

Додатак I

Прстени полинома

Конструкција прстена полинома

У глави 3 разматрали смо прстен полинома са једном неодређеном над комутативним прстеном са јединицом A , тј. прстен $A[X]$. Тада је било наведено да је то скуп свих формалних израза облика $a_0 + a_1X + \dots + a_nX^n$, где је $n \geq 0$ природан број, а a_i елементи прстена A , а да су операције онакве какве зnamо из средње школе. Уз додатак да је $a_0 + a_1X + \dots + a_nX^n = b_0 + b_1X + \dots + b_mX^m$ ако и само ако је $n = m$ и $a_i = b_i$ за све i .

Но, сада желимо да то исправимо, тј. да дамо стварну дефиницију прстена полинома, а уз то и његову конструкцију. У чему је проблем? Претходна неформална дефиниција доста подсећа на дефиницију скupa комплексних бројева из школе као скупа свих израза облика $a + bi$, где су a и b реални бројеви, а i је ‘имагинарна јединица’, тј. нови број за који важи $i^2 = -1$, а онда је речено да се операције врше на ‘убичајен начин’ узимајући у обзир ту чињеницу за број i . Но, тада је ипак речено да се то може и прецизно урадити. Посматра се скуп $\mathbb{R} \times \mathbb{R}$ и на њему се операције задају са:

$$(a, b) + (c, d) := (a + c, b + d) \quad (a, b) \cdot (c, d) := (ac - bd, ad + bc).$$

Потом се примести да се парови облика $(a, 0)$ ‘понашају’ као реални бројеви, тј. $(a, 0) + (b, 0) = (a + b, 0)$ и $(a, 0) \cdot (b, 0) = (ab, 0)$, а да за елемент $(0, 1)$ важи: $(0, 1) \cdot (0, 1) = (-1, 0)$. Уз чињеницу да важи и једнакост

$$(a, b) = (a, 0) + (b, 0)(0, 1),$$

констатује се да се парови облика $(a, 0)$ могу сматрати за реалне бројеве, док је пар $(0, 1)$ наведена имагинарна јединица и добија се онај неформални опис. Ми ћемо на овакав начин и показати да прстен полинома заиста постоји.

Наведимо најпре дефиницију прстена полинома.

Дефиниција I.1 Нека је A комутативни прстен са јединицом. Под прстеном полинома над прстеном A и са неодређеном X подразумевамо сваки комутативни прстен са јединицом B који садржи као свој потпрстен са јединицом прстен A' изоморфан прстену A и елемент X такав да се сваки елемент из B може на јединствен начин представити у облику $a_0 + a_1X + \dots + a_nX^n$ за $n \geq 0$ и $a_i \in A'$.

Оно што се одмах можемо запитати после ове дефиниције је да ли може постојати више прстена полинома над прстеном A и неодређеном X . Наравно, одговор је потврдан, али сви они су међусобно изоморфни. Наиме, нека су B_1 и B_2 такви прстени који, редом, садрже потпрстене A'_1 и A'_2 изоморфне прстену A и елементе $X_i \in B_i$ који се наводе у дефиницији. Пошто су A'_1 и A'_2 изоморфни прстену A , они су и међусобно изоморфни, дакле постоји изоморфизам $f: A'_1 \rightarrow A'_2$. Стога можемо задати $F: B_1 \rightarrow B_2$ са

$$F(a_0 + a_1X_1 + \dots + a_nX_1^n) := f(a_0) + f(a_1)X_2 + \dots + f(a_n)X_2^n.$$

С обзиром да је f изоморфизам, није тешко уврити се да је и F изоморфизам (проверите то!).

Дакле, свака два прстена полинома над прстеном A и неодређеном X међусобно су изоморфна и можемо користити ознаку $A[X]$ да означимо било који од њих. Но, горе смо показали да су свака два изоморфна ако постоје. А да ли уопште постоји такав објекат? Сада ћемо се у то уврити.

Приметимо да се у сваком неформално задатом полиному $a_0 + a_1X + \dots + a_nX^n$ појављује коначан низ (a_0, a_1, \dots, a_n) , односно бесконачан низ $(a_0, a_1, \dots, a_n, 0, 0, \dots)$. Са $A^\mathbb{N}$ је природно означити скуп свих низова (a_0, a_1, \dots) слесната из A . Но, нас не занимају сви такви низови, него само низови који су једнаки 0 почев од неког члана. Стога посматрамо скуп

$$A^\omega := \{(a_0, a_1, a_2, \dots) \in A^\mathbb{N} : (\exists n \in \mathbb{N})(\forall i > n) a_i = 0\}.$$

Потребно је дефинисати и операције на скупу A^ω . Сабирање се дефинише лако:

$$(a_0, a_1, a_2, \dots) + (b_0, b_1, b_2, \dots) := (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots),$$

док је множење нешто сложеније:

$$(a_0, a_1, a_2, \dots) \cdot (b_0, b_1, b_2, \dots) := (c_0, c_1, c_2, \dots),$$

где је за све $k \geq 0$:

$$c_k := \sum_{i+j=k} a_i b_j.$$

Покажимо да је $(A^\omega, +, \cdot)$ један прстен са јединицом. Нека је за низ $a \in A^\omega$ са a_n означен елемент који се налази на позицији n (дакле, на $(n+1)$ -ом месту, пошто индекси почињу са 0).

