
3. операција \cdot има неутрал;
4. за све $x, y, z \in A$ важи: $x \cdot (y + z) = x \cdot y + x \cdot z$.

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

Сви прстени¹, 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

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

¹Алгебарска структура $(A, +, \cdot)$ је прстен ако је операција \cdot асоцијативна на A , важе услове 1 и 4 из дефиниције 3.1, као и $(x+y) \cdot z = x \cdot z + y \cdot z$ за све $x, y, z \in A$. Тако $(M_n(\mathbb{R}), +, \cdot)$, где је $M_n(\mathbb{R})$ скуп квадратних матрица реда n над \mathbb{R} , јесте прстен, али није комутативан прстен са јединицом.

Уколико би у прстену A важило: $0_A = 1_A$ (приметимо да никада 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,

$$\begin{aligned} a + (-1_A) \cdot a &= 1_A \cdot a + (-1_A) \cdot a = a \cdot 1_A + a \cdot (-1_A) \\ &= a \cdot (1_A + (-1_A)) = a \cdot 0_A = 0_A, \end{aligned}$$

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

3.2 Инвертибилни елементи; делитељи нуле

У структури (A, \cdot) 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.

Дефиниција 3.2 Нека је A комутативан прстен са јединицом. Са $U(A)$, означавамо скуп свих инвертибилних елемената у прстену у односу на операцију множења, тј.

$$U(A) := \{a \in A : (\exists b \in A) a \cdot b = 1_A\}.$$

Докажимо да је $(U(A), \cdot)$ једна комутативна група (зваћемо је групом инвертибилних елемената прстена). Нека су $a_1, a_2 \in U(A)$. Тада постоје $b_1, b_2 \in A$ такви да је $a_1 \cdot b_1 = 1_A$ и $a_2 \cdot b_2 = 1_A$, па је

$$a_1 \cdot a_2 \cdot b_2 \cdot b_1 = a_1 \cdot 1_A \cdot b_1 = a_1 \cdot b_1 = 1_A,$$

и самим тим $a_1 \cdot a_2 \in U(A)$. Такође, $1_A \in U(A)$, а инверз елемента $a \in U(A)$ је баш елемент b такав да је $a \cdot b = b \cdot a = 1_A$ (јасно, важи $b \in U(A)$). Овим је доказ завршен. 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. Прстени у којима су сви елементи се 0 инвертибилни, су посебно значајни.

Дефиниција 3.3 ПОЉЕ је сваки комутативан прстен са јединицом A у коме је $U(A) = A \setminus \{0\}$.

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:

$$U(\mathbb{Z}_n) = \Phi(n) \quad (\text{погледајте поглавље 1.10}).$$

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 $A[X]$. У овом поглављу се нећемо детаљно бавити конструкцијом наведеног прстена, прихватићемо га као скуп свих формалних израза облика $a_0 + a_1X + \dots + a_nX^n$, при чemu $a_i \in A$, за све i , а сабирање и множење се изводи као што изводимо сабирање и множење полинома са којима смо радили у средњој школи (за детаљан опис ове конструкције можете погледати додатак I). 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 чemu је $a_n \neq 0$, онда је СТЕПЕН полинома p баш n . Тада полином p је МОНИЧАН уколико је ту $a_n = 1$. У средњој школи смо навикили 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 $\mathbb{Z}_6[X]$. Иска 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 $2 \cdot_6 3 = 0$, $2 \cdot_6 2 + 1 \cdot_6 3 = 1$ добијамо наведени резултат. Фсномен, који се овде појавио састоји се у томе да производ два ненула елемената ипак може бити једнак 0.

Дефиниција 3.4 За елемент $a \neq 0$, комутативног прстена са јединицом A , кажемо да је ПРАВИ делитељ нуле у A уколико постоји елемент $b \in A \setminus \{0\}$ такав да је $a \cdot b = 0$.

Став 3.5 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 $b \neq 0$. \square

Дефиниција 3.6 Комулативан 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 3.7 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 $a \cdot a' = 1$, тј. a има инверз. \square

Дефиниција 3.8 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” искс једнакости. Примстимо да су инвертибилни елементи обавезно и регуларни. Заиста, ако је $a \in A$ инвертибилан, тада множењем релације $a \cdot x = a \cdot y$ слева са a^{-1} добијамо $x = y$. Међутим, 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 3.7 није тешко уопштити (коришћењем сличног доказа).

