

Предавања из Алгебре 2 за академску 2023/24. годину

Зоран Петровић

Комутативни прстени са јединицом; основни резултати

У Алгебри 1 упознали смо се са појмом комутативних прстена са јединицом. Овде ипак понављамо те основне појмове.

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

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

Моноид означава структуру са једном бинарном операцијом која је асоцијативна и за коју постоји неутрални елемент. Неутрал за сабирање (операцију $+$ у прстену) у комутативном прстену A означавамо са 0 (или понекад, због прецизности, са 0_A) и зовемо нулом прстена A , док неутрал за множење (операцију \cdot у прстену) означавамо са 1 (или понекад, због прецизности, са 1_A) и зовемо ЈЕДИНИЦОМ прстена A .

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

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

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

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

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

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

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

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

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

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

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

Наведимо неке примере комутативних прстена са јединицом:

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

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

$$U(\mathbb{Z}_n) = \Phi(n) .$$

Подсетимо се да је $\Phi(n)$ заправо скуп свих природних бројева између 1 и n који су узајамно прости са n . А из Дискретних структура 1 би требало да нам је познато да за сваки $x \in \Phi(n)$ постоји $y \in \Phi(n)$ такав да је $x \cdot y \equiv 1 \pmod{n}$, односно да је $x \cdot_n y = 1$. Дакле,

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

Приметимо да су операције у прстену \mathbb{Z}_6 сабирање и множење по модулу 6, те како је $2 \cdot_6 3 = 0$ видимо да производ два ненулта елемента у прстену ипак може бити једнак 0.

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

Став 3 У пољу нема правих делитеља нуле.

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

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

што противречи претпоставци $b \neq 0$. □

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

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

Став 5 Сваки коначан домен је поље.

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

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

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

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

Упутство: Погледајте доказ става 5. □

Дакле, сваки елемент у коначном прстену је или делитељ нуле или инвертибилан. Уколико скуп свих делитеља нуле у прстену A означимо

са $Z(A)$, овај резултат можемо кратко записати и на следећи начин. Ако је A коначан комутативан прстен са јединицом онда је

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

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

Дефиниција 8 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ комутативни прстени са јединицом при чему је $B \subseteq A$. Уколико је за све $x, y \in B$ испуњено:

$$x + y = x +' y, \quad x \cdot y = x \cdot' y$$

и $1_A = 1_B$, онда је B један потпрстен са јединицом прстена A .

Приметимо да такође важи и $0_A = 0_B$, но та се чињеница може извести из преосталих, што није тачно за једнакост $1_A = 1_B$. На пример, нека је $A = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ и $B = \{(0, 0), (1, 0)\}$, где су операције дефинисане по координатама, а на свакој координати су сабирање, односно множење по модулу 2. Тада B јесте комутативан прстен са јединицом, но јединица у B је елемент $(1, 0)$, а јединица у A је $(1, 1)$. Стога B није потпрстен са јединицом прстена A .

Важнији од појма потпрстена је појам ИДЕАЛА.

Дефиниција 9 Нека је A комутативан прстен са јединицом и I непразан подскуп од A . Тада је I ИДЕАЛ у A уколико

1. за све $x, y \in I$: $x + y \in I$;
2. за све $a \in A$ и $x \in I$: $a \cdot x \in I$.

Приметимо да $0 \in I$ за сваки идеал I . Наиме, како је I непразан, то постоји $x \in I$. Но, тада је и $0 = 0 \cdot x \in I$. Ознака $I \triangleleft A$ означава да је I идеал у A .

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

Дефиниција 10 Нека су I и J идеали прстена A .

1. $I + J := \{x + y : x \in I, y \in J\}$;
2. $I \cdot J := \{x_1 y_1 + \dots + x_n y_n : x_r \in I, y_s \in J \text{ за све } n \geq 1, r, s \in \{1, \dots, n\}\}$.

Директна провера показује да су $I + J$ и $I \cdot J$ заиста идеали у прстену A . Приметимо да је $I \cdot J$ заправо најмањи идеал који садржи све могуће производе елемената из I са елементима из J .