Нека су $p, q, r \in A^\omega$. Провера асоцијативности сабирања је лака:

$$\begin{aligned} ((p+q)+r)_n &= (p+q)_n + r_n = ((p_n+q_n)) + r_n \\ &= (p_n + (q_n + r_n)) = p_n + (q+r)_n = (p+(q+r))_n. \end{aligned}$$

Нешто је сложенија провера дистрибутивности множења у односу на сабирање:

$$\begin{aligned} (p \cdot (q+r))_n &= \sum_{i+j=n} p_i(q+r)_j = \sum_{i+j=n} p_i(q_j+r_j) \\ &= \sum_{i+j=n} p_i q_j + \sum_{i+j=n} p_i r_j = (p \cdot q)_n + (p \cdot r)_n. \end{aligned}$$

Најсложенија је провера асоцијативности множења:

$$\begin{aligned} ((p \cdot q) \cdot r)_n &= \sum_{s+k=n} (p \cdot q)_s r_k = \sum_{s+k=n} \sum_{i+j=s} (p_i q_j) r_k \\ &= \sum_{i+j+k=n} p_i (q_j r_k) = \sum_{i+t=n} p_i \sum_{j+k=t} q_j r_k \\ &= \sum_{i+t=n} p_i (q \cdot r)_t = (p \cdot (q \cdot r))_n. \end{aligned}$$

Врло лако се проверава да су и сабирање и множење комутативне операције. Са \bar{a} за $a \in A$, означавамо низ коме је нулти члан једнак a , а сви остали једнаки $0 (= 0_A)$:

$$\bar{a} := (a, 0, 0, \dots).$$

Уз чињеницу да је $\overline{1_A} \cdot p = p \cdot \overline{1_A}$ за свако $p \in A^\omega$, где смо са 1_A означили јединицу у прстену A , добијамо да је заиста $(A^\omega, +, \cdot)$ један комутативни прстен са јединицом, где је $1_{A^\omega} = \overline{1_A}$.

Означимо са X елемент $(0, 1, 0, \dots)$. Дакле, X је низ елемената из A^ω такав да је

$$X_k = \begin{cases} 1, & k = 1 \\ 0, & \text{иначе.} \end{cases}$$

Тада је

$$(X^2)_k = \sum_{i+j=k} X_i X_j = \begin{cases} 1, & k = 2 \\ 0, & \text{иначе.} \end{cases}$$

Индукцијом се може добити да је за $n \geq 1$

$$(X^n)_k = \begin{cases} 1, & k = n \\ 0, & \text{иначе.} \end{cases}$$

Подсестимо се да смо за $a \in A$ означили са \bar{a} низ $(a, 0, 0, \dots)$. Тада је

$$(\bar{a} \cdot X^n)_k = \sum_{i+j=k} \bar{a}_i (X^n)_j = a(X^n)_k = \begin{cases} a, & k = n \\ 0, & \text{иначе.} \end{cases}$$

Дакле, $\bar{a} \cdot X^n = (0, \dots, 0, a, 0, \dots)$, где се a налази на позицији n .

Сада можемо видети како се записује произвољни елемент из A^ω . Наиме, сваки елемент $p \in A^\omega$ је облика $p = (a_0, \dots, a_n, 0, \dots)$ за неки $n \geq 0$ и $a_i \in A$. Тада добијамо

$$\begin{aligned} p &= (a_0, \dots, a_n, 0, \dots) \\ &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \cdots + (0, \dots, 0, a_n, 0, \dots) \\ &= \bar{a}_0 + \bar{a}_1 X + \cdots + \bar{a}_n X^n. \end{aligned}$$

Наравно, уместо $\bar{a}_i \cdot X^i$ писали смо краће $\bar{a}_i X^i$. Уколико је

$$\bar{a}_0 + \bar{a}_1 X + \cdots + \bar{a}_n X^n = \bar{b}_0 + \bar{b}_1 X + \cdots + \bar{b}_m X^m,$$

онда је заправо

$$(a_0, a_1, \dots, a_n, 0, \dots) = (b_0, b_1, \dots, b_m, 0, \dots),$$

те следи да је $n = m$ и $a_i = b_i$ за све i .

Приметимо да важе следеће једнакости:

$$\bar{a} + \bar{b} = \overline{a + b} \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}.$$

Из ових једнакости можемо закључити да је са $f(a) := \bar{a}$ задат један хомоморфизам прстене $f: A \rightarrow A^\omega$, који је '1-1' и стога успоставља изоморфизам између A и његове слике $A' = \{\bar{a} : a \in A^\omega\}$. На основу свега добијеног можемо закључити да прстен A^ω заиста задовољава све услове који се захтевају од прстене полинома над прстеном A са неодређеном X . Тиме смо показали да за сваки комутативни прстен са јединицом A заиста постоји прстен полинома $A[X]$ над тим прстеном и са неодређеном X .

Еуклидско дељење у прстену $K[X]$

Уколико је $0 \neq a(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ и $a_n \neq 0$, тада кажемо да је полином $a(X)$ степена n и то пишемо овако: $\deg(a(X)) = n$. Како је производ ненула елемената у пољу такође ненула елемент, ако су полиноми $a(X)$ и $b(X)$ различити од 0, онда је $\deg(a(X) \cdot b(X)) = \deg(a(X)) + \deg(b(X))$. Но, погодно је имати ову једнакост чак и ако је један од полинома једнак 0. Стога уводимо да је $\deg(0) := -\infty$, при чemu сматрамо да је $n + (-\infty) = (-\infty) + n = -\infty = (-\infty) + (-\infty)$. Ова конвенција нам мало скраћује запис неких резултата.