Став 3.9 У сваком коначном прстену сваки регуларан елемент је уједно и инвертибилан. \square

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

$$A = Z(A) \sqcup U(A). \quad (3.1)$$

3.3 Потпрстни и идеали

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

Дефиниција 3.10 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 прсосталих (јер је $(B, +')$ подгрупа групе $(A, +)$), што није тачно за једнакост $1_A = 1_B$. На пример, иако је $A = \{(0,0), (0,1), (1,0), (1,1)\}$ и $B = \{(0,0), (1,0)\}$, где су опрације 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 склопници $(1,0)$, а јединица у A је $(1,1)$. Стога B није потпрстен са јединицом прстена A .

Важнији од појма потпрстена је појам ИДЕАЛА.

Дефиниција 3.11 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 склопницима.

Дефиниција 3.12 Нека су I и J идеали комутативног прстена са јединицом A . Дефинишемо:

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

Став 3.13 Нека су I и J идеали комутативног прстена са јединицом A . Тада су $I \cap J$, $I + J$ и $I \cdot J$ идеали прстена A .

Доказ. Докажимо прво да је $I \cap J$ идеал прстена A . Иска су $x, y \in I \cap J$. Тада је $x, y \in I$ и $x, y \in J$, па како су I и J идеали следи $x + y \in I$ и $x + y \in J$, тј. $x + y \in I \cap J$. Даље, за $a \in A$ важи $a \cdot x \in I$ и $a \cdot x \in J$, тј. $a \cdot x \in I \cap J$, па је заиста $I \cap J$ идеал прстена A .

Докажимо да је $I + J$ идеал прстена A . Иска су $x, y \in I + J$. Тада је $x = i_1 + j_1$ и $y = i_2 + j_2$ за неке $i_1, i_2 \in I$ и $j_1, j_2 \in J$. Како су I и J идеали следи $i_1 + i_2 \in I$ и $j_1 + j_2 \in J$, па је $x + y = (i_1 + i_2) + (j_1 + j_2) \in I + J$. Даље, за $a \in A$ важи $a \cdot x = (a \cdot i_1) + (a \cdot j_1)$, па како је $a \cdot i_1 \in I$ и $a \cdot j_1 \in J$, то је $a \cdot x \in I + J$. Овим је доказано да је $I + J$ идеал прстена A .

Докажимо и да је $I \cdot J$ идеал прстена A . Иска су $x, y \in I \cdot J$. Тада је

$$x = i_1 \cdot j_1 + \cdots + i_n \cdot j_n \quad \text{и} \quad y = i'_1 \cdot j'_1 + \cdots + i'_m \cdot j'_m,$$

за неке $n, m \in \mathbb{N}$, $i_1, \dots, i_n, i'_1, \dots, i'_m \in I$ и $j_1, \dots, j_n, j'_1, \dots, j'_m \in J$. Тада је

$$x + y = i_1 \cdot j_1 + \cdots + i_n \cdot j_n + i'_1 \cdot j'_1 + \cdots + i'_m \cdot j'_m \in I \cdot J,$$

док за $a \in A$ важи

$$x = (a \cdot i_1) \cdot j_1 + \cdots + (a \cdot i_n) \cdot j_n,$$

што је такође елемент $I \cdot J$, јер је I идеал прстена A , па је $a \cdot i_k \in I$ за све $k = \overline{1, n}$. \square

Примстимо да је $I \cdot J$ заправо најмањи идеал који садржи све могуће производе склопната из I са склопнитима из J и да је $I \cdot J \subset I \cap J$. Са другог стране, унија $I \cup J$ је идеал ако и само ако је један од тих идеала садржан у другом. Заправо, ако посматрамо само операцију сабирања, приметимо да су идеали заправо подгрупе групе $(A, +)$, а знатмо 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 3.14 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 генериран склопнитом a .

Решење. 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 . \clubsuit

Став 3.15 Сваки идеал у \mathbb{Z} је облика $\langle m \rangle$ за неки природан број m .

