

АЛГЕБРА 2

ДОДАТНО О ПРСТЕНИМА И ПОЉИМА

ЗОРАН ПЕТРОВИЋ

Кинеска теорема о остацима

Сви прстени са којима радимо су комутативни прстени са јединицом, а $\subset$ означава релацију „бити прави подскуп”.

У произвољном комутативном прстену са јединицом могуће је формулисати и доказати основну Кинеску теорему о остацима. Најпре нам је потребна једна дефиниција.

Дефиниција 1. Идеали I и J комутативног прстена са јединицом A су копрости (или узајамно прости) уколико је $I + J = A$. 🙌

Приметимо да су у $\mathbb{Z}$ идеали $\langle m \rangle$ и $\langle n \rangle$ копрости акко су m и n узајамно прости – отуд и терминологија.

Став 2. Ако су I и J копрости, онда је $I \cdot J = I \cap J$.

🙌 Знамо да је $I \cdot J \subseteq I \cap J$. Докажимо да важи и обратно укључење. Претпоставимо да $z \in I \cap J$. Како је $I + J = A$, то постоје $x \in I$, $y \in J$ тако да је $x + y = 1$. Имамо да је $z = zx + zy$. Како $z \in I \cap J \subseteq J$, $x \in I$, имамо да $zx = xz \in I \cdot J$. Слично, из $z \in I$ добијамо да $zy \in I \cdot J$. Стога и $z = xz + yz \in I \cdot J$. 📖

Лема 3. Ако су I и J копрости, а такође и I и K копрости, онда су и I и $J \cdot K$ копрости.

🙌 Пошто су I и J копрости постоје $x_1 \in I$, $y \in J$ тако да је $x_1 + y = 1$. Како су и I и K копрости, постоје $x_2 \in I$, $z \in K$ тако да је $x_2 + z = 1$. Стога је

$$1 = (x_1 + y) \cdot (x_2 + z) = \underbrace{(x_1x_2 + x_1z + yx_2)}_{\in I} + \underbrace{yz}_{\in J \cdot K} \in I + J \cdot K,$$

па је $I + J \cdot K = A$, тј. I и $J \cdot K$ су копрости. 📖

Теорема 4. (Кинеска теорема о остацима) Нека су $I_1, \dots, I_n \triangleleft A$ пар по пар копрости. Тада важи изоморфизам:

$$A/(I_1 \cap \dots \cap I_n) \cong A/I_1 \times \dots \times A/I_n.$$

👉 Посматрамо хомоморфизам $f: A \rightarrow A/I_1 \times \cdots \times A/I_n$ дефинисан са

$$f(x) = (x + I_1, \dots, x + I_n).$$

Лако се проверава да је ово један хомоморфизам прстена. Имамо да

$$x \in \text{Ker } f \text{ акко } (x + I_1, \dots, x + I_n) = (I_1, \dots, I_n) \text{ акко } x \in I_1, \dots, x \in I_n,$$

те је $\text{Ker } f = I_1 \cap \cdots \cap I_n$. Докажимо да је f „на”. Из претпоставке и леме 3 индукцијом добијамо да су идеали I_i и $\prod_{j \neq i} I_j$ копости за све $i = \overline{1, n}$. Дакле, за све те i , постоје $a_i \in I_i$, $b_i \in \prod_{j \neq i} I_j$ тако да је $a_i + b_i = 1$. То посебно значи да је $b_i \equiv 1 \pmod{I_i}$ и $b_i \equiv 0 \pmod{I_j}$ за све $j \neq i$. Нека је $(x_1 + I_1, \dots, x_n + I_n)$ произвољан елемент из $A/I_1 \times \cdots \times A/I_n$. Уочимо елемент $x = \sum_{j=1}^n b_j x_j$. Тада је, за све $i = \overline{1, n}$:

$$x \equiv_{I_i} 0 \cdot x_1 + \cdots + 1 \cdot x_i + \cdots + 0 \cdot x_n \equiv_{I_i} x_i.$$

Стога је $f(x) = (x_1 + I_1, \dots, x_n + I_n)$ и f је „на”. Теорема о изоморфизму за прстене завршава доказ. 

Прости и максимални идеали

Започнимо овај одељак следећим ставом.

Став 5. Нека је A комутативан прстен са јединицом и $P \triangleleft A$ ($P \neq A$). Следећи услови су еквивалентни.

- (1) За $I, J \triangleleft A$ важи: ако је $I \cdot J \subseteq P$, онда $I \subseteq P$ или $J \subseteq P$.
- (2) За $a, b \in A$ важи: ако $ab \in P$, онда $a \in P$ или $b \in P$.
- (3) Прстен A/P је домен.

👉 (1) $\implies$ (2). Посматрамо идеале $I = \langle a \rangle$, $J = \langle b \rangle$. Из претпоставке да $ab \in P$ и чињенице да је P идеал, следи да је $I \cdot J \subseteq P$. На основу (1) добијамо да је $I \subseteq P$, посебно: $a \in P$, или да је $J \subseteq P$, посебно: $b \in P$.

(2) $\implies$ (3). Нека је $(a + P) \cdot (b + P) = 0_{R/P} = P$. То даје $ab \in P$. Из (2) добијамо да $a \in P$, те је $a + P = P = 0_{R/P}$ или $b \in P$, те је $b + P = P = 0_{R/P}$. Дакле, R/P је домен, јер не садржи праве делитеље нуле.

(3) $\implies$ (1). Претпоставимо да је $I \cdot J \subseteq P$, $I \not\subseteq P$, $J \not\subseteq P$. Нека је $a \in I \setminus P$, $b \in J \setminus P$. Тада $ab \in I \cdot J \subseteq P$, те је $(a + P) \cdot (b + P) = ab + P = P = 0_{R/P}$. Но, то није могуће, јер је, по претпоставци A/P домен, а $a + P \neq P = 0_{R/P}$, јер $a \notin P$ и $b + P \neq P = 0_{R/P}$, јер $b \notin P$. 

Дефиниција 6. За идеал $P \triangleleft A$ кажемо да је **прост** уколико испуњава неко (а тиме и сва) од претходна три еквивалентна својства. 👉

Уколико је P прост идеал, а $a_1, \dots, a_n \in A$, онда из $a_1 \cdots a_n \in P$ следи да $a_i \in P$ за неко $i \in \{1, \dots, n\}$ и то се (лако) доказује индукцијом по n .

У основној школи смо се упознали са појмом простих бројева и тамо су они били дефинисани као бројеви који немају других делилаца сем 1 и самих себе (при чему смо се збуњивали питањем да ли је 1 прост број 😊). Но, у

домену разликујемо појам простог и нерастављивог елемента. А ту свакако не спадају инвертибилни елементи прстена.

Дефиниција 7. Нека је A домен. Елемент $a \in A \setminus (U(A) \cup \{0\})$ је

- **прост** уколико за $a, b \in A$ важи: ако $p \mid ab$, онда $p \mid a$ или $p \mid b$;
- **нерастављив** или **атом** уколико за $a, b \in A$ важи: ако је $p = ab$, онда је $a \in U(A)$ или је $b \in U(A)$.

Веза ипак постоји.

Став 8. Сваки прост елемент домена је атом.

👉 Нека је $p \in A$ прост елемент и нека је $p = ab$. То свакако повлачи да $p \mid ab$. Како је он прост, добијамо $p \mid a$ или $p \mid b$. Уколико $p \mid a$, имамо да је $a = pa_1$, за неки $a_1 \in A$. Стога је $p = ab = pa_1b$, па како је A домен сваки елемент сем 0 је регуларан, па је $1 = a_1b$ и закључујемо да $b \in U(A)$. На потпуно аналоган начин, из претпоставке $p \mid b$ добијамо да $a \in U(A)$. Дакле, p је атом. 📌

У произвољном домену имамо атоме који нису прости.

Пример 9. У прстену $\mathbb{Z}[\sqrt{-5}]$ елемент 3 је атом, али није прост.

Најпре је $\mathbb{Z}[\sqrt{-5}] = \{p(\sqrt{-5}) : p(X) \in \mathbb{Z}[X]\} = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}$. Дефинишемо норму елемента $z \in \mathbb{Z}[\sqrt{-5}]$ са: $N(z) := z\bar{z}$. Основна својства комплексних бројева нам кажу да је $N(zu) = N(z)N(u)$ за све z, u . Претпоставимо да је $3 = (p + q\sqrt{-5}) \cdot (r + s\sqrt{-5})$, за неке $p, q, r, s \in \mathbb{Z}$. Тада је $N(3) = N(p + q\sqrt{-5})N(r + s\sqrt{-5})$. Добијамо да је $9 = (p^2 + 5q^2)(r^2 + 5s^2)$. Уколико би и q и s били различити од 0, са десне стране једнакости бисмо добили број који није мањи од 10. Стога је бар један од њих једнак 0. Нека је то q . Добијамо $3^2 = p^2(r^2 + 5s^2)$. Уколико је $p \neq \pm 1$ добијамо да мора бити $p \in \{-3, 3\}$, те је $1 = r^2 + 5s^2$, што нам даје $r \in \{-1, 1\}$, $s = 0$, тј. $r + s\sqrt{-5} \in \{1, -1\}$, те је $r + s\sqrt{-5}$ инвертибилан. А, уколико је $p \in \{-1, 1\}$, добијамо да је $p + q\sqrt{-5} \in \{-1, 1\}$, дакле инвертибилан. На сличан начин, из почетне претпоставке $s = 0$, добили бисмо да је један од ова два фактора инвертибилан, те је 3 атом.

Да бисмо показали да он није прост, приметимо да $3 \mid 9$, тј.

$$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Ако би 3 био прост, то би значило да дели неки од ова два фактора. Нека, на пример, $3 \mid (2 + \sqrt{-5})$. То значи да је $2 + \sqrt{-5} = 3 \cdot (p + q\sqrt{-5})$ за неке $p, q \in \mathbb{Z}$. Налажењем норми добијамо да је $9 = 9 \cdot (p^2 + 5q^2)$, те је $p^2 + 5q^2 = 1$ и добијамо да $p + q\sqrt{-5} \in \{-1, 1\}$, те је стога $2 + \sqrt{-5} \in \{-3, 3\}$, што свакако није тачно. Стога 3 није прост. 👍

Напомена. Приметимо да једнакост $3 \cdot 3 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5})$ даје две различите факторизације 9 у облику производа атома. То је директно повезано са чињеницом да нису сви атоми уједно и прости.

Пример 10. Нека је A прстен тригонометријских полинома, тј. нека је $A = \mathbb{R}[c, s]$ где су $c, s: \mathbb{R} \rightarrow \mathbb{R}$, функције задате са: $c(x) = \cos x$, $s(x) = \sin x$. Из добро нам познатог идентитета $\sin^2 x + \cos^2 x = 1$, следи:

$$s \cdot s = (1 - c) \cdot (1 + c).$$

Остављамо читаоцима да покажу да су функције s и $1 - c$ атоми у овом прстену, као вежбу из Анализе 😊

Следећи став је помало и очекиван.

Став 11. *Елемент у домену је прост ако је идеал њим генерисан прост идеал.*

👉 Нека је $p \in A$. На основу става 5, део под (2), имамо:

$\langle p \rangle$ је прост идеал ако $(\forall a \in A)(\forall b \in A) (a \cdot b \in \langle p \rangle \Rightarrow a \in \langle p \rangle \text{ или } b \in \langle p \rangle)$
 ако $(\forall a \in A)(\forall b \in A) (p \mid a \cdot b \Rightarrow p \mid a \text{ или } p \mid b)$

ако p је прост елемент. 📌

Пређимо сада на појам максималног идеала.