Формулишими одмах теорему о дељењу полинома са остатком.

Теорема I.2 Нека је K поље, $a(X) \in K[X]$, $b(X) \in K[X] \setminus \{0\}$. Тада постоје и јединствено су одређени полиноми $q(X), r(X) \in K[X]$ за које важи

$$a(X) = q(X)b(X) + r(X), \quad \deg(r(X)) < \deg(b(X)).$$

Доказ. Докажимо најпре егзистенцију полинома $q(X)$ и $r(X)$. Доказ изводимо индукцијом по $\deg(a(X))$.

Ако је $\deg(a(X)) < \deg(b(X))$, онда можемо узети да је $q(X) = 0$ и $r(X) = a(X)$, јер је тада $a(X) = 0 \cdot b(X) + a(X)$ и $\deg(a(X)) < \deg(b(X))$.

Претпоставимо да $n = \deg(a(X)) \geq \deg(b(X))$ и да је тврђење тачно за све полиноме степена мањег од n . Тада је $a(X) = a_n X^n + \dots + a_1 X + a_0$, а $b(X) = b_m X^m + \dots + b_1 X + b_0$, при чemu је $n \geq m$. Знамо како се дељење изводи: пореде се $a_n X^n$ и $b_m X^m$ и први члан у количнику је заправо једнак $\frac{a_n}{b_m} X^{n-m}$. Сада формирајмо нови полином $a_1(X)$, краће a_1 , са:

$$a_1 := a - \frac{a_n}{b_m} X^{n-m} \cdot b.$$

На овај начин смо елиминисали водећи моном из полинома a , па добијамо да је $\deg(a_1) < \deg(a)$ и прсма индуктивној хипотези, постоје полиноми q_1 и r_1 за које је

$$a_1 = q_1 \cdot b + r_1, \quad \deg(r_1) < \deg(b).$$

Тада је и

$$a = q \cdot b + r,$$

ако је $q = \frac{a_n}{b_m} X^{n-m} + q_1$, а $r = r_1$. Овим смо доказали сгзистенцију тражених полинома.

Докажимо сада јединственост ових полинома. Претпоставимо да постоје и полиноми q_1, r_1 за које важи

$$a = q_1 b + r_1, \quad \deg(r_1) < \deg(b).$$

Дакле

$$qb + r = q_1 b + r_1,$$

па је

$$(q - q_1)b = r - r_1.$$

Уколико је $q \neq q_1$, тј. $q - q_1 \neq 0$, добијамо да је

$$\deg(r - r_1) = \deg((q - q_1)b) = \deg(q - q_1) + \deg(b) \geq \deg(b),$$

што је немогуће јер је

$$\deg(r - r_1) \leq \max\{\deg(r), \deg(r_1)\} < \deg(b).$$

Закључујемо да мора бити $q = q_1$, но тада следи да је и $r = r_1$, чиме смо доказали да су полиноми q и r јединствено одређени. \square

Следећа последица је добро позната.

Последица I.3 Нека је K поље и $a(X) \in K[X] \setminus \{0\}$. Тада у K полином $a(X)$ има највише $\deg(a(X))$ нула.

Доказ. Најједноставније је ово доказати индукцијом по степену полинома. За базу индукције је довољно констатовати да ненула полином степена 0, дакле константа различита од нуле, нема ниједну нулу.

Претпоставимо стога да је тврђење тачно за све полиноме степена мањег од $n > 0$ и нека је $a(X)$ полином степена n . Уколико он нема нула, немамо шта да доказујемо. Уколико је $\alpha \in K$ једна нула полинома $a(X)$, онда поделимо полином $a(X)$ полиномом $X - \alpha$. Добијамо да је

$$a(X) = q(X)(X - \alpha) + r(X), \quad \deg(r(X)) < \deg(X - \alpha) = 1.$$

Дакле, $r(X) = r_0 \in K$. Добијамо:

$$0 = a(\alpha) = q(\alpha)(\alpha - \alpha) + r_0 = r_0.$$

Према томе $a(X) = q(X)(X - \alpha)$. Добили смо резултат који заправо знамо још из средње школе као Безуов став: неки елемент α је нула полинома $a(X)$ ако и само ако $(X - \alpha) | a(X)$ (пажљиви читалац сигурно примећује да смо овде доказали само један смер, али се други смер наравно врло лако показује). Уколико је $\beta \in K$ нула полинома $a(X)$ добијамо да је

$$q(\beta)(\beta - \alpha) = 0.$$

С обзиром да је K поље, следи да је $q(\beta) = 0$ или је $\beta = \alpha$. Дакле, свака нула полинома $a(X)$ или је једнака α или је нула полинома $q(X)$. Како је $\deg(a(X)) = \deg(q(X)) + 1$, по индуктивној хипотези имамо да полином $q(X)$ има највише $n - 1$ нулу, па стога и полином $a(X)$ има највише n нула. \square

Приметимо да је овде веома важно да у прстену коефицијената полинома нема делитеља нуле, што је наравно испуњено у случају да су коефицијенти у пољу.

Пример I.4 Нека је $a(X) = X^2 + 5X + 6 \in \mathbb{Z}_{10}[X]$. Овај полином, који је степена 2 има бар три нуле: $a(2) = 4 + 10 + 6 = 0$, $a(3) = 9 + 15 + 6 = 0$, $a(7) = 49 + 35 + 6 = 0$.