Доказ. Иска је $I \triangleleft \mathbb{Z}$. Како је $(I, +)$ подгрупа групе $(\mathbb{Z}, +)$ (која је циклична), то на основу става 1.14 добијамо да је $I = \langle m \rangle$. \square

Напомена: Идеал $\langle m \rangle$ једнак је $m\mathbb{Z}$ (скуп свих целобројних умножака броја m).

Пример 3.16 Нека су m и n позитивни цели бројеви. Одредити:

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

Решење. Прес 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 је по ставу 3.15 идеал $\langle m \rangle + \langle n \rangle$ сигурно главни, потребно је само одредити који је његов генератор. Но, није потребно много размишљати о томе. Из горње једнакости се намеће да је

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

где је $d = \text{NZD}(m, n)$. Прес 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 $d | m$ и $d | n$, 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 $\langle m \rangle \cap \langle n \rangle$. Примстимо да $x \in \langle m \rangle \cap \langle n \rangle$ ако и само ако $m | x$ и $n | x$. Но, то управо значи да је $\langle m \rangle \cap \langle n \rangle = \langle \text{NZS}(m, n) \rangle$. ♠

Пример 3.17 У прстену $\mathbb{Z}[X]$ постоји идеал који није главни.

Решење. Посматрајмо идеал I генерисан са два елемента 2 и X , тј. $I = \langle 2, X \rangle$. Ознака $\langle S \rangle$ означава најмањи идеал (који увек постоји јер је пресек свих колекција 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 $a(X) | X$, 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 $1 = 2p(0)$, те би следило да $\frac{1}{2} \in \mathbb{Z}$. Закључујемо да наведени идеал није главни. ♠

Став 3.18 Нека је K ма које поље. Тада је сваки идеал у прстену $K[X]$ главни.

Доказ. Користићемо 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

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

Ово је познато еуклидско дељење полинома, или дељење са остатком, са којим смо упознati у средњој школи (погледати додатак I).

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 јер је I идеал. Докажимо да је $I = \langle \mu \rangle$. Посматрајмо произвољни елемент $a \in I$. На основу резултата наведеног горе, постоји полиноми² q и r 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 $\mu | a$, тс да $a \in \langle \mu \rangle$, чиме је доказ завршен. \square

Став 3.19 Нека је K поље и $I \triangleleft K$. Тада је $I = \{0\}$, или је $I = K$.

Доказ. Претпоставимо да је I идеал у K и да је $I \neq \{0\}$. То значи да идеал I садржи неки елемент $x \neq 0$. Ако је a ма који елемент из K , добијамо да и a припада идеалу I . Наимс, 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 . Закључујемо да је $I = K$. \square

Пример 3.20 Нека је A комутативан прстен са јединицом и $u \in U(A)$. Тада је $\langle u \rangle = A$.

Решење. Доказ се изводи као у претходном примеру. ♣

3.4 Хомоморфизми

Пређимо сада на појам хомоморфизма.

Дефиниција 3.21 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ два комутативна прстена са јединицом. Функција $f: A \rightarrow B$ је хомоморфизам комутативних прстена са јединицом 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 3.22 Нека је $n \geq 2$ природан број. 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.

² 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.

Решење. Ово директно следи из задатка 1.1. ♣

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

Дефиниција 3.23 Нека је $f: A \rightarrow B$ хомоморфизам комутативних прстена са јединицом. ЈЕЗГРО хомоморфизма f , у означи $\text{Ker}(f)$ дефинише се као:

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

Став 3.24 Нека је $f: A \rightarrow B$ хомоморфизам комутативних прстена са јединицом. Тада важи:

- a) $\text{Ker}(f) \triangleleft A$;
- 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) Иако $x, y \in \text{Ker}(f)$. 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 $a \in A$:

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

па $a \cdot x \in \text{Ker}(f)$.

б) Иако 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, $x + y \in f^{-1}[J]$.

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) Иако 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 неке $x \in I$. Како је I идеал, $a \cdot x$ припада I , па је $b \cdot u = f(a) \cdot f(x) = f(a \cdot x)$ из $f[I]$. □

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

Пример 3.25 У општем случају директна слика идеала не мора бити идеал.