Дефиниција 12. *Прави идеал M прстена A је максималан, ако не постоји $I \triangleleft A$ такав да је $M \subset I \subset A$.*

Став 13. *Прави идеал M прстена A је максималан идеал ако је A/M поље.*

👉 $\Rightarrow$. Претпоставимо да је M максималан идеал и нека је $a + M \neq 0_{A/M}$. То значи да $a \notin M$, па је $M \subset M + \langle a \rangle$. Из претпоставке о максималности M следи да је $M + \langle a \rangle = A$, те постоје $x \in M$, $r \in A$, тако да је $x + ra = 1$. Преласком на количнички прстен добијамо једнакост:

$$(x + M) + (r + M) \cdot (a + M) = 1 + M = 1_{A/M}$$

Но, како је $x \in M$, имамо да је $x + M = M = 0_{A/M}$ и добијамо

$$(r + M) \cdot (a + M) = 1_{A/M},$$

те је $a + M$ инвертибилан у A/M .

$\Leftarrow$. Нека је $M \subset I \triangleleft A$. Желимо да покажемо да је $I = A$. У ту сврху, нека је $a \in I \setminus M$. По претпоставци је A/M поље, па како је $a + M \neq M = 0_{A/M}$, постоји $b + M$ тако да је $(a + M) \cdot (b + M) = 1_{A/M} = 1 + M$. Одавде добијамо да је $ab - 1 \in M$, па је $1 = ab - x$, за неки $x \in M$. Но, $ab = ba \in I$, па како је и $x \in M \subset I$, добијамо $1 = ab - x \in I$, те, како идеал I садржи 1_A , мора бити $I = A$, што се и тражило. 📌

Напомена. Видимо да из овог става следи да је сваки максималан идеал прост, јер у пољу нема правих делитеља нуле.

Веза између атома и максималних идеала дата је следећим ставом.

Став 14. *Елемент $a \in A$ је атом ако је $\langle a \rangle$ максималан у скупу свих главних идеала домена A .*

☞ $\implies$. Претпоставимо да је $\langle a \rangle \subset \langle b \rangle$. То значи да је $a = bc$ за неки $c \in A$. Како је a атом, то значи да је $b \in U(A)$ или је $c \in U(A)$. Уколико $c \in U(A)$, онда је $b = ac^{-1} \in \langle a \rangle$, па је $\langle b \rangle \subseteq \langle a \rangle$ и добили бисмо да је $\langle a \rangle = \langle b \rangle$, али то по претпоставци није тачно. Закључујемо да је $b \in U(A)$, те је $\langle b \rangle = A$ и добијамо да нема правог главног идеала који садржи $\langle a \rangle$.

$\Leftarrow$. Нека је $a = bc$. То значи да је $a \in \langle b \rangle$, што нам даје $\langle a \rangle \subseteq \langle b \rangle$. Како је $\langle a \rangle$ максималан у скупу свих главних идеала прстена A , то значи да мора бити $\langle a \rangle = \langle b \rangle$ или $\langle b \rangle = A$. Уколико је $\langle b \rangle = A$, онда постоји $d \in A$ тако да је $bd = 1$, те је $b \in U(A)$. А уколико је $\langle a \rangle = \langle b \rangle$, онда је $b \in \langle a \rangle$, па постоји $e \in A$ тако да је $b = ae$. Добијамо да је $a = bc = aec$, па како је $a \neq 0$, а у домену су сви такви елементи регуларни, закључујемо да је $ec = 1$, те је $c \in U(A)$. Стога је a атом. 

Следећу теорему нећемо доказивати, само је наводимо ради комплетности.

Теорема 15. Нека је $I \triangleleft A$. Тада постоји максималан идеал $M \triangleleft A$ такав да је $I \subseteq M$. 

Факторизација

Сви прстени којима се бавимо у овом одељку су домени.

Дефиниција 16. Два елемента $a, b \in A$ су **придružена**, у ознаци $a \sim b$ уколико постоји елемент $u \in U(A)$ такав да је $a = ub$.

Јасно је да је овако дефинисана једна релација еквиваленције. Осим тога, ако је p прост (атом), онда је то и сваки њему придružени елемент.

Дефиниција 17. Домен A је **домен са једнозначном факторизацијом** уколико су испуњени следећи услови.

- (1) $(\forall a \in A \setminus (U(A) \cup \{0\})) (\exists p_1, \dots, p_r) (p_1, \dots, p_r \text{ су атоми и } a = p_1 \cdots p_r)$.
- (2) Ако су $p_1, \dots, p_r, q_1, \dots, q_s$ атоми и $p_1 \cdots p_r = q_1 \cdots q_s$, онда је $r = s$ и постоји пермутација $\sigma \in \mathbb{S}_n$ таква да $(\forall i \in \{1, \dots, r\}) (p_i \sim q_{\sigma(i)})$.

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

Став 18. Домен A је домен са једнозначном факторизацијом ако се сваки елемент из $A \setminus (U(A) \cup \{0\})$ може приказати у облику производа простих елемената.

☞ $\Leftarrow$. Покажимо најпре да је сваки атом прост. Нека је q атом. На основу претпоставке, постоје прости $p_1, \dots, p_r$ такви да је $q = p_1 \cdots p_r$. Но, q је атом те се не може представити у облику производа два елемента који су оба неинвертибилни. То значи да мора бити $r = 1$, те је q заправо прост.

По претпоставци имамо растав на производ простих, а како су прости уједно и атоми, услов (1) из горње дефиниције је испуњен. Покажимо јединственост приказа. У ту сврху нека је

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

при чему су сви ови елементи атоми. Но, на основу доказаног, они су сви прости. Радимо индукцијом по r . Ако је $r = 1$, онда је све јасно, по самој дефиницији атома. Нека је тврђење тачно за $r - 1$. Из горње једнакости и чињенице да $p_1 \mid q_1 \cdots q_s$, пошто је p_1 прост, добијамо $p_1 \mid q_j$ за неки $j \in \{1, \dots, s\}$. Но, како је q_j атом, имамо да је $q_j = u_j p_1$, за неки инвертибилан u_j . Скраћивањем са p_1 добијамо једнакост

$$p_2 \cdots p_r = u_j q_1 \cdots \widehat{q_j} \cdots q_s,$$

где „капица” изнад q_j означава да смо тај елемент изоставили. Ако је $u_j q_1 = q'_1$ добијамо једнакост

$$p_2 \cdots p_r = q'_1 \cdots \widehat{q_j} \cdots q_s.$$

Индуктивна хипотеза нам даје тражено.

$\Rightarrow$. Довољно је показати да је сваки атом прост. Стога претпоставимо да је q атом и нека $q \mid ab$. То значи да је $ab = qc$ за неки $c \in A$. Представимо елементе a, b, c у облику производа атома: $a = p_1 \cdots p_r$, $b = q_1 \cdots q_s$, $c = z_1 \cdots z_t$. Добијамо једнакост

$$p_1 \cdots p_r q_1 \cdots q_s = q x_j \cdots z_t.$$

Како се атом q налази са десне стране ове једнакости, на основу јединствености растава следи да се неки њему придружени елемент налази са леве стране. Дакле, то је један од елемената $p_1, \dots, p_r$ или један од елемената $q_1, \dots, q_s$ (можда је и у једном и у другом скупу, не смета). У првом случају добијамо да $q \mid a$, а у другом да $q \mid b$. 

Показаћемо да је сваки **главноидеалски домен** (домен у коме је сваки идеал главни, тј. генерисан је једним елементом) домен са једнозначном факторизацијом. Најпре доказујемо да је сваки главноидеалски домен један **NZD домен**, тј. домен у коме за свака два елемента постоји највећи заједнички делилац. Наравно, знамо да је највећи заједнички делилац одређен до на инвертибилан елемент прстена. У прстену целих бројева смо могли изабрати позитиван број за највећи заједнички делилац, у прстену полинома моничан елемент, али у произвољном прстену немамо неки канонски избор. Можемо се договарати за сваки конкретан случај.

Став 19. У сваком главноидеалском домену свака два елемента имају највећи заједнички делилац.

 Нека је A главноидеалски домен и $a, b \in A$. Тада је $\langle a, b \rangle = \langle d \rangle$ за неки $d \in A$. Како $a \in \langle d \rangle$, имамо да је $a = da_1$ за неки a_1 , те $d \mid a$. На аналогни начин се покаже и да $d \mid b$. С друге стране претпоставимо да $d' \mid a$ и $d' \mid b$. То значи да је $a = d'a'$, $b = d'b'$. Из чињенице да $d \in \langle a, b \rangle$, добијамо да је

$d = ax + by$ за неке $x, y \in A$. Но, тада је $d = d'a'x + d'b'y = d'(a'x + b'y)$, па $d' \mid d$. Дакле d је највећи заједнички делилац елемената a и b . 

Последица 20. Нека је A главноидеалски домен и $a, b, c \in A$ такви да $a \mid bc$, $\text{NZD}(a, b) \in U(A)$. Тада $a \mid c$.

 У претходном доказу смо видели да, ако је $d = \text{NZD}(a, b)$ онда постоје $x, y \in A$, такви да је $d = ax + by$ (Безуова релација). Дакле, у нашем случају постоје $x', y' \in A$, такви да је $u = ax' + by'$, где је $u \in U(A)$. Множењем са u^{-1} добијамо да је $1 = ax + by$ за неке $x, y \in A$. Множењем те једнакости са c добијамо $c = acx + bcy$. Како $a \mid bc$, постоји $z \in A$ тако да је $bc = az$. Добијамо: $c = acx + bcy = acx + azy = a(cx + zy)$, из чега следи да $a \mid c$. 

Теорема 21. Сваки главноидеалски домен је домен са једнозначном факторизацијом.

 Докажимо најпре да у главноидеалском домену сваки непразан скуп идеала има максимални елемент. У ту сврху, нека је $\mathcal{I}$ неки непразан скуп идеала и нека не постоји максималан елемент у њему. Узмимо ма који идеал $I_0 \in \mathcal{I}$. По претпоставци он није максималан у $\mathcal{I}$, па постоји $I_1 \in \mathcal{I}$ такав да је $I_0 \subset I_1$. Ни I_1 није максималан, па постоји $I_2 \in \mathcal{I}$ такав да је $I_0 \subset I_1 \subset I_2$. Настављајући поступак добијамо бесконачни строго растући низ идеала у $\mathcal{I}$. Но, ово није могуће. Наиме, формирајмо унију $J = \cup_{n \geq 0} I_n$. Лако је проверити да је ово идеал. Наиме, ако $x, y \in J$, онда $x \in I_r$, а $y \in I_s$ за неке r, s . Тада $x, y \in I_{\max\{r, s\}}$, па $x + y \in I_{\max\{r, s\}} \subseteq J$. Још лакше се покаже друго својство, јер из $x \in J$, $a \in A$, следи да $x \in I_r$, па $a \cdot x \in I_r \subseteq J$. Дакле, $J \triangleleft A$. Но, у A је сваки идеал главни, па је $J = \langle b \rangle$, за неки $b \in A$. Но, то значи да је $b \in \cup_{n \geq 0} I_n$, те $b \in I_t$ из чега следи да је $J = I_t$, те је немогуће да је $I_t \subset I_{t+1}$ пошто су оба садржани у J , тј. I_t .