Као и у случају подгрупа, пресек два идеала $I \cap J$ јесте идеал, док је њихова унија $I \cup J$ идеал ако и само ако је један од тих идеала садржан

у другом. Заправо, ако посматрамо само операцију сабирања, приметимо да су идеали подгрупе групе $(A, +)$, а знамо да из чињенице да је унија две подгрупе подгрупа, следи да је једна од њих садржана у другој. Други смер се лако проверава.

Наведимо неке примере.

Пример 11 Ако је A комутативан прстен са јединицом и $a \in A$ произвољан елемент, онда је

$$\langle a \rangle := \{r \cdot a : r \in A\},$$

идеал. Овај идеал назива се главни идеал генерисан елементом a .

Како је $r \cdot a + s \cdot a = (r + s) \cdot a$, као и $s \cdot (r \cdot a) = (sr) \cdot a$, видимо да је $\langle a \rangle$ заиста идеал у прстену A . ♣

Пример 12 Сваки идеал у \mathbb{Z} је облика $\langle m \rangle$ за неки природан број m .

Нека је $I \triangleleft \mathbb{Z}$. Како је $(I, +)$ подгрупа групе $(\mathbb{Z}, +)$, то на основу претходног знања о подгрупама групе \mathbb{Z} , добијамо да је $I = \langle m \rangle$. ♣

Напомена: Идеал $\langle m \rangle$ означава се и са $m\mathbb{Z}$ (скуп свих целобројних умножака броја m).

Пример 13 Нека су m и n позитивни цели бројеви. Одредити:

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

Пре свега, $\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle$ важи у сваком прстену и за све елементе a и b (проверите!). Стога је $\langle m \rangle \cdot \langle n \rangle = \langle mn \rangle$. На основу дефиниције:

$$\langle m \rangle + \langle n \rangle = \{mx + ny : x, y \in \mathbb{Z}\}.$$

Како ми знамо да је $\langle m \rangle + \langle n \rangle$ сигурно главни идеал, потребно је само одредити који је његов генератор. Но, није потребно много размишљања о томе. Из горње једнакости се просто намеће да је

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

где је $d = \text{NZD}(m, n)$. Пре свега, добро нам је познато да увек постоје $p, q \in \mathbb{Z}$ за које је $mp + nq = d$. Стога, $d \in \langle m \rangle + \langle n \rangle$, па мора бити и $\langle d \rangle \subseteq \langle m \rangle + \langle n \rangle$. Но, како $d \mid m$ и $d \mid n$, то постоје m_1 и n_1 такви да је $m = dm_1$ и $n = dn_1$. Уколико је $mx + ny$ произвољан елемент из $\langle m \rangle + \langle n \rangle$ добијамо:

$$mx + ny = dm_1x + dn_1y = d(m_1x + n_1y),$$

те закључујемо да $mx + ny \in \langle d \rangle$, те је заиста $\langle m \rangle + \langle n \rangle = \langle d \rangle$.

Одредимо још и $\langle m \rangle \cap \langle n \rangle$. Приметимо да $x \in \langle m \rangle \cap \langle n \rangle$ ако и само ако $m \mid x$ и $n \mid x$. Но, то управо значи да је $\langle m \rangle \cap \langle n \rangle = \langle \text{NZS}(m, n) \rangle$. ♣

Пример 14 Нека је K поље и $I \triangleleft K$. Тада је $I = \{0\}$, или је $I = K$.

Претпоставимо да је I идеал у K и да је $I \neq \{0\}$. То значи да идеал I садржи неки елемент $x \neq 0$. Уколико је a ма који елемент из K , добијамо да и a припада идеалу I . Наиме, како је I идеал, а $x \neq 0$, то постоји x^{-1} и елемент $(ax^{-1}) \cdot x$ мора припадати идеалу I , а јасно је да је тај елемент једнак елементу a . ♣

Пример 15 Нека је A ма који комутативан прстен са јединицом и $u \in U(A)$. Тада је $\langle u \rangle = A$.

Доказ се изводи на исти начин као у претходном примеру. ♣

Пређимо сада на појам хомоморфизма прстена.