Решење. 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 става 3.19, једини идеали у \mathbb{Q} : $\{0\}$ и \mathbb{Q} . \clubsuit

Став 3.26 Нека је $n \geq 2$ цео број. Тада је сваки идеал у \mathbb{Z}_n главни.

Доказ. Искористићемо хомоморфизам $\rho_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$, који је „на“. Нека је $J \triangleleft \mathbb{Z}_n$. Тада је $\rho_n^{-1}[J] \triangleleft \mathbb{Z}$. На основу става 3.15, знамо да постоји $m \geq 0$ такав да је $\rho_n^{-1}[J] = \langle m \rangle$. Како је пресликавање ρ_n „на“ важи $J = \rho_n[\rho_n^{-1}[J]]$, док је

$$\begin{aligned} \rho_n[\langle m \rangle] &= \{\rho_n(a \cdot m) : a \in \mathbb{Z}\} = \{\rho_n(a) \cdot \rho_n(m) : a \in \mathbb{Z}\} \\ &= \{b \cdot \rho_n(m) : b \in \mathbb{Z}\} = \langle \rho_n(m) \rangle \end{aligned}$$

(претпоследња једнакост следи из чињенице да је ρ_n „на“). Дакле, J је главни идеал генерисан са $\rho_n(m)$, чиме је доказ завршен. \square

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 ове групе, а по ставу 1.14 знамо како изгледају 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} за право 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, који остављамо читаоцу.

Пример 3.27 Навести пример комутативног прстена са јединицом и подгрупе адитивне групе тог прстена, која није идеал.

Решење. 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 (директан производ прстена се дефинише на начин аналоган дефиницији директног производа група). 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. \clubsuit

Пример 3.28 Наћи све идеале у прстену \mathbb{Z}_{12} .

Решење. По ставу 3.26, сви идеали у овом прстену су 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 $m \notin \Phi(12)$ (на основу (3.1)), тј. ако и само ако $2 \mid m$ или $3 \mid m$. 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 генералисати). Такође имамо да важи $9 = -3 = (-1) \cdot 3$, па је и $\langle 9 \rangle = \langle 3 \rangle$. Слично 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 цисо број q такав да је $2 = 4m - 12q$. Међутим, десна страна ове једнакости је деливa са 4, док лева није, што није могуће. Како је очигледно $4 \in \langle 2 \rangle$, то добијамо да је $\langle 4 \rangle \subset \langle 2 \rangle$ (идсал генерисан са 4 је прави подскуп идсала 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 идсали прстен \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.

3.5 Количнички прстени; теорема о изоморфизму

Започнимо следећом дефиницијом.

Дефиниција 3.29 Нека је $I \triangleleft A$. На A дефинишемо релацију КОНГРУЕНЦИЈЕ ПО МОДУЛУ I са:

$$a \equiv b \pmod{I} \quad \text{акко} \quad a - b \in I.$$

Проверимо да је ова релација једна релација сквиваленције, која се добро слаже са операцијама.

Рефлексивност. Како је $a - a = 0 \in I$, то је заиста $a \equiv a \pmod{I}$ за све елементе $a \in A$.

Симетричност. Иако 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. Иако 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 +. Иако 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

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

па је $a + b \equiv a' + b' \pmod{I}$.

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

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

те је $a \cdot b \equiv a' \cdot b' \pmod{I}$.

Приметимо да је класа сквиваленције елемента a заправо скуп

$$a + I = \{a + x : x \in I\}.$$

Скуп класа сквиваленције означавамо са A/I . Приметимо да „слагање са +“ имплицира да је са

$$(a + I) + (b + I) := (a + b) + I$$

добро дефинисана операција сабирања на A/I . Заиста, ако је $a + I = a' + I$ и $b + I = b' + I$, тада је $a \equiv a' \pmod{I}$ и $b \equiv b' \pmod{I}$, па је $a + b \equiv a' + b' \pmod{I}$, а самим тим $(a + b) + I = (a' + b') + I$. На сличан начин се може доказати да „слагање са ·“ имплицира да је са

$$(a + I) \cdot (b + I) := (a \cdot b) + I$$

добро дефинисана операција множења на A/I . Није тешко проверити да је овако дефинисана алгебарска структура $(A/I, +, \cdot)$ један комутативан прстен са јединицом. Овај прстен се назива **КОЛИЧНИЧКИ ПРСТЕН ПРСТЕНА A ПО ИДЕАЛУ I**. Наравно, приликом рачуна у A/I искс од заграда (из дефиниције операција) нећемо увек записивати.