Докажимо најпре да је у сваки атом прост. У ту сврху, нека је a атом и нека $a \mid bc$. Посматрајмо $d = \text{NZD}(a, b)$. Имамо да је $a = da_1$, а како је a атом, то значи да је $d \in U(A)$ или је $a_1 \in U(A)$. У првом случају, применом горње последице добијамо да $a \mid c$. У другом случају имамо да је $d = aa_1^{-1}$, $b = db_1$, па је $b = aa_1^{-1}b_1$ из чега следи да $a \mid b$. Закључујемо да је a прост.

Претпоставимо да постоји елемент из $A \setminus (U(A) \cup \{0\})$ који нема факторизацију на просте елементе. Посматрајмо колекцију идеала из :

$$\mathcal{I} = \{\langle a \rangle : a \in A \setminus (U(A) \cup \{0\}) \text{ и } a \text{ нема растав на производ простих}\}.$$

По претпоставци је ова колекција непразна, па према доказаном мора имати максималан елемент. Нека је то идеал $I_0 = \langle a_0 \rangle$. То значи да a_0 нема растав на просте. Како је сваки атом прост, па има једночлан растав на просте, закључујемо да a_0 није атом те постоје $b \notin U(A)$, $c \notin U(A)$ такви да је $a_0 = bc$. Дакле, $a_0 \in \langle b \rangle$ и $a_0 \in \langle c \rangle$, те $\langle a_0 \rangle \subset \langle b \rangle$ и $\langle a_0 \rangle \subset \langle c \rangle$, при чему су ово прави подскупови, јер $b, c \notin \langle a_0 \rangle$ (из $b \in \langle a_0 \rangle$ следи да је $b = a_0 e$ за неко e те је тада $b = bce$). Скраћивањем са b добијамо да је $ce = 1$, па $c \in U(A)$ што није тачно). Одавде закључујемо да су идеали $\langle b \rangle$ и $\langle c \rangle$

строго већи од идеала $\langle a_0 \rangle$, који је максималан у $\mathcal{I}$, те они нису у $\mathcal{I}$. То пак значи да и b и c имају растав на производ простих елемената: $b = p_1 \cdots p_r$, $c = q_1 \cdots q_s$, па је $a = p_1 \cdots p_r \cdot q_1 \cdots q_s$, растав елемента a на производ простих, а претпоставили смо да такав растав не постоји. Ова контрадикција завршава доказ. 

Домен са једнозначном факторизацијом карактерише се тиме да се у њему прости елементи и атоми подударају и да се сваки ненула, неинвертибилан елемент a може представити у облику $a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}$ где је u инвертибилан, p_i прости, $\alpha_1 > 0$ и $p_i \not\sim p_j$, за $i \neq j$. При томе, ако је $a = vq_1^{\beta_1} \cdots q_l^{\beta_l}$ други растав тог типа, онда је $k = l$ и постоји пермутација $\sigma \in S_k$ таква да је, за све $i \in \{1, \dots, k\}$: $p_i \sim q_{\sigma(i)}$ и $\alpha_i = \beta_{\sigma(i)}$. Инвертибилан елемент u у општем случају не можемо избећи, као што то не можемо ни у прстену целих бројева. На пример, $-36 = (-1) \cdot 2^2 \cdot 3^2$. Наравно, можемо то записати и овако: $-36 = 2 \cdot (-2) \cdot 3^2$, али ту су прости елементи 2 и -2 придружени један другом.

У доменима са једнозначном факторизацијом свака два елемента имају највећи заједнички делилац. Наравно, то је једино занимљиво ако нису инвертибилни нити је неки од њих једнак 0. Дакле, нека су $a, b \in A \setminus (U(A) \cup \{0\})$, где је A домен са једнозначном факторизацијом. Посматрамо факторизације ова два елемента на производе простих и ако се појављују придружени прости фактори код оба елемента, заменимо их тако да су исти у обе факторизације. То можемо постићи променом оног инвертибилног елемента. Дакле, можемо да претпоставимо да имамо факторизације:

$$a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad b = vp_1^{\beta_1} \cdots p_k^{\beta_k}$$

при чему су u, v инвертибилни и $\alpha_i \geq 0, \beta_i \geq 0$ за све i . Дакле, може се десити да се неки од простих фактора не налази у обе факторизације, али су $p_1, \dots, p_k$ сви прости елементи који су неопходни за факторизацију ова два броја. Тада је јасно да је

$$\text{NZD}(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}}.$$

Наравно, постоји и $\text{NZS}(a, b)$ и јасно је да овде узимамо максималне степене простих бројева у раставу.

Но, у произвољним доменима са једнозначном факторизацијом не важи Безуова релација. На пример, јасно је да је $\text{NZD}(2, X) = 1$ у прстену $\mathbb{Z}[X]$, али не постоје полиноми $p(X)$ и $q(X)$ из $\mathbb{Z}[X]$ за које је $1 = 2p(X) + Xq(X)$.

Еуклидски домени

Знамо да су и $\mathbb{Z}$ и $K[X]$ главноидеалски домени и то захваљујући томе што у њима имамо дељење са остатком. Уведимо сада појам домена у коме постоји такво дељење.

Дефиниција 22. За домен A кажемо да је **Еуклидски домен** уколико постоји функција $\phi: A \setminus \{0\} \rightarrow \mathbb{N}$ тако да важе следећи услови.

- (1) $(\forall a, b \in A \setminus \{0\})(\phi(ab) \geq \phi(a))$.
- (2) $(\forall b \in A)(\forall a \in A \setminus \{0\})(\exists q, r \in A)(a = qb + r \wedge (r = 0 \vee \phi(r) < \phi(b)))$.

Пример 23. У случају $A = \mathbb{Z}$, узимамо да је $\phi(m) := |m|$, а у случају $A = K[X]$ узимамо $\phi(p) := \deg p$. 🙌

Како Еуклидски домен долази са одговарајућом функцијом, њу ћемо наводити у пару са прстеном.

Став 24. Сваки Еуклидски домен је главноидеалски домен.

👉 Нека је (A, ϕ) Еуклидски домен и $I \triangleleft A$. Ако је $I = \{0\}$, онда је $I = \langle 0 \rangle$. Претпоставимо да је $I \neq \{0\}$ и нека је $d \in I$ такав да је $\phi(d) = \min\{\phi(x) : x \in I\}$. Нека је $a \in I$. Тада постоје $q, r \in A$ такви да је $a = qd + r$, где је $r = 0$ или је $\phi(r) < \phi(d)$. Но, $a, d \in I$, те и $r = a - qd \in I$. Закључујемо да не може бити $\phi(r) < \phi(d)$, те мора бити $r = 0$, тј. $d \mid a$, па $a \in \langle d \rangle$. 📌

На основу става 19 знамо да у сваком Еуклидском домену за свака два елемента постоји њихов највећи заједнички делилац. За његово налажење можемо користити Еуклидов алгоритам. Наиме, ако су $a, b \in A \setminus \{0\}$, онда постоје q, r такви да је $b = qa + r$ при чему је $r = 0$ или је $\phi(a) < \phi(r)$. Уколико је $r = 0$, онда $a \mid b$ и $\text{NZD}(a, b) = a$. У супротном, имамо да је $a = qb + r$ и знамо да је $\text{NZD}(a, b) = \text{NZD}(b, r)$. Тада постоје q_1, r_1 такви да је $b = q_1r + r_1$, при чему је $r_1 = 0$ или је $\phi(r) < \phi(r_1) < \phi(b)$. Уколико је $r_1 = 0$, имамо да је $b = q_1r$, па је $r = \text{NZD}(b, r) = \text{NZD}(a, b)$. У супротном је $\text{NZD}(b, r) = \text{NZD}(r, r_1)$ и настављамо поступак са r, r_1 . Но, како је $\phi(b) > \phi(r) > \phi(r_1)$ овај се поступак мора завршити и тако добијамо највећи заједнички делилац.

Став 25. Нека је (A, ϕ) један Еуклидски домен.

- (а) Ако су $a, b \in A \setminus \{0\}$ и $b \mid a$ и $a \nmid b$, онда је $\phi(b) < \phi(a)$.
- (б) $(\forall a \in A \setminus \{0\})(\phi(a) \geq 1)$.
- (в) $(\forall a \in A)(\phi(a) = \phi(1) \text{ акко } a \in U(A))$.

👉 (а) Нека је $b = aq + r$, при чему је $\phi(r) < \phi(a)$ и $a = bc$. Тада је $r = b - aq = b - bcq = b(1 - cq)$, па је $\phi(r) = \phi(b(1 - cq)) \geq \phi(b)$.

(б) Ово је јасно: $a = 1 \cdot a$, па је $\phi(a) = \phi(1 \cdot a) \geq \phi(1)$.

(в) Имамо: $a \in U(A)$ акко $a \mid 1$ акко $\phi(1) \geq \phi(a)$ акко $\phi(a) = \phi(1)$. 📌

Важан пример је прстен **Гаусових целих бројева**: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

Став 26. Прстен $\mathbb{Z}[i]$ је Еуклидски домен, у коме је тражена функција дата са $\phi(a + bi) = a^2 + b^2$.

👉 Јасно је да је $\mathbb{Z}[i]$ домен пошто је потпрстен поља $\mathbb{C}$. Приметимо да је, заправо $\phi(z) = z\bar{z} = |z|^2$, те знамо да је $\phi(ab) = \phi(a)\phi(b) \geq \phi(a)$ за $b \neq 0$. Треба установити својство дељења. У ту сврху, нека су дати $a + bi, c + di \in \mathbb{Z}[i]$

при чему је $c + di \neq 0$. Посматрамо комплексан број $\frac{a+bi}{c+di} = x_1 + x_2i \in \mathbb{Q}[i]$. Уколико је он из $\mathbb{Z}[i]$, онда $(c + di) \mid (a + bi)$. Претпоставимо да није једнак 0. Тада је $[x_i] \leq x_i < [x_i] + 1$, при чему $[x]$ означава цео део броја x . Нека је $q_i \in \mathbb{Z}$ онај од бројева $[x_i], [x_i] + 1$ који је ближи броју x_i ; у случају да су подједнако удаљени, можемо да узмемо ма који од њих. Тада је $|x_i - q_i| \leq \frac{1}{2}$, па је

$$|(x_1 + x_2i) - (q_1 + q_2i)|^2 = |(x_1 - q_1) + (x_2 - q_2)i|^2 = (x_1 - q_1)^2 + (x_2 - q_2)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

Нека је $r_1 + r_2i = (a + bi) - (q_1 + q_2i)(c + di)$. Тада је

$$\begin{aligned} \phi(r_1 + r_2i) &= |r_1 + r_2i|^2 = |(a + bi) - (q_1 + q_2i)(c + di)|^2 \\ &= \left| \left(\frac{a + bi}{c + di} - (q_1 + q_2i) \right) (c + di) \right|^2 \\ &= |(x_1 + x_2i) - (q_1 + q_2i)|^2 |c + di|^2 \\ &\leq \frac{1}{2} \phi(c + di) \\ &< \phi(c + di). \end{aligned}$$

Дакле, за дате $a + bi, c + di \in \mathbb{Z}[i]$ постоје $q_i + q_2i, r_1 + r_2i \in \mathbb{Z}[i]$ тако да је $a + bi = (q_1 + q_2i)(c + di) + (r_1 + r_2i)$, при чему је $r_1 + r_2i = 0$ или је $\phi(r_1 + r_2i) < \phi(c + di)$, те је заиста $\mathbb{Z}[i]$ један Еуклидски домен. 