Дефиниција 16 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ два комутативна прстена са јединицом. Функција $f: A \rightarrow B$ је хомоморфизам прстена уколико је $f(1_A) = 1_B$ и уколико за све $x, y \in A$ важи:

$$f(x + y) = f(x) +' f(y) \quad \text{и} \quad f(x \cdot y) = f(x) \cdot' f(y).$$

Пример 17 Функција $\rho_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$ задата са $\rho_n(x) := \rho(x, n)$, где је са $\rho(x, n)$ означен остатак при дељењу x са n , је један хомоморфизам прстена.

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

Дефиниција 18 Нека је $f: A \rightarrow B$ хомоморфизам комутативних прстена са јединицом. ЈЕЗГРО хомоморфизма f , у ознаци $\text{Ker}(f)$ дефинише се са:

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

Став 19 Нека је $f: A \rightarrow B$ хомоморфизам комутативних прстена са јединицом. Тада важи:

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

Доказ.

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

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

па $x + y \in \text{Ker}(f)$.

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

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

те $a \cdot x \in \text{Ker}(f)$.

б) Нека је J идеал у B и $x, y \in f^{-1}[J]$. То значи да је $f(x) \in J$ и $f(y) \in J$. Како је J идеал, закључујемо да и $f(x+y) = f(x) + f(y) \in J$. Дакле, $x+y \in f^{-1}[J]$.

Такође, уколико је $x \in f^{-1}[J]$ и $a \in A$, добијамо да је $f(a \cdot x) = f(a) \cdot f(x) \in J$, пошто $f(x) \in J$, а J је идеал. Закључујемо да $a \cdot x \in f^{-1}[J]$.

в) Нека су $u, v \in f[I]$. То значи да је $u = f(x)$ и $v = f(y)$ за неке $x, y \in I$. Како је I идеал, то је $x+y \in I$, а како је $u + v = f(x) + f(y) = f(x+y)$, закључујемо да је $u + v \in f[I]$.

Уколико је $u \in f[I]$, а $b \in B$, с обзиром да је по претпоставци f „на”, добијамо да постоји $a \in A$ тако да је $b = f(a)$. Осим тога је $u = f(x)$ за неко $x \in I$. Како је I идеал, $a \cdot x$ припада I , па је $b \cdot u = f(a) \cdot f(x) = f(a \cdot x)$ из $f[I]$. \square

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

У општем случају директна слика идеала не мора бити идеал. На пример, јасно је да функција $i: \mathbb{Z} \rightarrow \mathbb{Q}$ дефинисана са $i(x) = x$ за све $x \in \mathbb{Z}$, јесте хомоморфизам (то је инклузија прстена целих бројева у поље рационалних бројева). Но,

$$i[\langle 2 \rangle] = \{2m : m \in \mathbb{Z}\},$$

а то очигледно није идеал у \mathbb{Q} , пошто су, на основу раније доказаног, једини идеали у \mathbb{Q} : $\{0\}$ и \mathbb{Q} .

Пример 20 Нека је $n \geq 2$ цео број. Тада је сваки идеал у \mathbb{Z}_n главни.

Искористићемо хомоморфизам $\rho_n: \mathbb{Z} \rightarrow \mathbb{Z}_n$, који је и „на”. Нека је $J \triangleleft \mathbb{Z}_n$. Тада је $\rho_n^{-1}[J] \triangleleft \mathbb{Z}$. На основу структуре идеала прстена \mathbb{Z} , знамо да постоји $m \geq 0$ такав да је $\rho_n^{-1}[J] = \langle m \rangle$. Но, тада је

$$J = \rho_n[\rho_n^{-1}[J]] = \rho_n[\langle m \rangle] = \langle \rho_n(m) \rangle.$$

Приметимо да једнакост $J = \rho_n[\rho_n^{-1}[J]]$ следи из чињенице да је ρ_n „на”, док је јасно да је

$$f[\langle a \rangle] = \langle f(a) \rangle$$

за сваки епиморфизам (хомоморфизам који је „на”) $f: A \rightarrow B$, произвољне прстене A, B и сваки елемент $a \in A$.

\subseteq . Нека $c \in \langle a \rangle$. Тада је $c = ra$ за неко $r \in A$, па је $f(c) = f(ra) = f(r)f(a) \in \langle f(a) \rangle$.