Еуклидов алгоритам у прстену $K[X]$

Дефиниција I.5 Нека је K поље и $a(X)$ и $b(X)$ полиноми из $K[X] \setminus \{0\}$. Највећи заједнички делилац ових полинома је било који полином $d(X)$ из $K[X] \setminus \{0\}$ који задовољава следећа два услова.

- 1) $d(X) | a(X)$ и $d(X) | b(X)$.
- 2) Ако је $c(X) \in K[X]$ такав да $c(X) | a(X)$ и $c(X) | b(X)$, онда $c(X) | d(X)$.

Дакле, највећи заједнички делилац полинома није јединствено одређен, јер ако је $d(X)$ највећи заједнички делилац и $\alpha \in K \setminus \{0\}$, онда је и $\alpha d(X)$ највећи заједнички делилац тих полинома. Да бисмо ипак имали јединственост, бираћемо за највећи заједнички делилац моничан полином. Користићемо ознаку $\text{NZD}(a(X), b(X))$ за моничан полином који је највећи заједнички делилац полинома $a(X)$ и $b(X)$.

Следећа лема је једноставна и корисна.

Лема I.6 Ако је $a_1(X) = q(X)a_2(X) + a_3(X)$ за неке ненула полиноме $a_1(X)$, $a_2(X)$ и $a_3(X)$, онда је $\text{NZD}(a_1(X), a_2(X)) = \text{NZD}(a_2(X), a_3(X))$.

Доказ. Довољно је показати да је скуп свих делилаца полинома $a_1(X)$ и $a_2(X)$ једнак скупу свих делилаца полинома $a_2(X)$ и $a_3(X)$. Но, то је јасно: ако $b(X) | a_1(X)$ и $b(X) | a_2(X)$, онда $b(X) | (a_1(X) - q(X)a_2(X))$, тј. $b(X) | a_3(X)$. Слично, ако $b(X) | a_2(X)$ и $b(X) | a_3(X)$, онда важи и $b(X) | (q(X)a_2(X) + a_3(X))$, тј. $b(X) | a_1(X)$. \square

Наведимо сада добро познати Еуклидов алгоритам за налажење $\text{NZD}(a(X), b(X))$. Он уједно и показује да за свака два ненула полинома постоји највећи заједнички делилац.

$$a(X) = q(X)b(X) + r(X), \quad 0 \leq \deg(r(X)) < \deg(b(X))$$

$$b(X) = q_1(X)r(X) + r_1(X), \quad 0 \leq \deg(r_1(X)) < \deg(r(X))$$

$$r(X) = q_2(X)r_1(X) + r_2(X), \quad 0 \leq \deg(r_2(X)) < \deg(r_1(X))$$

⋮

$$r_{n-2}(X) = q_n(X)r_{n-1}(X) + r_n(X), \quad 0 \leq \deg(r_n(X)) < \deg(r_{n-1}(X))$$

$$r_{n-1}(X) = q_{n+1}(X)r_n(X).$$

Дакле, $r_n(X)$ је последњи ненула остатак. Вишеструком применом прстходног леме добијамо

$$\text{NZD}(a(X), b(X)) = \text{NZD}(b(X), r(X)) = \cdots = \text{NZD}(r_{n-1}(X), r_n(X)).$$

Но, како $r_n(X) | r_{n-1}(X)$, закључујемо да је $r_n(X)$ највећи заједнички делилац полинома $a(X)$ и $b(X)$, тј. је

$$\text{NZD}(a(X), b(X)) = c^{-1}r_n(X),$$

где је c водећи коефицијент полинома $r_n(X)$. (Рекли смо да ћемо бирати моничан полином, те се стога појављује дељење водећим коефицијентом полинома $r_n(X)$.)

Из наведених једнакости добијамо:

$$\begin{aligned} r_n(X) &= r_{n-2}(X) - q_n(X)r_{n-1}(X) \\ &= r_{n-2}(X) - q_n(X)(r_{n-3}(X) - q_{n-1}(X)r_{n-2}(X)) \\ &= (-q_n(X))r_{n-3}(X) + (1 + q_n(X)q_{n-1}(X))r_{n-2}(X). \end{aligned}$$

„Пењањем” уз тај систем једнакости добијамо да постоје полиноми $u_1(X)$ и $v_1(X)$ такви да је $r_n(X) = u_1(X)a(X) + v_1(X)b(X)$. Дељењем водећим коефицијентом полинома $r_n(X)$ добијамо следећи резултат.

Теорема I.7 Нека је K поље. За свака два полинома $a(X), b(X) \in K[X] \setminus \{0\}$ постоје $u(X), v(X) \in K[X]$ такви да је

$$u(X)a(X) + v(X)b(X) = \text{NZD}(a(X), b(X)).$$

Додатак II

Ред производа елемената

У овом делу показаћемо да за свака три природна броја m, n, r који су сви већи од 1, постоји група G и елементи a и b из G такви да је $\omega(a) = m$, $\omega(b) = n$ и $\omega(ab) = r$.

Пођимо од групе $SL_2(\mathbb{C})$:

$$SL_2(\mathbb{C}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{C}, ad - bc = 1 \right\}.$$

Докажимо најпре да је $-I$ једини елемент ове групе који је реда 2 (овдес I означава јединичну матрицу). Наиме, уколико је $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ реда 2, онда је

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \begin{bmatrix} a & b \\ c & d \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

те добијамо

$$a^2 + bc = 1, \quad ab + bd = 0, \quad ca + dc = 0, \quad cb + d^2 = 1. \quad (\text{II.1})$$

Претпоставимо да је $a + d = 0$. Тада из једнакости $ad - bc = 1$ добијамо $a^2 + bc = -1$, што противречи првој једнакости у (II.1). Дакле, $a + d \neq 0$ и из друге и треће једнакости у (II.1) добијамо $b = c = 0$. Следи да је $a^2 = d^2 = 1$ и $ad = 1$. Према томе $a = d \in \{-1, 1\}$. С обзиром да је A реда 2, дакле, $A \neq I$, добијамо да је $A = -I$, што смо и желели да докажемо.