Не тврдимо да су количник и остатак јединствено одређени у произвољном Еуклидском домену.

Пример 27. Посматрајмо елементе $8 - i$ и $5 + i$ из $\mathbb{Z}[i]$. Имамо да је

$$\frac{8 - i}{5 + i} = \frac{(8 - i)(5 - i)}{26} = \frac{40 - 8i - 5i - 1}{26} = \frac{39 - 13i}{26} = \frac{3}{2} - \frac{1}{2}i.$$

- 1) Имамо да је $8 - i = 1 \cdot (5 + i) + (3 - 2i)$ и $\phi(3 - 2i) = 13 < 26 = \phi(5 + i)$.
- 2) А имамо и $8 - i = (5 + i)(2 - i) + (-3 + 2i)$ и $\phi(-3 + 2i) = 13 < 26 = \phi(5 + i)$.

Нађимо $\text{NZD}(8 - i, 5 + i)$. Користимо, на пример, прву варијанту дељења. Треба да поделимо $5 + i$ са $3 - 2i$:

$$\frac{5 + i}{3 - 2i} = \frac{(5 + i)(3 + 2i)}{13} = \frac{15 + 10i + 3i - 2}{13} = \frac{13 + 13i}{13} = 1 + i.$$

Последњи остатак различит од нуле је био $3 - 2i$ те је $\text{NZD}(8 - i, 5 + i) = 3 - 2i$. Да смо користили другу варијанту дељења добили бисмо да је највећи заједнички делилац $-3 + 2i$, а ти су елементи придружени један другом. 

Знамо да је $\mathbb{Z}[i]$ домен са једнозначном факторизацијом. Одредимо просте елементе у том домену. У ту сврху, нека је $\pi \in \mathbb{Z}[i]$ прост. Тада је идеал $\pi\mathbb{Z}[i] \triangleleft \mathbb{Z}[i]$ прост. Посматрамо прост идеал $(\pi\mathbb{Z}[i]) \cap \mathbb{Z} \triangleleft \mathbb{Z}$ (уверите се да је ово прост идеал). Како $\pi\pi \in \langle \pi \rangle \setminus \{0\}$ имамо да је $(\pi\mathbb{Z}[i]) \cap \mathbb{Z} = p\mathbb{Z}$ за неки прост $p \in \mathbb{Z}$. То значи да $p \in \pi\mathbb{Z}[i]$, па постоји $\sigma \in \mathbb{Z}[i]$ тако да је $p = \pi\sigma$. Тада је $\phi(p) = \phi(\pi)\phi(\sigma)$, па је $p^2 = (a^2 + b^2)(c^2 + d^2)$ за неке $a, b, c, d \in \mathbb{Z}$.

Имамо две могућности ($\phi(\pi) \neq 1$, јер би то значило да је $\pi \in \{1, -1, i, -i\}$, дакле инвертибилан):

1) $c^2 + d^2 = 1$, па је $\pi \sim p$.

2) $a^2 + b^2 = c^2 + d^2 = p$. Дакле, поставља се питање када је неки прост број у $\mathbb{Z}$ сума квадрата. Наравно, $2 = 1^2 + 1^2 = (1+i)(1-i) \sim (1+i)^2$. Тако смо добили нерастављив Гаусов цео број $1+i$, који је стога прост. Остају нам непарни прости бројеви. Приметимо да бројеви облика $4k+3$ не могу бити суме квадрата два цела броја различита од нуле: остатак при дељењу са 4 квадрата ма ког броја је или 1 или 0, па у збиру два таква никако не можемо добити 3. Дакле, прости бројеви облика $4k+3$ су прости и у $\mathbb{Z}[i]$. С друге стране, ако је p прост облика $4k+1$, онда је група $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ циклична група реда $4k$ и она мора да садржи елемент x реда 4. Дакле, у пољу $\mathbb{Z}_p$ имамо једнакост $x^4 = 1$, па добијамо $(x^2 - 1)(x^2 + 1) = 0$. Но, $x^2 - 1 \neq 0$, јер елемент x није реда 2, па добијамо $x^2 + 1 = 0$ у $\mathbb{Z}_p$. То значи да $p \mid (x^2 + 1)$ у $\mathbb{Z}$, па $p \mid (x+i)(x-i)$ у $\mathbb{Z}[i]$. Уколико би p био прост у $\mathbb{Z}[i]$, имали бисмо да $p \mid (x+i)$ или $p \mid (x-i)$, те би имали једнакост $x \pm i = pc \pm pdi$, што би значило да је $p \in \{-1, 1\}$. Дакле, добијамо да прости цели бројеви облика $4k+1$ нису прости у $\mathbb{Z}[i]$ и они су заправо облика $p = a^2 + b^2 = (a+bi)(a-bi)$. Ови бројеви $a \pm bi$ јесу нерастављиви, па тиме и прости (то нам даје претходна анализа). Приметимо да они нису придружени у $\mathbb{Z}[i]$: из придружености би следило да је $a + bi = u(a - bi)$, за неки $u \in U(\mathbb{Z}[i]) = \{-1, 1, i, -i\}$ и лако се можемо уверити да то није могуће. На пример, ако је $a + bi = i(a - bi)$, имали бисмо да је $b = a$, па би следило да је $p = (a + bi)(a - bi) = a^2(1+i)(1-i) = 2a^2$.

Да резимирамо урађено у облику става.

Став 28. Прости бројеви у $\mathbb{Z}[i]$ су:

1. $1+i$, при чему је $2 \sim (1+i)^2$.
2. Сви прости бројеви из $\mathbb{Z}$ облика $4k+3$.
3. За сваки прост број $p \in \mathbb{Z}$ облика $4k+1$, постоје a, b такви да је $p = (a+bi)(a-bi)$ и тада су $a \pm bi$ прости у $\mathbb{Z}[i]$.

Пример 29. а) Раставићемо број $60 + 56i \in \mathbb{Z}[i]$ на просте факторе. Најпре имамо да је $60 + 56i = 4(15 + 14i)$. Како је $4 = 2^2 = (((-i)(1+i))^2)^2 = (-1)(1+i)^4$, остаје нам да факторишемо $15 + 14i$. Но, $\phi(15 + 14i) = 421$ и то је прост број, па је заправо $15 + 14i$ прост у $\mathbb{Z}[i]$ и тражена факторизација је: $60 + 56i = (-1)(1+i)^4(15 + 14i)$.

б) Одредимо факторизацију броја $46 + 78i \in \mathbb{Z}[i]$. Како је $46 + 78i = 2 \cdot (23 + 39i)$ и $2 = (-i)(1+i)^2$ треба факторисати $23 + 39i$. Имамо да је $\phi(23 + 39i) = 2050 = 2 \cdot 5^2 \cdot 401$, очекујемо да се у факторизацији појави прост Гаусов цео број π такав да је $\phi(\pi) = 5$ и можда да се појави двоструко. Један такав је број $2+i$. Проверимо да ли $(2+i)^2 \mid (23 + 39i)$:

$$\frac{23+39i}{(2+i)^2} = \frac{23+39i}{4+4i-1} = \frac{23+39i}{3+4i} = \frac{(23+39i)(3-4i)}{25} = \frac{69+156+(117-92)i}{25} = \frac{225+25i}{25} = 9+i.$$

Како је $\phi(9+i) = 82 = 2 \cdot 41$, очекујемо да се појави $1+i$ у факторизацији:

$$\frac{9+i}{1+i} = \frac{(9+i)(1-i)}{2} = \frac{10-8i}{2} = 5-4i.$$

Како је $\phi(5-4i) = 41$, а то је прост број, закључујемо да је $5-4i$ Гаусов прост и имамо факторизацију: $46+78i = (-i)(1+i)^3 \cdot (2+i)^2 \cdot (5-4i)$.

Шта би се десило да смо делили са $(2-i)^2$ уместо са $(2+i)^2$? Уосталом, и $2-i$ је Гаусов прост за који је $\phi(2-i) = 5$. Проверимо:

$$\frac{23+39i}{(2-i)^2} = \frac{23+39i}{4-4i-1} = \frac{23+39i}{3-4i} = \frac{(23+39i)(3+4i)}{25} = \frac{69-156+(117+92)i}{25} = \frac{-87+209i}{25}$$

и видимо да нема дељивости! Но, то није никакав проблем, нити контрадикција. Просто смо имали среће у претходној провери ☺. Из чињенице да $5 \mid z$ следи да се у факторизацији за z појављује $2+i$ или $2-i$, али свакако не оба елемента. Подсетимо се да они нису придружени. Заправо, из дељивости $5^2 \mid z$ следи да се појављује један или други, или чак и оба, заправо имамо ту три могућности. Треба проверити која се од могућности реализује. 🍌

Поље разломака домена

У случају домена, важна је конструкција којом се од тог домена долази до поља „инвертовањем” свих елемената сем нуле. Уосталом, то смо радили и у школи и врло добро знамо да разломци нису уређени парови: $\frac{2}{3} = \frac{4}{6}$, а $(2, 3) \neq (4, 6)$. Разломци су заправо **класе еквиваленције**, но потпуно је оправдано да се то не спомиње експлицитно у основној школи 🤔.

Нека је A домен. На скупу $A \times (A \setminus \{0\})$ дефинишемо релацију $\approx$ са:

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

Није тешко уверити се да је $\approx$ релација еквиваленције. Проверимо транзитивност. Нека је $(a, s) \approx (b, t)$, $(b, t) \approx (c, u)$. То значи да је $ta = sb$, $ub = tc$. Но, тада је $uta = usb = sub = stc$, па скраћивањем са $t (\neq 0)$ добијамо $ua = sc$, тј. $(a, s) \approx (c, u)$. Са $Q(A)$ означавамо скуп класа еквиваленције при овој релацији, а класу еквиваленције пара (a, s) са $\frac{a}{s}$. Операције на $Q(A)$ задајемо са:

$$\frac{a}{s} + \frac{b}{t} := \frac{ta + sb}{st}, \quad \frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

Наравно, овде нам је важно било да је A домен, те из $s \neq 0$, $t \neq 0$ следи $st \neq 0$. Треба проверити добру дефинисаност ових операција. Урадићемо то за сабирање, а ви за вежбу урадите за множење.

Дакле, нека је $\frac{a}{s} = \frac{a'}{s'}$ и $\frac{b}{t} = \frac{b'}{t'}$. Треба показати да је $\frac{ta+sb}{st} = \frac{t'a'+s'b'}{s't'}$. Рачунамо:

$$s't'(ta+sb) = s't'ta + s't'sb = (s'a)t't + (t'b)s's = sa't't + tb's's = (st)(t'a' + s'b'),$$

а то је заиста оно што је тражено. Може се проверити да је $Q(A)$ комутативан прстен са јединицом. Овде је јединица класа пара $(1, 1)$ (или било ког пара

(a, a) , за $a \neq 0$): $1_{Q(A)} = \frac{1}{1}$, а $0_{Q(A)} = \frac{0}{1}$. Осим тога, $Q(A)$ је поље: ако је $\frac{a}{s} \neq \frac{0}{1}$, тј. ако је $a \neq 0$, имамо једнакост $\frac{a}{s} \cdot \frac{s}{a} = \frac{as}{sa} = \frac{1}{1} = 1_{Q(A)}$. Ово поље се назива **пољем разломака домена A** . У случају да је $A = \mathbb{Z}$, добијамо $Q(\mathbb{Z}) = \mathbb{Q}$, а у случају да је $A = K[X]$ добијамо **прстен рационалних функција**:

$$Q(K[X]) = K(X) = \left\{ \frac{p(X)}{q(X)} : p(X), q(X) \in K[X], q(X) \neq 0 \right\}.$$

Једнозначна факторизација у прстену полинома

У овом одељку, прстен A је домен са једнозначном факторизацијом. Главни резултат је следећа теорема.