Као и у случају група, важе и теореме о изоморфизмима за прстене. Навешћемо само прву.

Теорема 3.30 (**Теорема о изоморфизму за прстене**) Нека је $f: A \rightarrow B$ хомоморфизам комутативних прстена са јединицом. Тада је $\tilde{f}: A/\text{Ker}(f) \rightarrow \text{Im}(f)$ задато са:

$$\tilde{f}(a + \text{Ker}(f)) := f(a)$$

изоморфизам комутативних прстена са јединицом. Дакле, $A/\text{Ker}(f) \cong \text{Im}(f)$.

Доказ. Проверимо најпре да је \tilde{f} добро дефинисано. У ту сврху, нека је $a + \text{Ker}(f) = b + \text{Ker}(f)$. То значи да $a - b \in \text{Ker}(f)$, тј. да је $f(a) = f(b)$. Закључујемо да је \tilde{f} заиста добро дефинисано.

Проверимо да је \tilde{f} хомоморфизам. Важи:

$$\begin{aligned} \tilde{f}(a + \text{Ker}(f)) + \tilde{f}(b + \text{Ker}(f)) &= f(a) + f(b) = f(a + b) = \tilde{f}((a + b) + \text{Ker}(f)) \\ &= \tilde{f}((a + \text{Ker}(f)) + (b + \text{Ker}(f))), \end{aligned}$$

као и

$$\begin{aligned} \tilde{f}(a + \text{Ker}(f)) \cdot \tilde{f}(b + \text{Ker}(f)) &= f(a) \cdot f(b) = f(a \cdot b) = \tilde{f}((a \cdot b) + \text{Ker}(f)) \\ &= \tilde{f}((a + \text{Ker}(f)) \cdot (b + \text{Ker}(f))). \end{aligned}$$

Јасно је да је \tilde{f} „на“. Остаје да се провери да је \tilde{f} „1–1“. Важи:

$$\begin{aligned}\tilde{f}(a + \text{Ker}(f)) = \tilde{f}(b + \text{Ker}(f)) &\implies f(a) = f(b) \\ &\implies f(a - b) = 0 \\ &\implies a - b \in \text{Ker}(f) \\ &\implies a + \text{Ker}(f) = b + \text{Ker}(f).\end{aligned}$$

Проверимо још и да \tilde{f} слика јединицу прстена у јединицу прстена:

$$\tilde{f}(1_A + \text{Ker}(f)) = f(1_A) = 1_B.$$

Закључујемо да је \tilde{f} заиста један изоморфизам комутативних прстена са јединицом. \square

Пример 3.31 Нека је $I \triangleleft A$. Тада је $p: A \rightarrow A/I$ један епиморфизам. ♣

Пример 3.32 За све $n \geq 1$ важи: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Решење. Хомоморфизам $\rho_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$, дат раније, је „на“, а осим тога $\text{Ker}(\rho_n) = n\mathbb{Z}$, те резултат следи из претходног теореме. ♣

3.6 Директан производ прстена; Кинеска теорема о остацима

Већ смо у претходној лекцији навели појам директног производа два прстена, наведимо дефиницију за директан производ коначно много прстена.

Дефиниција 3.33 Нека су $(A_1, +^1, \cdot^1), \dots, (A_n, +^n, \cdot^n)$ комутативни прстени са јединицом. На Декартовом производу

$$A = A_1 \times \cdots \times A_n,$$

задајемо структуру комутативног прстена са јединицом са:

$$\begin{aligned}(a_1, \dots, a_n) + (b_1, \dots, b_n) &:= (a_1 +^1 b_1, \dots, a_n +^n b_n), \\ (a_1, \dots, a_n) \cdot (b_1, \dots, b_n) &:= (a_1 \cdot^1 b_1, \dots, a_n \cdot^n b_n).\end{aligned}$$

За овај комутативан прстен са јединицом кажемо да је ДИРЕКТАН ПРОИЗВОД ПРСТЕНА $(A_1, +^1, \cdot^1), \dots, (A_n, +^n, \cdot^n)$.