\supseteq . Ако је $w \in \langle f(a) \rangle$, онда је $w = df(a)$ за неки $d \in B$. Но, како је f „на”, то постоји $u \in A$ тако да је $d = f(u)$. Тада је $w = f(u)f(a) = f(ua) \in f[\langle a \rangle]$, јер $ua \in \langle a \rangle$. \clubsuit

Напомена. Можда је читалац приметио да смо овај резултат могли да докажемо као и у случају прстена целих бројева. Наиме, сваки идеал у

\mathbb{Z}_n је и подгрупа цикличне групе, па је тиме и сама циклична. А знамо како изгледају цикличне подгрупе групе \mathbb{Z}_n . У овом доказу само треба обратити пажњу на чињеницу да је свака подгрупа од \mathbb{Z}_n заиста идеал (у случају прстена \mathbb{Z} , то је тривијално испуњено, пошто се множење елементима из \mathbb{Z} заправо своди на сабирање (уз евентуално множење са -1 које одговара тражењу супротног елемента)). Чињеница да је то испуњено и за \mathbb{Z}_n захтева мали доказ. Размислите мало о томе.

Пример 21 Навести пример комутативног прстена са јединицом и подгрупе адитивне групе тог прстена, која није идеал.

Посматрамо прстен $A = \mathbb{Z}_2 \times \mathbb{Z}_2$. Овде су операције дефинисане по координатама и заправо је A директан производ прстена \mathbb{Z}_2 и \mathbb{Z}_2 . Скуп $\{(0,0), (1,1)\}$ је подгрупа адитивне групе тог прстена, али није идеал пошто елемент $(1,0) \cdot (1,1) = (1,0)$ не припада том скупу, а $(1,1)$ му припада. ♣

Пример 22 Наћи све идеале у прстену \mathbb{Z}_{12} .

Знамо да су сви идеали у овом прстену главни. Такође знамо да је сваки елемент у \mathbb{Z}_{12} или делитељ нуле или инвертибилан. Како сваки инвертибилан елемент генерише, према једном од раније наведених примера, цео прстен, остаје да се види које идеале генеришу делитељи нуле. Приметимо да је $m \in \mathbb{Z}_{12}$ делитељ нуле ако и само ако $2 \mid m$ или $3 \mid m$ (зашто?). Стога је

$$Z(\mathbb{Z}_{12}) = \{0, 2, 3, 4, 6, 8, 9, 10\}.$$

Приметимо да, пошто је $5 \in U(\mathbb{Z}_{12})$ и $10 = 5 \cdot_{12} 2$ имамо да је $\langle 10 \rangle = \langle 2 \rangle$ (размислите како се ово може генерализовати). Такође је $9 = -3 = (-1) \cdot 3$, па је и $\langle 9 \rangle = \langle 3 \rangle$. Добијамо да је и $\langle 8 \rangle = \langle 4 \rangle$.

С друге стране, $\langle 2 \rangle \neq \langle 4 \rangle$. Наиме, претпоставимо да $2 \in \langle 4 \rangle$. Тада би постојао $m \in \mathbb{Z}_{12}$ такав да је $2 = 4 \cdot_{12} m$. То би значило да постоји цео број q такав да је $2 = 4m + 12q$. Делењем са 2 добили бисмо да је $1 = 2m + 6q$ за неке целе бројеве m и q што свакако није могуће. Како је очигледно $4 \in \langle 2 \rangle$, то добијамо да је $\langle 4 \rangle \subset \langle 2 \rangle$ (идеал генерисан са 4 је прави подскуп идеала генерисаног са 2). На сличан начин се добија да је $\langle 6 \rangle \subset \langle 3 \rangle$. Читаоцима остављамо да се увере да су сви различити идеали прстена \mathbb{Z}_{12} следећи:

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

Прстен полинома — појам и конструкција

У курсу Алгебре 1 бавили смо се и прстеном полинома са једном неодређеном над комутативним прстеном са јединицом A , тј. прстеном $A[X]$. 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 знамо из средње школе. Уз додак 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.

Наведимо најпре дефиницију прстена полинома.

Дефиниција 23 Нека је A комутативни прстен са јединицом. Под прстеном полинома над прстеном A и 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 неко $n \geq 0$ и неке $a_i \in A'$.