Теорема 30. *Ако је A домен са једнозначном факторизацијом, онда је и $A[X]$ домен са једнозначном факторизацијом.*

Но, ово није тако лако доказати и биће нам потребни неки припремни резултати. У даљем ћемо са K означити поље разломака $Q(A)$ домена A . Докажимо најпре следећу лему.

Лема 31. *Ако је p прост елемент у A , онда је $\langle p \rangle \triangleleft A[X]$ прост идеал.*

👉 Важно је да разликујемо идеал pA прстена A генерисан елементом p и идеал $pA[X]$ прстена $A[X]$ генерисан тим истим елементом; овај потоњи идеал је горенаведени $\langle p \rangle$. Пошто је $\langle p \rangle$ прост елемент у A , онда је, по ставу 11, pA прост идеал у A и A/pA је домен. Ми треба да покажемо да је $A[X]/pA[X]$ домен. Дефинишимо пресликавање $\varphi: A[X] \rightarrow (A/pA)[X]$ са:

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) := \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_nX^n,$$

где је са $\bar{a}$ означена класа елемента a у количничком прстену: $\bar{a} = a + pA \in A/pA$. Како је придруживање $a \mapsto \bar{a}$ један епиморфизам (хомоморфизам који је „на”), лако се проверава да је и φ један епиморфизам. Но

$$a_0 + \cdots + a_nX^n \in \text{Ker } \varphi \text{ ако } (\forall i)(\bar{a}_i = 0_{A/pA})$$

$$\text{ако } (\forall i)(p \mid a_i)$$

$$\text{ако } (\forall i)(\exists b_i)(b_i = pa_i)$$

$$\text{ако } (\exists b_0, \dots, b_n)(a_0 + \cdots + a_nX^n = p(b_0 + \cdots + b_nX^n))$$

$$\text{ако } (a_0 + \cdots + a_nX^n \in pA[X]),$$

па је $\text{Ker } \varphi = pA[X]$. Закључујемо да је $A[X]/pA[X] \cong (A/pA)[X]$, а како је $(A/pA)[X]$ домен, добијамо да је и $A[X]/pA[X]$, па је идеал $\langle p \rangle = pA[X]$ прост. 📖

Дефиниција 32. *За полином $a(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ кажемо да је примитиван уколико је $\text{NZD}(a_0, a_1, \dots, a_n) = 1$.* 👉

Лема 33. (Гаусова лема) *Ако су $f, g \in A[X]$ примитивни, онда је и $f \cdot g$ примитиван.*

👉 Довољно је доказати да не постоји прост елемент који дели сваки коефицијент полинома $f \cdot g$. У супротном, нека је p прост елемент који дели сваки коефицијент овог производа. То значи да је тада $\varphi(f \cdot g) = 0_{(A/pA)[X]}$, где је φ горенаведени хомоморфизам. Но, како је f примитиван, p не дели све његове коефицијенте, те је $\varphi(f) \neq 0_{(A/pA)[X]}$. Из примитивности g следи да је $\varphi(g) \neq 0_{(A/pA)[X]}$. Но, како је $(A/pA)[X]$ домен, то је $\varphi(f) \cdot \varphi(g) \neq 0_{(A/pA)[X]}$, а $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g)$. Ова контрадикција завршава доказ. ■

Лема 34. Нека је $f \in K[X] \setminus \{0\}$. Тада:

- а) $f = c(f) \cdot f_0$, где је $f_0 \in A[X]$ примитиван полином, а $c(f) \in K$ је одређен до на инвертибилан елемент из A .
- б) $c(f \cdot g) = u \cdot c(f) \cdot c(g)$, где је $u \in U(A)$.

👉 а) Нека је $f = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \dots + \frac{a_n}{b_n}X^n$, где $a_i, b_i \in A$. Ако је $d = b_0b_1 \dots b_n$, јасно је да $df \in A[X]$. Како $d \frac{a_i}{b_i} \in A$, може се дефинисати

$$c = \text{NZD} \left(d \frac{a_0}{b_0}, d \frac{a_1}{b_1}, \dots, d \frac{a_n}{b_n} \right).$$

Тада је полином $f_0 = \frac{d}{c}f \in A[X]$ примитиван полином и имамо да је $f = \frac{c}{d}f_0$. Докажимо јединственост оваквог представљања. Нека је $f = c_1f_1 = c_2f_2$, где су $c_1, c_2 \in K$, а $f_1, f_2 \in A[X]$ примитивни полиноми. Уколико је $c_1 = \frac{p_1}{q_1}$, $c_2 = \frac{p_2}{q_2}$, при чему је $\text{NZD}(p_i, q_i) = 1$, онда из $\frac{p_1}{q_1}f_1 = \frac{p_2}{q_2}f_2$, множењем са q_1q_2 , добијамо $q_2p_1f_1 = q_1p_2f_2$. Како су f_1 и f_2 примитивни полиноми, то је q_2p_1 највећи заједнички делилац коефицијената полинома $q_2p_1f_1$, а q_1p_2 највећи заједнички делилац коефицијената полинома $q_1p_2f_2$. Како су ово једнаки полиноми, закључујемо да је $q_2p_1 \sim q_1p_2$, тј. постоји $u \in U(A)$ тако да је $q_2p_1 = uq_1p_2$, те је $\frac{p_1}{q_1} = u \frac{p_2}{q_2}$, тј. $c_1 = uc_2$ за неки $u \in U(A)$.

б) Нека је $f = c(f)f_1$, $g = c(g)g_1$, $h = f \cdot g = c(f \cdot g)h_0$, $f_0, g_0, h_0 \in A[X]$ примитивни полиноми. Тада је $f \cdot g = c(f)c(g)f_0g_0$, где је f_0g_0 примитиван по Гаусовој лем. Дакле, $c(f)c(g)f_0g_0 = c(f \cdot g)h_0$. На основу а) добијамо да је $c(f \cdot g) = u \cdot c(f) \cdot c(g)$ за неки $u \in U(A)$. ■

Приметимо да, уколико $f \in A[X] \setminus \{0\}$, онда наравно $c(f) \in A$.

Лема 35. Прости елементи у $A[X]$ су или прости елементи у A или примитивни полиноми из $A[X]$ који су нерастављиви у $K[X]$.

👉 Нека је $f \in A[X]$ прост елемент. Ако је $\deg f = 0$, онда је f прост елемент у A . Ако је пак $\deg f > 0$, онда f свакако мора бити примитиван полином. Наиме, ако постоји p , који је прост у A и који дели све коефицијенте полинома f , онда је $f = pg(X)$ за неки $g(X) \in A[X]$ и не би био нерастављив, па самим тим ни прост. Може ли f бити растављив у $K[X]$? Уколико би то било тако, тј. ако би постојали полиноми g, h степена бар 1 такви да је $f = g \cdot h$, онда би, на основу претходне две леме, важило да је $c(f) = u \cdot c(g) \cdot c(h)$, за неки $u \in U(A)$. Како је f примитиван полином, то је $c(f) = 1$ (или је неки

инвертибилан у A , што не мења ништа) и имали бисмо да $c(g) \cdot c(h) \in U(A)$.
Тада је

$$f = c(g)g_0 \cdot c(h)h_0 = \underbrace{c(g) \cdot c(h)}_{\in U(A)} g_0 h_0$$

и добили бисмо да је f нерастављив у $A[X]$ што противречи претпоставци да је f прост елемент у $A[X]$. Тиме смо доказали да ако је f прост елемент у $A[X]$, који није константан полином, онда је он примитиван полином, који је нерастављив у $K[X]$.

Докажимо сада и други смер. Ако је f прост елемент у A , онда из леме 31 следи да је он прост и у $A[X]$. Претпоставимо сада да је f примитиван полином из $A[X]$, који је нерастављив у $K[X]$. Треба показати да је он прост у $A[X]$. Претпоставимо да $f \mid g \cdot h$, за неке $g, h \in A[X]$. Како је f нерастављив у $K[X]$, а $K[X]$ јесте домен са једнозначном факторизацијом и ту се прости и нерастављиви елементи подударају, онда $f \mid g$ у $K[X]$ или $f \mid h$ у $K[X]$. Нека $f \mid g$ у $K[X]$. Тада је $g = k \cdot f$ за неки $k \in K[X]$. На основу леме 34 имамо да је $c(g) = c(k) \cdot c(f) \cdot u$, за неки $u \in U(A)$. Како је f примитиван, то је $c(f) = 1$, па је $c(k) = c(g) \cdot u^{-1} \in A$ ($g \in A[X]$, па $c(g) \in A$), па је заправо $k \in A[X]$ и $f \mid g$ у $A[X]$. На аналогни начин доказујемо да ако $f \mid h$ у $K[X]$, онда $f \mid h$ у $A[X]$. Тиме смо показали да је f прост елемент у $A[X]$ што завршава доказ. 

Сада најзад можемо доказати теорему 30.

👉 Знамо да је довољно показати да се сваки елемент из $A[X] \setminus (U(A[X]) \cup \{0\})$ може приказати у облику производа простих елемената. Наравно, имамо да је $U(A[X]) = U(A)$. Посматрајмо растав од f на атоме у $K[X]$ за који знамо да постоји: $f = f_1 \cdots f_k$. Но, $f_i = c(f_i)g_i$, где $c(f_i) \in K$, а g_i су примитивни полиноми у $A[X]$, који су нерастављиви у $K[X]$, јер су полиноми f_i нерастављиви у $K[X]$. Дакле,

$$f = c(f_1) \cdots c(f_k) g_1 \cdots g_k.$$

Како су g_i примитивни у $A[X]$, који су нерастављиви у $K[X]$, они су прости елементи у $A[X]$. Но, из горње једнакости следи да $c(f_1) \cdots c(f_k) \in A$, а како је A домен са једнозначном факторизацијом, постоје $d_1, \dots, d_r$ који су прости у A (а тиме и прости у $A[X]$ на основу леме 31), тако да је

$$c(f_1) \cdots c(f_k) = d_1 \cdots d_r.$$

Тако смо добили да је

$$f = d_1 \cdots d_r g_1 \cdots g_k$$

и то је тражена факторизација од f у производ простих елемената из $A[X]$. 

Као последицу ове теореме имамо чињеницу да су доменн $\mathbb{Z}[X]$, $\mathbb{Z}[X, Y]$, $\mathbb{Z}[X, Y, Z], \dots$ домени са једнозначном факторизацијом. Истакнимо још да смо доказали и да је примитиван полином у $A[X]$ нерастављив у $A[X]$ **акко** је нерастављив у $K[X]$.

Став 36. Нека је A домен са једнозначном факторизацијом, K његово поље разломака и $f, g \in A[X]$. Тада је $\text{NZD}(f, g) = \text{NZD}(c(f), c(g)) \cdot d$, где је $d \in A[X]$ примитивни полином у $A[X]$, који је највећи заједнички делилац полинома f и g у $K[X]$.

👉 Пре свега, знамо да је $A[X]$ домен са једнозначном факторизацијом, те да у њему свака два елемента имају највећи заједнички делилац. Докажимо најпре да је наведени полином заједнички делилац полинома f и g .