Приметимо да је $0_A = (0_{A_1}, \dots, 0_{A_n})$ и $1_A = (1_{A_1}, \dots, 1_{A_n})$. Проверу да смо овако заиста добили комутативни прстен са јединицом остављамо читаоцима.

Став 3.34 Нека су m_1, \dots, m_n позитивни цели бројеви такви да за све $i \neq j$ важи: $\text{NZD}(m_i, m_j) = 1$. 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

$$f: \mathbb{Z} \rightarrow (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})$$

са:

$$f(x) = (x + m_1\mathbb{Z}, \dots, x + m_n\mathbb{Z}).$$

Остављамо читаоцима да провере да је f заиста хомоморфизам. Одредимо језгро овог хомоморфизма. Нека је $x \in \text{Кер}(f)$. То значи да је $f(x) = (m_1\mathbb{Z}, \dots, m_n\mathbb{Z})$, тј. то значи да $x \in m_1\mathbb{Z}, \dots, x \in m_n\mathbb{Z}$. Дакле, у језгру се налазе они цели бројеви, који су дељиви свим бројевима m_1, \dots, m_n . Како су m_i узајамно прости то језгро чине умношти од $m_1 \cdots m_n$, тј.

$$\text{Кер}(f) = (m_1 \cdots m_n)\mathbb{Z}.$$

По творсми 3.30 добијамо да је

$$\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z} \cong \text{Im}(f).$$

Но, како је $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$ (по примсру 3.32), то је

$$|\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z}| = m_1 \cdots m_n = |(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})|.$$

Дакле, f мора бити „на”. Тиме смо добили тражени изоморфизам. \square

Последица 3.35 (Кинеска теорема о остацима) Нека су m_1, \dots, m_n позитивни цели бројеви који су пар по пар узајамно прости и x_1, \dots, x_n произвољни цели бројеви. Тада постоји цео број x такав да је

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\vdots \\ x &\equiv x_n \pmod{m_n}. \end{aligned}$$

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

$$(x_1 + m_1\mathbb{Z}, \dots, x_n + m_n\mathbb{Z}) \in (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z}).$$

Како је хомоморфизам f , из доказа претходног творсма, „на”, то постоји $x \in \mathbb{Z}$ који се слика у наведени елемент, тј. постоји $x \in \mathbb{Z}$ за који је

$$x + m_1\mathbb{Z} = x_1 + m_1\mathbb{Z}, \dots, x + m_n\mathbb{Z} = x_n + m_n\mathbb{Z},$$

но, то управо значи да је

$$x \equiv x_1 \pmod{m_1}, \dots, x \equiv x_n \pmod{m_n}.$$

Уколико је x' други цео број који задовољава наведене конгруенције, то значи да је $f(x) = f(x')$, тј.

$$x - x' \in \text{Ker}(f) = (m_1 \cdots m_n)\mathbb{Z},$$

као што је и тврђено. \square

Став 3.36 Ако су прстени A и B изоморфни, онда је $(U(A), \cdot) \cong (U(B), \cdot)$

Доказ. Инвертибилни елементи се 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 $f: A \rightarrow B$. 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. \square

Став 3.37 Важи једнакост: $U(A_1 \times \cdots \times A_n) = U(A_1) \times \cdots \times U(A_n)$.

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

$$\begin{aligned} a \in U(A_1 \times \cdots \times A_n) &\iff \text{постоји } b = (b_1, \dots, b_n) \in A : a \cdot b = 1 \\ &\iff \text{постоји } b_i \in A_i : a_i \cdot b_i = 1 \text{ за све } i \\ &\iff a_1 \in U(A_1), \dots, a_n \in U(A_n) \\ &\iff a \in U(A_1) \times \cdots \times U(A_n), \end{aligned}$$

што је и требало доказати. \square

Теорема 3.38 Ако су m_1, \dots, 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 за сваки природан број $m \geq 2$ важи $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$ (по примеру 3.32), то први резултат следи из става 3.34. Осим тога, $\varphi(m) = |U(\mathbb{Z}_m)|$, те резултат за Ојлерову функцију следи из става 3.36 и става 3.37. \square