Иска су сада u, v, w елементи из $\mathbb{C} \setminus \{0\}$ редова $2m, 2n, 2r$. Посматрајмо матрице

$$A = \begin{bmatrix} u & 1 \\ 0 & u^{-1} \end{bmatrix}, \quad B = \begin{bmatrix} v & 0 \\ t & v^{-1} \end{bmatrix},$$

где је $t = w + w^{-1} - uv - u^{-1}v^{-1}$. Покажимо најпре да је $\omega(A) = 2m$. Рачунајмо првих неколико степена матрице A :

$$\begin{aligned} A^2 &= \begin{bmatrix} u^2 & u + u^{-1} \\ 0 & u^{-2} \end{bmatrix}, \\ A^3 &= \begin{bmatrix} u^3 & u^2 + 1 + u^{-2} \\ 0 & u^{-3} \end{bmatrix}, \\ A^4 &= \begin{bmatrix} u^4 & u^3 + u + u^{-1} + u^{-3} \\ 0 & u^{-4} \end{bmatrix}. \end{aligned}$$

Може се приметити правилност. Препоручујемо читаоцу да индукцијом докаже да је

$$A^{2k} = \begin{bmatrix} u^{2k} & u^{2k-1} + u^{2k-3} + \cdots + u + u^{-1} + \cdots + u^{-(2k-3)} + u^{-(2k-1)} \\ 0 & u^{-2k} \end{bmatrix}$$

и

$$A^{2k+1} = \begin{bmatrix} u^{2k+1} & u^{2k} + \cdots + u^2 + 1 + u^2 + \cdots + u^{-(2k)} \\ 0 & u^{-(2k+1)} \end{bmatrix}$$

Како је ред слемента u једнак $2m$, то је $u^s \neq 1$ за $1 \leq s < 2m$, а $u^{2m} = u^{-2m} = 1$. Но, из чињенице да је $u^{2m} = 1$ добијамо да је

$$u^{-1} = u^{2m-1}, \quad u^{-3} = u^{2m-3}, \dots, \quad u^{-(2m-1)} = u.$$

Стога је $u^{2m-1} + u^{2m-3} + \cdots + u + u^{-1} + \cdots + u^{-(2m-3)} + u^{-(2m-1)}$ једнако

$$2(u^{2m-1} + u^{2m-3} + \cdots + u) = 2u(u^{2m-2} + u^{2m-4} + \cdots + 1).$$

Но, из $0 = u^{2m} - 1 = (u^2 - 1)(u^{2m-2} + u^{2m-4} + \cdots + 1)$ и чињенице да $u^2 \neq 1$, добијамо да је $u^{2m-2} + \cdots + 1 = 0$, те је $A^{2m} = I$. Како је $A^k \neq I$ за $1 \leq k < 2m$, добили смо да је $\omega(A) = 2m$.

На врло сличан, готово идентичан начин, може се показати да је $\omega(B) = 2n$. Број t који се појављује не утиче на резултат у шта се можете уверити директним рачуном. Свакако препоручујемо да овај доказ изведете.

Израчунајмо сада AB :

$$AB = \begin{bmatrix} uv + t & v^{-1} \\ u^{-1}t & u^{-1}v^{-1} \end{bmatrix} = \begin{bmatrix} w + w^{-1} - u^{-1}v^{-1} & v^{-1} \\ u^{-1}t & u^{-1}v^{-1} \end{bmatrix}.$$

Ово је знатно сложенија матрица од претходних. Но, покушајмо да јој нађемо сличну матрицу која је једноставнија. Подсетимо се да су матрице C и D сличне уколико постоји инвертибилна матрица S таква да је $SCS^{-1} = D$. У групи $SL_2(\mathbb{C})$ сличне матрице су заправо конјуговани слементи и зnamо да они имају исти ред.

Приметимо да уколико првој колони додамо другу колону помножену са u^{-1} поједностављујемо члан на позицији $(1, 1)$. Знамо да се

трансформације на колонама постижу множењем здесна одговарајућим елементарним матрицама. Но, морамо да пазимо – не тражимо еквивалентну, него сличну матрицу. То значи да ако нашу матрицу здесна помножимо неком инвертибилном матрицом, морамо је и слева помножити инверзом те матрице. Рачунамо:

$$\begin{bmatrix} 1 & 0 \\ -u^{-1} & 1 \end{bmatrix} \begin{bmatrix} w + w^{-1} - u^{-1}v^{-1} & v^{-1} \\ u^{-1}t & u^{-1}v^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ u^{-1} & 1 \end{bmatrix} = \begin{bmatrix} w + w^{-1} & v^{-1} \\ -v & 0 \end{bmatrix}.$$

Имали смо среће – заиста је добијена једноставнија матрица. Она је истог реда као и почетна. Елимиништимо још и w^{-1} на позицији (1, 1):

$$\begin{bmatrix} 1 & w^{-1}v^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} w + w^{-1} & v^{-1} \\ -v & 0 \end{bmatrix} \begin{bmatrix} 1 & -w^{-1}v^{-1} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} w & 0 \\ -v & w^{-1} \end{bmatrix}.$$

Последња матрица је облика као и раније. Знамо сада да је њен ред $2r$ (ред комплексног броја w је $2r$), а како је она слична матрици AB , закључујемо да је $\omega(AB) = 2r$.