Како $d \mid f$ у $K[X]$, те и $\text{NZD}(c(f), c(g)) \cdot d \mid f$ у $K[X]$, имамо једнакост $f = \text{NZD}(c(f), c(g)) \cdot d \cdot q$ за неки полином $q \in K[X]$. Добијамо да је $c(f) = \text{NZD}(c(f), c(g))c(q)u$, за неки $u \in U(A)$, пошто је $c(d) = 1$, јер је d примитиван полином. Но, $\text{NZD}(c(f), c(g)) \mid c(f)$, те можемо да скратимо тим елементом из A и добијамо да је $c(q) \in A$, те $q \in A[X]$ и наведени полином дели f у $A[X]$. На исти начин се показује да он дели и g у $A[X]$.

Нека је сада $D \in A[X]$ полином који дели и f и g у $A[X]$. Тада је $f = Dq_1$ у $A[X]$, те је $c(f) = c(D)c(q_1)v$, за неки $v \in U(A)$. То значи да $c(D) \mid c(f)$ у A , јер је $c(q_1)v \in A$. Такође, $c(D) \mid c(g)$ у A и добијамо да $c(D) \mid \text{NZD}(c(f), c(g))$ у A . Ако искористимо приказ $D = c(D)D_0$, где је D_0 примитиван полином и чињеницу да $D \mid d$ у $K[X]$, јер је d највећи заједнички делилац ових полинома у $K[X]$, онда $D \mid \text{NZD}(c(f), c(g))d$ у $K[X]$ и $\text{NZD}(c(f), c(g))d = DQ$ у $K[X]$, за неки $Q \in K[X]$. Тада је $\text{NZD}(c(f), c(g))c(d) = c(D)c(Q) \cdot w$, за неки $w \in U(A)$. Како $c(D) \mid \text{NZD}(c(f), c(g))$ у A , то је $\text{NZD}(c(f), c(g)) = c(D)a$, за неки $a \in A$ и добијамо да је $c(Q) = aw^{-1} \in A$. Стога је $Q \in A[X]$ и D дели наведени полином у $A[X]$. Стога полином $\text{NZD}(c(f), c(g)) \cdot d$ испуњава оба услова за највећи заједнички делилац и то завршава доказ овог става, ■

Илуструјмо став 36 примерима.

Пример 37. Одредимо највећи заједнички делилац полинома $f(X) = 8X^5 + 8X^4 + 4X^3 + 4X^2 + 4X + 8$ и $g(X) = 18X^4 + 24X^3 + 12X^2 - 6X - 12$ у прстену $\mathbb{Z}[X]$.

Имамо да је

$$c(f) = \text{NZD}(8, 8, 4, 4, 4, 8) = 4, \quad c(g) = \text{NZD}(18, 24, 12, -6, -12) = 6$$

из чега добијамо $\text{NZD}(c(f), c(g)) = 2$. Следеће што треба да урадимо је да нађемо највећи заједнички делилац ових полинома у $\mathbb{Q}[X]$. Потом, пошто знамо да је највећи заједнички делилац одређен до на инвертибилан елемент, према ставу 36 треба да изаберемо полином који је примитиван у $\mathbb{Z}[X]$. Он наравно не мора бити моничан.

Како радимо са коефицијентима у пољу $\mathbb{Q}$, сви цели бројеви различити од нуле су инвертибилни, те је $\text{NZD}(ma(X), nb(X)) = \text{NZD}(a(X), b(X))$ за све целе бројеве $m, n \neq 0$. Поступак наравно изводимо Еуклидовим алгоритмом, али користимо ову идеју да бисмо поједноставили међурезултате. Како је $f(X) = 4(2X^5 + 2X^4 + X^3 + X^2 + X + 2)$ и $g(X) = 6(3X^4 + 4X^3 + 2X^2 - X - 2)$, то Еуклидов алгоритам можемо применити на ове примитивне полиноме у

заградама. Дакле, могли бисмо да започнемо дељењем полинома $2X^5 + 2X^4 + X^3 + X^2 + X + 2$ полиномом $3X^4 + 4X^3 + 2X^2 - X - 2$ у $\mathbb{Q}[X]$. Наравно, видимо да ће нам се одмах појавити разломци. Нема ничег лошег у разломцима, али ради лакше рачунице бисмо волели да их избегнемо. Видимо да то можемо да постигнемо ако први примитиван полином помножимо са 3. То ће свакако дати цео број као коефицијент на почетку, али се дељење не завршава у једном кораку пошто је разлика у степенима ових полинома једнака 1. Стога се у другом кораку може појавити разломак. Зато је погодно први примитивни полином помножити са $3^2 = 9$.

Дакле, делимо полином $18X^5 + 18X^4 + 9X^3 + 9X^2 + 9X + 18$ полиномом $3X^4 + 4X^3 + 2X^2 - X - 2$. То радимо стандардно и добијамо да је количник $6X - 2$, а остатак $5X^3 + 19X^2 + 19X + 14$. Сада полином $3X^4 + 4X^3 + 2X^2 - X - 2$ треба поделити полиномом $5X^3 + 19X^2 + 19X + 14$. Да бисмо избегли разломке, први полином множимо са $5^2 = 25$.

Када полином $75X^4 + 100X^3 + 50X^2 - 25X - 50$ поделимо полиномом $5X^3 + 19X^2 + 19X + 14$ добијамо количник $15X - 37$ и остатак $468X^2 + 468X + 468 = 468(X^2 + X + 1)$. Потом полином $5X^3 + 19X^2 + 19X + 14$ делимо полиномом $X^2 + X + 1$ и добијамо количник $5X + 14$, а остатак је једнак 0.

Како је последњи нунула остатак, до на константан умножак, једнак $X^2 + X + 1$, а то је још и примитиван полином у $\mathbb{Z}[X]$ бирамо баш њега и коначно добијамо да је $\text{NZD}(f, g) = 2(X^2 + X + 1)$ на основу става 36. 🍌

Пример 38. Одредимо највећи заједнички делилац полинома $f(X, Y) = X^3Y + X^2Y^2 - 2XY^3 + XY^2 + 2Y^4$ и полинома $g(X, Y) = X^4Y^2 + 2X^3Y^3 + XY^4 + XY^2 + 2Y^5 + 2Y^3$ у прстену $\mathbb{Z}[X, Y]$.

Да бисмо применили став 36, представимо наше полиноме као полиноме у прстену $\mathbb{Z}[Y][X]$ (дакле овде ће основни прстен бити $A = \mathbb{Z}[Y]$) и означимо први са P , а други са Q : $P = YX^3 + Y^2X^2 + (-2Y^3 + Y^2)X + 2Y^3$, а $Q = Y^2X^4 + 2Y^3X^3 + (Y^4 + Y^2)X + 2Y^5 + 2Y^3$. Тада је $c(P) = \text{NZD}(Y, Y^2, -2Y^3 + Y^2, 2Y^3) = Y$, док је $c(Q) = \text{NZD}(Y^2, 2Y^3, Y^4 + Y^2, 2Y^5, 2Y^3) = Y^2$. Дакле, $\text{NZD}(c(P), c(Q)) = Y$.

Сада треба да нађемо највећи заједнички делилац полинома $P_0 = X^3 + YX^2 + (-2Y^2 + Y)X + 2Y^3$ и $Q_0 = X^4 + 2YX^3 + (Y^2 + 1)X + 2Y^3 + 2Y$ у прстену $\mathbb{Q}(Y)[X]$ и да онда изаберемо такав који је примитивни полином у $\mathbb{Z}[Y][X]$ (поље разломака прстена $\mathbb{Z}[Y]$ је поље $\mathbb{Q}(Y)$).

Поделимо полином Q_0 полиномом P_0 . Добијамо количник $X + Y$ и остатак $(Y^2 - Y)X^2 + (2Y^3 - 2Y^2 + 1)X + 2Y$. Сада би полином P_0 требало поделити тим остатком. Да би се избегло појављивање правих рационалних функција, делићемо полином $(Y^2 - Y)^2P_0$ тим остатком. После доста рачунања ☺, добијамо да је количник $(Y^2 - Y)X - Y^3 + Y^2 - 1$, а остатак $(Y^5 - 2Y^4 + 2Y^3 - Y^2 + 1)X + (2Y^6 - 4Y^5 + 4Y^4 - 2Y^3 + 2Y)$. Имамо да је $2Y^6 - 4Y^5 + 4Y^4 - 2Y^3 + 2Y = 2Y(Y^5 - 2Y^4 + 2Y^3 - Y^2 + 1)$, те је остатак заправо

$(Y^5 - 2Y^4 + 2Y^3 - Y^2 + 1)(X + 2Y)$ и у даљем можемо користити $X + 2Y$ пошто је сваки ненула полином по Y инвертибилан у $\mathbb{Q}(Y)$!

Дакле, остало је да се полином $(Y^2 - Y)X^2 + (2Y^3 - 2Y^2 + 1)X + 2Y$ подели полиномом $X + 2Y$. Добијамо да је количник $(Y^2 - Y)X + 1$, а остатак 0. Стога је највећи заједнички дилац полинома P_0 и Q_0 у $\mathbb{Q}(Y)[X]$ полином $X + 2Y$ и како је он примитиван у $\mathbb{Z}[Y][X]$ (коефицијенти су му 1 и $2Y$), можемо узети њега. Коначно нам став 36 даје: $\text{NZD}(f, g) = Y(X + 2Y)$. 🍌

За вежбу урадите овај пример тако што ћете ове полиноме посматрати као полиноме из $\mathbb{Z}[X][Y]$

Докажимо сада важан Ајзенштајнов критеријум за нерастављивост полинома и дајемо једну његову примену.

Став 39. (Ајзенштајнов критеријум) Нека је A домен са једнозначном факторизацијом, K његово поље разломака и $f = a_n X^n + \dots + a_1 X + a_0 \in A[X]$ такав да постоји прост елемент $p \in A$ за који важи:

- (1) $p \mid a_0, p \mid a_1, \dots, p \mid a_{n-1}, p \nmid a_n$;
- (2) $p^2 \nmid a_0$.

Тада је f нерастављив у $K[X]$.

🍌 Претпоставимо да је $f = g \cdot h$ у $K[X]$, факторизација на неконстантне полиноме. Тада је $c(f) = c(g)c(h)u$, за неки $u \in U(A)$. Како је $f \in A[X]$, то је $c(g)c(h) \in A$ и добијамо да је $f = c(g)g_0c(h)h_0 = g_1h_1$, при чему је $g_1 = c(g)c(h)g_0 \in A[X]$, $h_1 = h_0$. Дакле, имамо факторизацију $f = g_1h_1$ у $A[X]$.

Искористимо сада хомоморфизам φ из доказа леме 31. На основу прве претпоставке, добијамо да је $\varphi(f) = \overline{a_n}X^n$. Факторизација $f = g_1h_1$ нам даје $\overline{a_n}X^n = \varphi(f) = \varphi(g_1) \cdot \varphi(h_1)$. Но, како је A/pA домен, ово је могуће само ако је $\varphi(g_1) = \overline{c}X^k$, $\varphi(h_1) = \overline{d}X^{n-k}$, за неке c, d , при чему је $1 < k < n$. Посебно су слободни чланови полинома $\varphi(g_1)$ и $\varphi(h_1)$ једнаки 0, што заправо значи да су слободни чланови самих полинома g_1 и h_1 дељиви са p . Но, њихов производ је слободан члан полинома f , тј. a_0 , па би он био дељив са p^2 , а то је супротно другој претпоставци. Стога закључујемо да је f нерастављив у $K[X]$. 🍌

Пример 40. Нека је p прост број. Показаћемо да је полином $a(X) = X^{p-1} + \dots + X + 1 \in \mathbb{Z}[X]$ нерастављив у $\mathbb{Q}[X]$.