Кинеска теорема о остацима, поред свог теоријског значаја и занимљивости, има и практичну примену базирану на једноставној опсервацији да је лакше рачунати са малим бројевима, него са величима. Тако

да, у случају да морамо да рачунамо са вишсифреним бројевима, а зnamо да резултат сигурно неће премашити неки одређени број N , посао можемо урадити коришћењем паралелног израчунавања и Кинеске теореме о остацима на следећи начин. Ако имамо процесор са r језгара, изаберемо r у паровима узајамно простих природних бројева n_1, n_2, \dots, n_r (нпр. можемо изабрати да су ово различити прости бројеви), тако да је $n_1 n_2 \cdots n_r > N$. Затим, на i -том процесору израчунамо остатак при дељењу датог израза са n_i , а коначан резултат добијамо из ових r остатака примсном Кинеској теоремом о остацима.

3.7 Коначне подгрупе мултипликативне групе поља; примитивни корен

Групе $U(\mathbb{Z}_n)$ имају занимљиву структуру, но ми се њима у овом поглављу нећемо детаљно бавити (погледати додатак III). Но, ипак ћемо, због примсна, 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 3.39 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. Како је Абелова група A коначна, по тсорсми 2.11 је она изоморфна производу коначних цикличних група:

$$A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n},$$

где је $d_1 > 1$ и $d_i \mid d_{i+1}$ за све $i = \overline{1, n-1}$. Овде је $m = |A| = d_1 \cdots d_n$. Приметимо да је за све $a \in A$ испуњено да је $d_n a = 0$. Наиме, ако је $x = (x_1, \dots, x_n) \in \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$, онда је

$$d_n x = d_n(x_1, \dots, x_n) = (d_n x_1, \dots, d_n x_n) = (0, \dots, 0),$$

јер, за све i , $\omega(x_i) \mid d_i \mid d_n$, па мора бити $d_n x_i = 0$, за све i , на основу (1.9). С обзиром да је A изоморфна групи $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_n}$, заиста је за све $a \in A$: $d_n a = 0$. Но, то значи да у A постоји $m = d_1 \dots d_n$ слемената a за које је $d_n a = 0$, те на основу претпоставке закључујемо да мора бити $m \leq d_n$, што нам заправо показује да је $n = 1$, тј да је $A \cong \mathbb{Z}_{d_1}$. \square

Теорема 3.40 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 нула 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 полином различит од 0. 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 .

Прећимо 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. \square

Дакле, доказали смо да је свака КОНАЧНА подгрупа мултипликативне групе поља циклична. Нагласимо 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. Према свега, уведимо терминологију.

Дефиниција 3.41 Сваки генератор групе $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ зове се ПРИМИТИВНИ КОРЕН модуло p .

Став 3.42 Нека је r ма који примитивни корен модуло p . Тада је са:

$$\text{ind}_r(a) = x \text{ ако } r^x = a,$$

дефинисан изоморфизам $\text{ind}_r: (\mathbb{Z}_p \setminus \{0\}, \cdot_p) \rightarrow (\mathbb{Z}_{p-1}, +_{p-1})$.

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 $p - 1$ елемента, то $x \in \mathbb{Z}_{p-1}$. Ми треба да проверимо да ли је ind_r хомоморфизам, тј. да ли је

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

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

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

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

Пример 3.43 Наћи све примитивне корене модуло 13.

Решење. 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 таблику за ind_2 .

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

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

Ова таблица нам омогућава да нађемо и све остале примитивне корене модуло 13. Наиме, на основу става 1.11 важи следеће:

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

Пошто је у нашем случају $\omega(2) = 12$, то је $\omega(2^m) = 12$ ако и само ако је $\text{NZD}(m, 12) = 1$, 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 3.44 Решити конгруенцију

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

Решење. Већ знајмо 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 $\text{ind}_2(x) \in \mathbb{Z}_{12}$. На овај начин смо примнном 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 $y = \text{ind}_2(x)$, добијамо да је

$$x \equiv 2^y \equiv 2^7 \equiv 11 \pmod{13}.$$



Задаци

3.1 Иска је p прост број и $R = \left\{ \frac{m}{n} \in \mathbb{Q} : p \nmid n \right\}$. Доказати да је R потпрстен од \mathbb{Q} .