Скоро смо завршили, добили смо да у $SL_2(\mathbb{C})$ постоје елементи A и B реда $2m$ и $2n$ (редом), при чему је елемент AB реда $2r$. Остаје да искако ‘скратимо’ ту двојку.

Посматрајмо подгрупу у $SL_2(\mathbb{C})$ генерисану елементом реда 2, тј. подгрупу $\langle -I \rangle$. Јасно је да је $X(-I) = -X = (-I)X$ за све $X \in SL_2(\mathbb{C})$, тј. је $\langle -I \rangle \triangleleft SL_2(\mathbb{C})$. Иска је G количничка група: $G = SL_2(\mathbb{C})/\langle -I \rangle$. Уочимо елементе $a = A\langle -I \rangle$ и $b = B\langle -I \rangle$ у овој групи. Како је A реда $2m$ у $SL_2(\mathbb{C})$, то је A^m реда 2, а једини елемент реда 2 у $SL_2(\mathbb{C})$ је $-I$. Слично и за матрицу B . Закључујемо да је $\omega(a) = m$, $\omega(b) = n$, док је наравно и $\omega(ab) = r$. Тиме смо нашли тражени пример.

Напомена. Уколико бисмо искористили више знања Линеарне алгебре, до резултата бисмо дошли брже. Наиме, карактерични полином матрице A је $\chi_A(\lambda) = (\lambda - u)(\lambda - u^{-1})$. С обзиром да је $u \neq u^{-1}$, добијамо не само да је то минималан полином, него и да је минималан полином производ РАЗЛИЧИТИХ линсарних фактора, што значи да је матрица слична дијагоналној матрици $\begin{bmatrix} u & 0 \\ 0 & u^{-1} \end{bmatrix}$. Како је ред комплексног броја u једнак $2m$, то је и ред ове матрице једнак $2m$. Слично је и матрица B слична матрици $\begin{bmatrix} v & 0 \\ 0 & v^{-1} \end{bmatrix}$, те је њен ред $2n$. Коначно,

$$\begin{aligned} \chi_{AB}(\lambda) &= (uv + t - \lambda)(u^{-1}v^{-1} - \lambda) - u^{-1}v^{-1}t = \lambda^2 - (uv + t + u^{-1}v^{-1})\lambda + 1 \\ &= \lambda^2 - (w + w^{-1})\lambda + 1 = (\lambda - w)(\lambda - w^{-1}). \end{aligned}$$

Дакле, матрица AB је слична матрици $\begin{bmatrix} w & 0 \\ 0 & w^{-1} \end{bmatrix}$, тј. је реда $2r$. Овако видимо и зашто је t изабрано на наведени начин.

Додатак III

Структура групе $U(\mathbb{Z}_{p^n})$

У овом делу доказаћемо следеће:

$$U(\mathbb{Z}_{p^n}) \cong \begin{cases} \mathbb{C}_{p^{n-1}(p-1)}, & p \text{ је непаран прост број, } n \geq 2 \\ \mathbb{C}_2 \times \mathbb{C}_{2^{n-2}}, & p = 2, n \geq 3, \\ \mathbb{C}_2, & p = 2, n = 2. \end{cases}$$

Утврдимо најпре структуру групе $U(\mathbb{Z}_{2^n})$ за $n \geq 3$. Посматрајмо подгрупе H и K ове групе: $H = \langle -1 \rangle$, $K = \langle 5 \rangle$. Група H је наравно циклична група реда 2, тј је $H \cong \mathbb{C}_2$. Покажимо да је K циклична група реда 2^{n-2} . У ту сврху, докажимо индукцијом по k да је:

$$5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}. \quad (\text{III.1})$$

Уколико је $k = 1$ имамо да је

$$5^2 = (1 + 4)^2 = 1 + 8 + 16 \equiv 1 + 2^3 \pmod{2^4}.$$

Претпоставимо да је тврђење тачно за k , докажимо га за $k+1$. Имамо:

$$\begin{aligned} 5^{2^{k+1}} &= \left(5^{2^k}\right)^2 = (1 + 2^{k+2} + 2^{k+3}y)^2, \text{ за неко } y \text{ по индуктивној хипотези} \\ &= 1 + 2^{k+3} + 2^{k+4}y + (2^{k+2} + 2^{k+3}y)^2 \\ &= 1 + 2^{k+3} + 2^{k+4}(y + 2^k(1 + 2y)^2) \\ &\equiv 1 + 2^{k+3} \pmod{2^{k+4}}. \end{aligned}$$

Као специјалне случајеве од (III.1), добијамо

$$5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n}, \quad 5^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+1}} \equiv 1 \pmod{2^n}.$$

Дакле, у групи $U(\mathbb{Z}_{2^n})$ је $5^{2^{n-3}} \neq 1$, а $5^{2^{n-2}} = 1$. Следи $\omega(5) \mid 2^{n-2}$ и $\omega(5) \nmid 2^{n-3}$, па је ред елемента 5 једнак 2^{n-2} . Приметимо да $5^{2^{n-3}} \neq -1$ у овој групи, јер бисмо у том случају имали да је

$$-1 \equiv 1 + 2^{n-1} \pmod{2^n},$$

тј би $2^n \mid (2^{n-1} + 2)$, што свакако није тачно за $n \geq 3$. Дакле, добили смо да је K циклична подгрупа реда 2^{n-2} и да је $H \cap K = \{1\}$. Закључујемо да је $HK \cong \mathbb{C}_2 \times \mathbb{C}_{2^{n-2}}$. С обзиром да је $|U(\mathbb{Z}_{2^n})| = \phi(2^n) = 2^{n-1}$, то је $HK = U(\mathbb{Z}_{2^n})$ и добили смо тражени резултат.