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 уверити се да је и F изоморфизам.

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 уверити.

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) при чему можемо сматрати да су све то елементи из A . Но, различитим полиномима одговарају низови различите дужине. Са $A^{\mathbb{N}}$ је природно означити скуп свих низова (a_0, a_1, \dots) елемената из A . Но, нас не занимају сви такви низови, но 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 задати и операције на скупу A^ω . Сабирање се лако задаје:

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

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.

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 комутативан 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 $n \geq 1$

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

Подсетимо 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 елемент a налази на позицији n (дакле на $n + 1$ ом месту, пошто индекси почињу са 0).

Сада можемо видети како се може изразити 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

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

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

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

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 прстена $f: A \rightarrow A^\omega$, 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 A^ω заиста задовољава све услове који се захтевају од прстена 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 .

Ми ћемо се у даљем углавном бавити прстеном полинома над неким пољем. Но, нећемо се фокусирати само на једну неодређену. Нека је K неко поље. Уколико за A узмемо прстен $K[X]$, онда имамо и прстен $A[Y]$, где је Y нова неодређена. Тако се и добија прстен полинома са две неодређене: $K[X, Y] = K[X][Y]$. Јасно је да рекурзијом можемо задати прстен $K[X_1, \dots, X_n]$ за ма које $n \geq 1$.

Еуклидско дељење

Уколико је $0 \neq a(X) = a_0 + a_1X + \dots + a_nX^n \in K[X]$ 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 чему сматрамо да је $n + (-\infty) = (-\infty) + n = -\infty = (-\infty) + (-\infty)$. Ова конвенција нам мало скраћује запис неких резултата.

Формулишимо одмах теорему о дељењу са остатком, тј. о Еуклидском дељењу.

Теорема 24 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 $r(X) = a(X)$: $a(X) = 0 \cdot b(X) + a(X)$ 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 $a(X) = a_nX^n + \dots + a_1X + a_0$, а $b(X) = b_mX^m + \dots + b_1X + b_0$, при чему је $n \geq m$. Знамо како се дељење изводи: пореде се a_nX^n и b_mX^m и први члан у количнику је заправо $\frac{a_n}{b_m}X^{n-m}$. Хајде да уведемо ознаке које ће нам користити и касније. Водећи моном у полиному $a(X)$ је a_nX^n и то записујемо овако: $LM(a(X)) = a_nX^n$, или још краће: $LM(a) = a_nX^n$. Водећи коефицијент је a_n и то записујемо овако: $LC(a) = a_n$. Слично је $LM(b) = b_mX^m$ и $LC(b) = b_m$. Сада формирамо нови полином $a_1(X)$, краће a_1 , са:

$$a_1 := a - \frac{LM(a)}{LM(b)}b.$$

Ово се може записати и овако:

$$a \xrightarrow{b} a_1,$$

и то нам је први пример *редукције* полинома. Полином a редукујемо (сводимо) на полином a_1 помоћу полинома b .

У сваком случају, како смо на овај начин елиминисали водећи моноом из полинома a , добијамо да је $\deg(a_1) < \deg(a)$ и према 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 $q = \frac{LM(a)}{LM(b)} + q_1$, а $r = r_1$. Овим смо доказали егзистенцију 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 25 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 наравно 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 $(X - \alpha) \mid a(X)$ (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

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

С обзиром да је K поље, следи да је $q(\alpha) = 0$ 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 26 Нека је $a(X) = X^2 + 5X + 6 \in \mathbb{Z}_{10}[X]$. Овај полином, који је степена 2 има бар три нуле: $a(2) = 4 + 10 + 6 = 0$, $a(3) = 9 + 15 + 6 = 0$, $a(7) = 49 + 35 + 6 = 0$.

Напомена 27 Наравно да овде имамо сабирање у прстену \mathbb{Z}_{10} и да је, на пример $35 = \underbrace{1 + \dots + 1}_{35}$. \diamond

Еуклидов алгоритам у прстену $K[X]$

Дефиниција 28 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 $d(X) \in K[X] \setminus \{0\}$ који задовољава следећа два услова.