Јасно је да је полином $a(X)$ нерастављив ако и само ако је то полином $a(X + 1)$. Наиме, из нетривијалног растава $a(X + 1) = b(X)c(X)$ бисмо добили нетривијалан растав $a(X) = b(X - 1)c(X - 1) = a_1(X)b_1(X)$. Сада приметимо да је $(X - 1)a(X) = X^p - 1$, па је

$$Xa(X + 1) = X^{p+1} - 1 = \sum_{k=0}^n \binom{p}{p-k} X^{p-k} - 1 = \sum_{k=0}^{p-1} \binom{p}{p-k} X^{p-k}.$$

Стога је

$$a(X+1) = X^{p-1} + pX^{p-2} + \binom{p}{2}X^{p-3} + \dots + p.$$

Како за све $1 \leq k \leq p-1$ важи да $p \mid \binom{p}{k}$, а $p^2 \nmid p$ и $p \nmid 1$, на основу Ајзенштајновог критеријума полином $a(X+1)$ је нерастављив у $\mathbb{Q}[X]$. 🍑

За испитивање нерастављивости полинома, корисна је и провера да ли полином има нулу у пољу разломака. Ево става који нам у томе помаже.

Став 41. Нека је $f(X) = a_nX^n + \dots + a_1X + a_0 \in A[X]$, где је A домен са једнозначном факторизацијом. Уколико су $b, c \in A$ такви да је $c \neq 0$, $\text{NZD}(b, c) = 1$ и $f(b/c) = 0$, онда $b \mid a_0$ и $c \mid a_n$. Посебно, ако је $f(X)$ моничан полином, свака нула тог полинома, која се налази у K , заправо припада A .

🍑 Ако је $f(b/c) = 0$, онда је

$$a_n \left(\frac{b}{c}\right)^n + a_{n-1} \left(\frac{b}{c}\right)^{n-1} + \dots + a_1 \left(\frac{b}{c}\right) + a_0 = 0.$$

Множењем са c^n добијамо

$$a_nb^n + a_{n-1}b^{n-1}c + \dots + a_1bc^{n-1} + a_0c^n = 0.$$

Одавде добијамо да $b \mid a_0c^n$ и $c \mid a_nb^n$. Но, како је $\text{NZD}(b, c) = 1$, добијамо да $b \mid a_0$ и $c \mid a_n$. Ми смо ово извели за случај главноидеалских домена, а није тешко показати да резултат важи и за домене са једнозначном факторизацијом. Наиме, из $b \mid a_0c^n$ следи да је $bd = a_0c^n$, за неки $d \in A$. Докажимо да $b \mid a_0$ индукцијом по броју (s) простих фактора у раставу од b . Ако је $s = 1$, имамо да је b прост број те $b \mid a_0$ или $b \mid c^n$. Но, из $\text{NZD}(b, c) = 1$ следи да $b \nmid c$, па добијамо тражено. Претпоставимо да тврђење важи ако за елементе који имају растав на производ од s простих елемената и нека b има растав на производ од $s+1$ простих. Нека је p један од тих простих у раставу од b . Тада свакако $p \mid a_0c^n$, но $p \nmid c$ (па стога не дели ни c^n) јер b и c немају заједничких простих делилаца. Стога $p \mid a_0$. Дакле, имамо једнакости: $b = pb'$, $a_0 = pa'_0$. Добијамо да је $pb'd = pa'_0c^n$ те скраћивањем са p добијамо $b'd = a'_0c^n$. Наравно, $\text{NZD}(b', c) = 1$, па нам индуктивна хипотеза даје да $b' \mid a'_0$, а одатле следи да $pb' \mid pa'_0$, тј. $b \mid a_0$.

Посебно, ако је $f(X)$ моничан полином, имамо да је $a_n = 1$, па из $c \mid 1$ следи да је c инвертибилан у A , те $b/a \in A$. 🍑

Пример 42. Нека је прстен са једнозначном факторизацијом, K његово поље разломака, p прост елемент у A и $n \geq 2$ природан број. Покажимо да једначина $x^n = p$ нема решења у K .

Посматрамо полином $f(X) = X^n - p \in A[X]$. Ако би он имао нулу у K , како је он моничан полином, имао би нулу у A на основу претходног става. Но, тада бисмо добили да је $p = a^n$ у A , те би p био растављив, што противречи претпоставци да је он прост, па тиме и нерастављив. 🍑

Наравно, претходни пример је генерализација добро нам познатог резултата из средње школе, који је био познат и у старој Грчкој: $\sqrt{2}$ није рационалан број.

Конструкције лењиром и шестаром

У школи смо имали прилике да изучавамо конструкције које се могу извршити лењиром и шестаром. Наравно, ту се подразумева да лењир није „баждарен”, тј. да не можемо одмеравати дужине помоћу лењира (без обзира на чињеницу да лењери, који се продају као школски прибор јесу баждарени). Лењери само служе за повлачење правих кроз две дате тачке. У вези са тим су добро позната три конструктивна проблема Антикe (за које су вероватно неки од читалаца и чули).

1. Удвостручавање коцке. За дату коцку, наћи коцку двоструко веће запремине. С обзиром на то да је запремина коцке странице a једнака a^3 за налажење странице b за коју је $b^3 = 2a^3$ потребно је и довољно конструисати број $\sqrt[3]{2}$.

2. Трисекција угла. Дати угао поделити на три једнака дела. Добро нам је познато како да преполовимо угао, а и како да дату дуж поделимо на три једнака дела, али како поделити угао на три једнака дела? Показаћемо да се и то своди на питање конструкције броја који је решење неке једначине трећег степена (као што је и $\sqrt[3]{2}$ решење једначине $x^3 = 2$).

3. Квадратура круга. За дати круг наћи квадрат чија је површина једнака површини датог круга. С обзиром на то да је површина круга полу пречника r дата формулом $r^2\pi$, а да је површина квадрата странице a једнака a^2 решавање проблема се своди на конструкцију броја $\sqrt{\pi}$.

У овом одељку, укратко ћемо описати главне алгебарске идеје које се налазе у основи проблема конструкције лењиром и шестаром и показати да се прва два наведена проблема не могу решити на тај начин.

Све конструкције наравно вршимо у равни. У њој ћемо изабрати једну тачку O и две нормалне праве које кроз њу пролазе. Замислићемо, ради лакшег описа, да је једна ‘хоризонтална’, а друга ‘вертикална’ (оне представљају координатне осе). На хоризонталној оси, изабраћемо ‘са десне стране’ од тачке O једну тачку P и сматраћемо да дуж OP представља јединичну дуж. Дакле, координате тачке P биће $(1, 0)$.

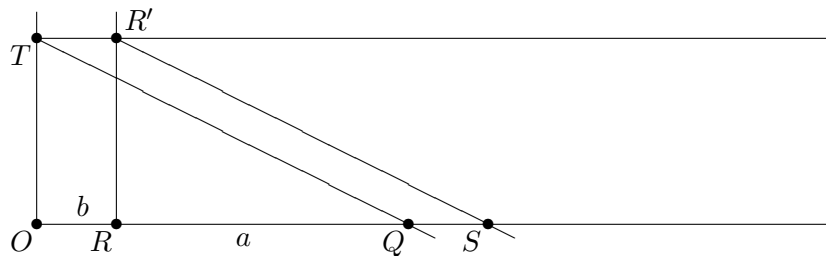
Основна конструкција лењиром је повлачење праве кроз две већ конструисане тачке, док је основна конструкција шестаром цртање круга са центром у једној конструисаној тачки која пролази кроз другу конструисану тачку. У пресеку тако конструисаних правих и кругова, добијамо нове тачке. Тачка у равни је конструктивна уколико се може добити понављањем основних конструкција коначно много пута. Приметимо да можемо посебно разматрати и конструкције тачака на координатним осама. Тако добијамо и појам конструктивних реалних бројева. Није тешко уверити се да важи следећи став.

Став 43. Тачка у равни са координатама (a, b) је конструктивна ако и само ако су a и b конструктивни реални бројеви.

Тачке у равни можемо да видимо и као комплексне бројеве на стан дардан начин. Следећи став је занимљив.

Став 44. Конструктивни бројеви чине поље.

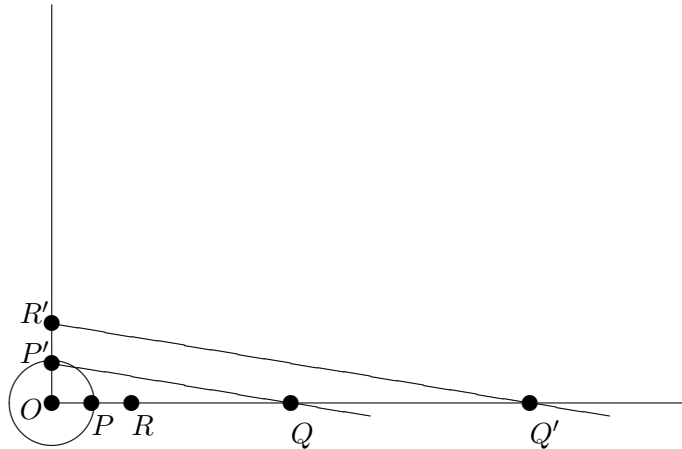
👉 Дајемо доказ за реалне бројеве. С обзиром на то како се изводе операције са комплексним бројевима, лако се потом добија резултат и за комплексне бројеве. Ми ћемо доказати да реални конструктивни бројеви чине потпоље од $\mathbb{R}$. У ту сврху, треба показати да, ако су a и b конструктивни реални бројеви, онда су то и бројеви $a \pm b$, $a \cdot b$, као и да је $\frac{1}{a}$ конструктиван број за сваки конструктиван број $a \neq 0$. Није тешко уверити се да је довољно ово показати када имамо позитивне реалне бројеве (негативни бројеви само уводе више случајева). Конструкција броја $a + b$ дата је следећим цртежом.



Наиме, ако је број a одређен тачком Q , а број b тачком P , онда најпре кроз неку тачку T (такву да је дужина дужи OT неки конструктиван број) на вертикалној оси конструишемо праву паралелну хоризонталној оси (то знамо да конструишемо помоћу лењира и шестара). Потом кроз тачку P конструишемо праву паралелну вертикалној оси и у пресеку добијамо тачку P' . Повлачимо и праву кроз тачке T и Q . На крају повлачимо праву кроз P' паралелну правој кроз тачке T и Q . У пресеку са хоризонталном осом добијамо тачку C која и одговара броју $a + b$.

Читаоцима остављамо да провере како се може конструисати број $a - b$.

За конструкцију броја $a \cdot b$ користимо следећу пропорцију: $ab : b = a : 1$. Ево цртежа (тачка P означава позицију броја 1).