Позабавимо се сада случајем испарног простог броја p . Иска је H подгрупа групе $U(\mathbb{Z}_{p^n})$ генерисана елементом $1 + p$. Показаћемо да је ред овог елемента p^{n-1} , те је $H \cong \mathbb{C}_{p^{n-1}}$.

Докажимо индукцијом по k да је:

$$(1 + p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}. \quad (\text{III.2})$$

За $k = 1$ имамо:

$$(1 + p)^p = 1 + p^2 + \sum_{i=2}^p \binom{p}{i} p^i.$$

Но, знамо да $p \mid \binom{p}{i}$ за све $1 < i < p$, тј $p^3 \mid \binom{p}{i} p^i$ за све $2 \leq i < p$, док је јасно да је p^p дељиво са p^3 , јер је $p \geq 3$. Стога је та сума дељива са p^3 те је заиста

$$(1 + p)^p \equiv 1 + p^2 \pmod{p^3}.$$

Претпоставимо да је тврђење тачно за k , докажимо га за $k + 1$. Имамо:

$$\begin{aligned} (1 + p)^{p^{k+1}} &= \left((1 + p)^{p^k} \right)^p = (1 + p^{k+1} + p^{k+2}y)^p, \text{ за неко } y \text{ по ИХ} \\ &= 1 + p^{k+2} + p^{k+3}y + \sum_{i=2}^p \binom{p}{i} (p^{k+1} + p^{k+2}y)^i. \end{aligned}$$

Како је за $i \geq 2$: $i(k+1) \geq 2(k+1) = 2k+2 \geq k+3$, за све $k \geq 1$, то имамо да $p^{k+3} \mid (p^{k+1} + p^{k+2}y)^i$ за све $i \geq 2$, тј заправо p^{k+3} дели целу ту пресосталу суму. Добијамо да је

$$(1 + p)^{p^{k+1}} = 1 + p^{k+2} + p^{k+3}z,$$

за неко z , те је заиста

$$(1 + p)^{p^{k+1}} \equiv 1 + p^{k+2} \pmod{p^{k+3}}.$$

За $k = n - 1$ и $k = n - 2$ у (III.2) добијамо:

$$(1 + p)^{p^{n-1}} \equiv 1 + p^n \pmod{p^{n+1}} \equiv 1 \pmod{p^n}, \quad (1 + p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n}.$$

Ово нам даје да $\omega(1 + p) \mid p^{n-1}$ и $\omega(1 + p) \nmid p^{n-2}$, те је $\omega(1 + p) = p^{n-1}$ у групи $U(\mathbb{Z}_{p^n})$.

Сада ћемо потражити елемент реда $p - 1$ у групи $U(\mathbb{Z}_{p^n})$. Иска је $g \in U(\mathbb{Z}_p)$ примитиван корен модуло p . Посматрамо елемент

$$a = g^{p^{n-1}} \in U(\mathbb{Z}_{p^n}).$$

Јасно је да је

$$a^{p-1} = \left(g^{p^{r-1}}\right)^{p-1} = g^{p^{r-1}(p-1)} = 1 \quad (\text{III.3})$$

у тој групи. Како је NZD($p^{r-1}, p-1$) = 1, то је

$$\omega(a) = \omega(g^{p^{r-1}}) = \omega(g) = p-1 \quad (\text{III.4})$$

у групи $U(\mathbb{Z}_p)$.

Покажимо да је елемент a баш реда $p-1$. Наиме, претпоставимо да је његов ред неки k . Тада $k \mid (p-1)$ на основу (III.3) и претпоставимо да је $k < p-1$. То значи да је

$$1 = a^k = \left(g^{p^{r-1}}\right)^k$$

у $U(\mathbb{Z}_{p^n})$, тј.

$$p^n \mid \left(g^{p^{r-1}}\right)^k - 1.$$

Но, тада следи да и

$$p \mid \left(g^{p^{r-1}}\right)^k - 1,$$

те је

$$\left(g^{p^{r-1}}\right)^k = 1$$

у $U(\mathbb{Z}_p)$, што противречи (III.4). Дакле, $\omega(a) = p-1$. С обзиром да је $\omega(1+p) = p^{n-1}$ и да су p^{n-1} и $p-1$ узајамно прости, уз чињеницу да је група $U(\mathbb{Z}_{p^n})$ комутативна, добијамо да је $\omega((1+p)a) = p^{n-1}(p-1) = \varphi(p^n) = |U(\mathbb{Z}_{p^n})|$. Дакле, заиста је $U(\mathbb{Z}_{p^n}) \cong \mathbb{C}_{p^{n-1}(p-1)}$.

Конечно, како је $\varphi(2^2) = 2$, то је јасно да је $U(\mathbb{Z}_{2^2}) \cong \mathbb{C}_2$.

Додатак IV

Групне релације

У овом делу ћемо приказати један занимљив метод за установљавање постојања изоморфизама. Докази се спроводе на сличан начин као и ранији, тако да ћемо их оставити амбициознијим читаоцима за вежбу.

Наведимо најпре дефиницију.