3.2 Иска је R комутативан прстен са јединицом. За слемент x кажемо да је нилпотентан уколико је за неко $n \geq 1$ испуњено $x^n = 0$. Доказати да скуп свих нилпотентних слемсната чини идеал прстена R .

3.3 Ако је x нилпотентан слемент комутативног прстена са јединицом R доказати да је слемент $1 - x$ инвертибилан.

3.4 Иска је $R = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Показати да је R потпрстен од \mathbb{C} у коме је сваки слемент различит од 0 инвертибилан.

3.5 Иска је $R = I + J$ за искс идеалс I, J прстена R . Доказати да је тада и $I^2 + J^2 = R$ ($I^2 = I \cdot I$).

3.6 Иска је S потпрстен комутативног прстена са јединицом R и I идеал у R . Доказати или оповргнути: $S + I$ је потпрстен од R .

3.7 Показати да је пресек два потпрстна увек потпрстен, као и да унија не мора бити потпрстен.

3.8 Одредити идеал $I \triangleleft \mathbb{Z}$ задат са: $I = (\langle 45 \rangle + \langle 36 \rangle) \cap \langle 12 \rangle$.

3.9 Одредити праве делитеље нуле у прстену: а) \mathbb{Z}_{21} ; б) \mathbb{Z}_{16} .

3.10 Одредити инвертибилис слементе у прстену: а) \mathbb{Z}_{15} ; б) \mathbb{Z}_{36} .

3.11 Одредити све идеале у прстену: а) \mathbb{Z}_{24} ; б) \mathbb{Z}_{16} .

3.12 а) Испитати да ли је са $f: \mathbb{Z}_{36} \rightarrow \mathbb{Z}_9$, $f(x) = \rho(x, 9)$, дефинисан хомоморфизам комутативних прстена са јединицом и у потврдном случају наћи $\text{Ker}(f)$.

б) Испитати да ли је са $f: \mathbb{Z}_{36} \rightarrow \mathbb{Z}_6$, $f(x) = \rho(x, 6)$, дефинисан хомоморфизам комутативних прстена са јединицом и у потврдном случају наћи $\text{Ker}(f)$.

в) Испитати да ли је са $f: \mathbb{Z}_{36} \rightarrow \mathbb{Z}_{10}$, $f(x) = \rho(x, 10)$, дефинисан хомоморфизам комутативних прстена са јединицом и у потврдном случају наћи $\text{Ker}(f)$.

3.13 Решити следеће конгруенције:

- a) $3x \equiv 4 \pmod{7}$;
- б) $4x \equiv 2 \pmod{6}$;
- в) $15x \equiv 4 \pmod{10}$;
- г) $12x \equiv 21 \pmod{15}$.

3.14 Решити системе конгруенција:

- а) $x \equiv 3 \pmod{7}$ $x \equiv 5 \pmod{8}$;
- б) $x \equiv 5 \pmod{13}$ $x \equiv -1 \pmod{8}$ $x \equiv 4 \pmod{7}$;
- в) $2x \equiv 1 \pmod{7}$ $4x \equiv 2 \pmod{9}$ $5x \equiv 3 \pmod{11}$.

3.15 Одредити барем један примитивни корен r модуло 7 и помоћу таблице за ind_r одредити све примитивне корене модуло 7. Коришћењем примитивног корена r решити следеће конгруенције:

- | | |
|------------------------------|------------------------------|
| а) $4x \equiv 3 \pmod{7}$; | б) $x^2 \equiv 2 \pmod{7}$; |
| в) $x^3 \equiv 2 \pmod{7}$; | г) $x^4 \equiv 3 \pmod{7}$. |

3.16 Одредити барем један примитивни корен r модуло 11 и помоћу таблице за ind_r одредити све примитивне корене модуло 11. Коришћењем примитивног корена r решити следеће конгруенције:

- | | |
|-------------------------------|--------------------------------|
| а) $4x \equiv 3 \pmod{11}$; | б) $x^2 \equiv 3 \pmod{11}$; |
| в) $x^3 \equiv 2 \pmod{11}$; | г) $x^4 \equiv -3 \pmod{11}$. |