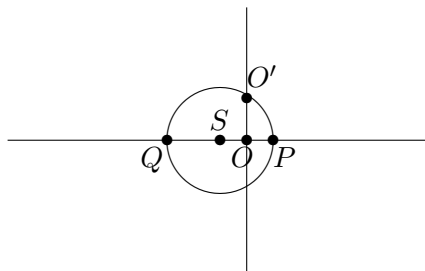
Постављамо кругове са центром у O који пролазе кроз тачке P (која одговара броју 1) и тачку R (која одговара броју b). У пресеку добијамо тачке P' и R' на вертикалној оси. Права кроз R' паралелна правој кроз тачке P' и Q сече хоризонталну осу у тачки Q' и та тачка одговара тачки $a \cdot b$. Наиме, правоугли троуглови $\triangle QOP'$ и $\triangle Q'OR'$ су слични, па је $OQ : OP' = OQ' : OR'$, односно $a : 1 = OQ' : b$. Стога тачка Q' заиста одговара броју $a \cdot b$.

Остављамо читаоцима за вежбу да покажу како се може конструисати број $\frac{1}{a}$ ако је a већ конструисан. 

Имамо и више од тога да конструктивни бројеви чине поље.

Став 45. *Ако је позитиван реалан број a конструктиван, конструктиван је и број $\sqrt{a}$.*

 Препоручујемо читаоцима да се увере да цртеж



даје решење. Овде тачка P одговара, као и раније, броју 1, тачка Q броју $-a$, а S је центар конструисаног круга. Дужина дужи OO' одговара броју $\sqrt{a}$. 

Став 46. *Нека су дате тачке A, B, C, D чије су координате у неком потпољу F поља $\mathbb{R}$. Тада су координате тачака које се добијају у пресеку две праве, два круга, или праве и круга, одређених са две од ових тачака, припадају или пољу F или пољу $F(\sqrt{r})$, где је $r \in F$.*

👉 Дакле, дате су тачке $A(x_1, y_1)$, $B(x_2, y_2)$, $C(x_3, y_3)$ и $D(x_4, y_4)$. Једначина праве кроз тачке A и B дата је са:

$$\frac{x - x_1}{y - y_1} = \frac{x_2 - x_1}{y_2 - y_1},$$

док је једначина круга који има центар у C и пролази кроз D дата са:

$$(x - x_3)^2 + (y - y_3)^2 = (x_4 - x_3)^2 + (y_4 - y_3)^2.$$

Стога се налажење пресека те праве и тог круга своди на решавање система од једне линеарне и једне квадратне једначине. Посматрањем прво линеарне једначине, можемо једну координату изразити преко друге (или се чак добија да је једна координата фиксирана, што опет значи да је изражена преко друге, само преко константне функције) и тако заменом у једначину круга добијамо квадратну једначину, а знамо да њено решавање укључује налажење квадратног корена из неког елемента који је изражен у облику количника полинома по коефицијентима, па стога припада пољу F . Дакле, нове координате су или из F или су у пољу $F(\sqrt{r})$, где је r тај број чији се корен тражи у поступку решавања једначине, а сигурно припада пољу F .

У случају да посматрамо пресек две праве, ситуација је још једноставнија, јер решења морају припадати пољу F , док се случај пресека два круга своди, одузимањем њихових једначина, на случај тражења решења система једне линеарне и једне квадратне једначине (квадратни чланови ће се одузимањем скратити). 

Наведимо сада најважнију теорему у овом одељку.

Теорема 47. Нека је α конструктибилан реалан број који не припада $\mathbb{Q}$. Тада постоји низ потпоља од $\mathbb{R}$

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \dots \subset F_n = F,$$

тако да $\alpha \in F$, $F_i = F_{i-1}(\sqrt{r_i})$, где је $r_i > 0$, $r_i \in F_{i-1}$, $\sqrt{r_i} \notin F_{i-1}$. Дакле,

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$$

за неко $s \geq 1$.

👉 Као што знамо, нека тачка је конструктибилна ако се може добити од конструктибилних тачака у коначно много корака од којих се сваки састоји од налажења пресека две праве, или праве и круга. А реалан број је конструктибилан уколико је координата неке конструктибилне тачке. Дакле, α је координата неке тачке A , која је добијена као последња тачка у низу. Као што знамо, сви рационални бројеви се могу конструисати почев од 0 и 1. Затим, евентуално, додајемо корен неког позитивног рационалног броја r_1 и добијамо поље $\mathbb{Q}(\sqrt{r_1})$, при чему $\sqrt{r_1} \notin \mathbb{Q}$. На основу става, у следећем кораку, највише што је потребно додати је опет корен неког броја из $\mathbb{Q}(\sqrt{r_1})$, који се ту не налази. Дакле, заиста добијамо низ поља као што је наведено и $\alpha \in F$, где је

F то последње поље. Но, с обзиром на то да је $F_i = F_{i-1}(\sqrt{r_i})$, при чему је $r_i \in F_{i-1}$ и $\sqrt{r_i} \notin F_{i-1}$, јасно је да је

$$[F_i : F_{i-1}] = 2,$$

јер је полином $X^2 - r_i$ минималан полином елемента $\sqrt{r_i}$ над пољем F_{i-1} . Стога је

$$[F : \mathbb{Q}] = [F_n : F_{n-1}] \cdot [F_{n-1} : F_{n-2}] \cdots [F_1 : F_0] = 2^n.$$

Но, како $\alpha \in F$, добијамо да је

$$2^n = [F : \mathbb{Q}] = [F : \mathbb{Q}(\alpha)] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}],$$

те је заиста $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$ за неко $s \geq 1$. 

Напомена. Одговарајући резултат важи и за конструктивилне комплексне бројеве: ако је $\alpha \in \mathbb{C} \setminus \mathbb{Q}$ конструктивилан, онда је $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^s$ за неко $s \geq 1$.

Сада можемо да решимо она два проблема. Позабавимо се најпре проблемом удвостручавања коцке.

Став 48. *Удвостручавање коцке није могуће извршити коришћењем искључиво лењира и шестара.*

👉 Видели смо да се то своди на конструктивилност броја $\sqrt[3]{2}$. Но, полином $a(X) = X^3 - 2$ је нерастављив над $\mathbb{Q}$ на основу Ајзенштајновог критеријума. Како је $a(\sqrt[3]{2}) = 0$, то је $a(X)$ минимални полином елемента $\sqrt[3]{2}$, те је $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \deg a(X) = 3$, што противречи претходној теорему, јер 3 свакако није степен двојке. 

Да бисмо доказали да није могуће извршити трисекцију произвољног угла коришћењем лењира и шестара, довољно је показати да се не може конструисати угао од 20° . Наиме, знамо да се угао од 60° може конструисати лењиром и шестаром, а ако је доказано да се угао од 20° не може конструисати лењиром и шестаром, то се угао од 60° не може поделити на три једнака дела само лењиром и шестаром.

Разматрањем јединичног круга, видимо да се немогућност конструкције угла од 20° своди на немогућност конструкције броја $\cos 20^\circ$. Докажимо то.

Став 49. *Број $\cos 20^\circ$ није конструктивилан.*

👉 Користићемо следећи индентитет:

$$\cos 3\varphi = 4 \cos^3 \varphi - 3 \cos \varphi.$$

Читаоци би требало да провере како се добија овај идентитет. У сваком случају, ако узмемо да је $\varphi = 20^\circ$ добијамо

$$4 \cos^3 20^\circ - 3 \cos 20^\circ = \cos 60^\circ = \frac{1}{2}.$$

Дакле,

$$\cos^3 20^\circ - \frac{3}{4} \cos 20^\circ - \frac{1}{8} = 0.$$

Посматрајмо полином $a(X) = X^3 - \frac{3}{4}X - \frac{1}{8} \in \mathbb{Q}[X]$. Докажимо да је он нерастављив над $\mathbb{Q}$. С обзиром на то да је у питању полином трећег степена, доказ се своди на проверу да ли тај полином има нулу у $\mathbb{Q}$. То би била и нула полинома $8a(X) = 8X^3 - 6X - 1$. Но ако је $\frac{p}{q} \in \mathbb{Q}$ једна нула тог полинома, при чему је $jq > 0$ и овај разломак нестратив, онда $p \mid (-1)$, а $q \mid 8$ по добро нам познатом критеријуму, који смо скоро доказали. Лако је проверити да такви p и q не постоје (уверите се у то). Алтернативно, посматрамо полином $b(X) = 8a(X+1) = 8X^3 - 24X^2 + 18X - 3$, који је нерастављив по Ајзенштајновом критеријуму – узимамо $p = 3$.

Добили смо да полином $a(X)$ није растављив над $\mathbb{Q}$. Како је $a(\cos 20^\circ) = 0$, закључујемо да је $a(X)$ минимални полином за $\cos 20^\circ$ над $\mathbb{Q}$, те је $[\mathbb{Q}(\cos 20^\circ) : \mathbb{Q}] = 3$, што показује да број $\cos 20^\circ$ није конструктибилан. 

Овај резултат нам показује да искључиво лењиром и шестаром није могуће конструисати правилни 18-угао. Наиме, јасно је да се конструкција правилног n -тоугла своди на конструкцију централног угла над његовом страницом, а то је угао од $\frac{360^\circ}{n}$, односно у случају правилног 18-тоугла ради се о у углу од 20° .

Следећи резултат је нешто тежи за доказ.

Став 50. *Ако је p непаран прост број и ако је могуће конструисати правилни p -тоугао, онда је p Фермаов прост број, тј. прост број облика $p = 2^{2^n} + 1$ за неко $n \geq 0$. Посебно, није могуће конструисати правилни седмоугао, нити правилни једанаестоугао.*

 Посматрамо полином

$$a(X) = X^{p-1} + X^{p-2} + \dots + X + 1.$$

По претпоставци је број $\zeta = e^{\frac{2\pi i}{p}}$ конструктибилан ($1, \zeta, \dots, \zeta^{p-1}$ чине темења правилног p -тоугла). Како је $\zeta^p = 1$ и, још је $\zeta \neq 1$, то је $a(\zeta) = 0$. Показали смо да је полином $a(X) \in \mathbb{Q}[X]$ нерастављив. Стога је он минимални полином елемента ζ и $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg a(X) = p - 1$. Како је ζ конструктибилан број, добијамо да је $p - 1 = 2^m$ за неки природан број m . Нека је $m = 2^n(2l + 1)$ за неке $n \geq 0$ и $l \geq 0$. Ако $l \neq 0$, онда је

$$p = 2^m + 1 = 2^{2^n(2l+1)} + 1 = (2^{2^n} + 1)(2^{2^n 2l} - 2^{2^n(2l-1)} + \dots + 1),$$

те p не би био прост број. Стога мора бити $p = 2^{2^n} + 1$, за неко $n \geq 0$, тј. p је Фермаов прост број. 

Напомена. Ако је $F_n := 2^{2^n} + 1$, онда знамо да су ово прости бројеви за $n = \overline{0, 4}$. Нису познати други Фермаови прости бројеви. Посебно, за $n = 2$, имамо да је $F_2 = 17$. Гаус је доказао, када је имао 19 година, да је могуће

конструисати правилни 17-оугао (још од Еуклида је познато да је могуће конструисати правилни троугао и правилни петоугао) и то му је, по његовим речима, указало на то да је математика обећавајућа професија за њега.

Недостаје нам знања, али је штета да за крај не наведемо следећу теорему, мада је не можемо доказати. Наведимо само, пошто се у теорему спомиње степен броја 2, да се лако може конструисати правилан $2n$ -тоугао, ако је већ конструисан правилан n -тоугао: само је потребно наћи симетрале централних углова који одговарају страницама тог n -тоугла, а то свакако знамо да урадимо лењиром и шестаром.

Теорема 51. *Правилни n -тоугао могуће је конструисати ако и само ако је n облика: $n = 2^k p_1 \cdots p_s$, за неко $k > 0$, где су p_i различити Фермаови прости бројеви.* 