Дефиниција IV.1 Нека су G и H групе. Под ГРУПНОМ РЕЛАЦИЈОМ Φ са G у H подразумевамо сваку подгрупу групе $G \times H$. Уколико је $\Phi \leq G \times H$, дефинишемо

1. $\text{Dom}(\Phi) := \{g \in G : (\exists h \in H)(g, h) \in \Phi\}$ (ДОМЕН);
2. $\text{Im}(\Phi) := \{h \in H : (\exists g \in G)(g, h) \in \Phi\}$ (СЛИКУ);
3. $\text{Ker}(\Phi) := \{g \in G : (g, \varepsilon) \in \Phi\}$ (ЈЕЗГРО);
4. $\text{Def}(\Phi) := \{h \in H : (e, h) \in \Phi\}$ (ДЕФЕКТ).

Са e , односно ε означени су одговарајући неутрали. Тада важи следећа основна теорема. Она је генерализација прве теореме о изоморфизму за групе и доказује се на стандардан начин.

Теорема IV.2 Важи следеће:

1. $\text{Ker}(\Phi) \triangleleft \text{Dom}(\Phi) \leq G$;
2. $\text{Def}(\Phi) \triangleleft \text{Im}(\Phi) \leq H$;
3. $\text{Dom}(\Phi)/\text{Ker}(\Phi) \cong \text{Im}(\Phi)/\text{Def}(\Phi)$.

Последица IV.3 (Друга теорема о изоморфизму за групе) Нека је G група, $H \leq G$ и $K \triangleleft G$. Тада је:

1. $H \cap K \triangleleft H$;
2. $H/H \cap K \cong HK/K$.

Доказ. Посматра се групна релација

$$\Phi = \{(h, hk) : h \in H, k \in K\} \leqslant G \times G.$$

Тврђење тада директно следи из теореме IV.2. \square

Последица IV.4 (Трећа теорема о изоморфизму за групе) Нека је G група, $H \triangleleft G$, $K \triangleleft G$ и $K \subseteq H$. Тада је:

1. $H/K \triangleleft G/K$;
2. $(G/K)/(H/K) \cong G/H$.

Доказ. Посматра се групна релација

$$\Phi = \{(gH, gK) : g \in G\} \leqslant G/H \times G/K.$$

Тврђење тада директно следи из теореме IV.2. \square

Последица IV.5 (Уопштење друге теореме о изоморфизму за групе) Нека је G група, $H \leqslant G$, $K \triangleleft G$ и $N \triangleleft G$. Тада је:

1. $(H \cap N)K \triangleleft HK$;
2. $(H \cap K)N \triangleleft HN$;
3. $HK/(H \cap N)K \cong HN/(H \cap K)N$.

Доказ. Посматра се групна релација

$$\Phi = \{(hk, hn) : h \in H, n \in N, k \in K\} \leqslant G \times G.$$

Тврђење тада директно следи из теореме IV.2. \square

Последица IV.6 (Лема о лептиру) Нека је G група, $U, V \leqslant G$, $u \triangleleft U$, $v \triangleleft V$. Тада је:

1. $u(U \cap v) \triangleleft u(U \cap V)$;
2. $(u \cap V)v \triangleleft (U \cap V)v$;
3. $u(U \cap V)/u(U \cap v) \cong (U \cap V)v/(u \cap V)v$.

Доказ. Посматра се групна релација

$$\Phi = \{(gx, gy) : g \in U \cap V, x \in u, y \in v\} \leqslant U \times V.$$

Тврђење тада директно следи из теореме IV.2. \square

Наравно у свим овим релацијама треба проверити да ли су то заиста подгрупе одговарајућег производа и идентификовати домен, слику, језгро и дефект.

Последица IV.7 Посматрајмо групе $(\mathbb{R}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{C} \setminus \{0\}, \cdot)$, (S, \cdot) , где је са S означен скуп свих комплексних бројева модула 1 и (U, \cdot) , где је са U означен скуп свих корена из јединице:

$$U := \{z \in \mathbb{C} : (\exists n \geq 2) z^n = 1\}.$$

Тада је:

1. $\mathbb{R}/\mathbb{Z} \cong S$;
2. $\mathbb{Q}/\mathbb{Z} \cong U$.

Доказ. Посматрањем групних релација

$$\{(\theta, \cos 2\pi\theta + i \sin 2\pi\theta) : \theta \in \mathbb{R}\} \leqslant \mathbb{R} \times (\mathbb{C} \setminus \{0\})$$

и

$$\{(\theta, \cos 2\pi\theta + i \sin 2\pi\theta) : \theta \in \mathbb{Q}\} \leqslant \mathbb{R} \times (\mathbb{C} \setminus \{0\}),$$

тврђења следе на основу теореме IV.2. \square

Наравно, ово смо могли да докажемо и на стандардан начин (погледати задатак 1.107), али је занимљиво видети како метод групних релација даје тај доказ на природан начин.

За крај један забаван пример.

Пример IV.8 Нека је A Абелова група. Посматрајмо групну релацију

$$\Phi = \{(x, y) \in A \times A : 2x - 3y = 0\} \leqslant A \times A.$$

Добијамо изоморфизам:

$$3A / \{x \in A : 2x = 0\} \cong 2A / \{x \in A : 3x = 0\}.$$

Јасно је да ће језгро састоји од слесната реда 2 и нуле, а дефект од елемената реда 3 и нуле. Мало је сложеније показати да је домен заправо $3A$, а слика $2A$. Тако добијамо тражени резултат.