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

Дакле, највећи заједнички делилац полинома није јединствено одређен, ако је $d(X)$ највећи заједнички делилац и $\alpha \in K \setminus \{0\}$, онда је и $\alpha d(X)$ највећи заједнички делилац. 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 29 Ако је $a_1(X) = q(X)a_2(X) + a_3(X)$, 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 $a_3(X)$ (зашто је то довољно?). Но, то је јасно: ако $b(X) \mid a_1(X)$ и $b(X) \mid a_2(X)$, онда $b(X) \mid (a_1(X) - q(X)a_2(X))$, тј. $b(X) \mid a_3(X)$. Слично, ако $b(X) \mid a_2(X)$ и $b(X) \mid a_3(X)$, онда $b(X) \mid (q(X)a_2(X) + a_3(X))$, тј. $b(X) \mid a_1(X)$. \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.

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

$$(1) \quad b(X) = q_1(X)r(X) + r_1(X), \quad -\infty < \deg(r_1(X)) < \deg(r(X))$$

$$(2) \quad r(X) = q_2(X)r_1(X) + r_2(X), \quad -\infty < \deg(r_2(X)) < \deg(r_1(X))$$

\vdots

$$(n-1) \quad r_{n-3}(X) = q_{n-1}(X)r_{n-2}(X) + r_{n-1}(X), \quad -\infty < \deg(r_{n-1}(X)) < \deg(r_{n-2}(X))$$

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

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

Дакле, $r_n(X)$ је последњи ненула остатак. Вишеструком применом претходне 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 $r_n(X) \mid r_{n-1}(X)$, закључујемо да је $r_n(X)$ највећи заједнички делилац полинома $a(X)$ и $b(X)$, те је

$$\text{NZD}(a(X), b(X)) = \frac{1}{LC(r_n(X))} r_n(X).$$

Рекосмо 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 да постоје $u(X), v(X) \in K[X]$ такви да је

$$\text{NZD}(a(X), b(X)) = u(X)a(X) + v(X)b(X). \quad (1)$$

Идеали се у прстену $K[X]$, где је K поље, лако описују.

Теорема 30 Нека је K поље. Тада је сваки идеал у прстену $K[X]$ главни, тј. генерисан је једним елементом.

Доказ. Нека је $I \triangleleft K[X]$. Уколико је $I = \{0\}$, он је генерисан елементом 0 и немамо шта да доказујемо. Претпоставимо да је $I \neq \{0\}$.

Докажимо да је $I = \langle \mu(X) \rangle$, где је $\mu(X)$ моничан полином најмањег степена који се налази у I . У ту сврху, нека је $a(X) \in I \setminus \{0\}$. Еуклидско дељење нам даје

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

Но, тада је $r(X) = a(X) - q(X)\mu(X) \in I$ и ако $r(X)$ не би било нула полином, полином $\frac{1}{LC(r(X))}r(X)$ би био моничан полином мањег степена од $\mu(X)$, који припада идеалу I , што противречи избору $\mu(X)$. Стога је $r(X) = 0$ и $\mu(X) \mid a(X)$. Према томе, $I \subseteq \langle \mu(X) \rangle$, а како је тривијално $\langle \mu(X) \rangle \subseteq I$, добијамо да је заиста $I = \langle \mu(X) \rangle$. \square

Пример 31 У прстену $\mathbb{Z}[X]$ постоји идеал који није главни.

Посматрајмо идеал I генерисан са два елемента 2 и X , $I = \langle 2, X \rangle$ (ознака $\langle S \rangle$ означава најмањи идеал (који увек постоји јер је пресек ма које колекције идеала идеал) који садржи скуп S ; у случају да је $S = \{x_1, \dots, x_n\}$ пишемо $\langle x_1, \dots, x_n \rangle$, уместо $\langle \{x_1, \dots, x_n\} \rangle$). Овај идеал сигурно није главни. Наиме, претпоставимо да је

$$\langle 2, X \rangle = \langle a(X) \rangle,$$

за неки полином $a(X)$. Како је $2 \in \langle a(X) \rangle$, то мора бити $2 = a(X) \cdot b(X)$ за неки полином $b(X)$. То значи да је $a(X)$ константан полином. Но, из чињенице да $X \in \langle a(X) \rangle$, следи да $a(X) \mid X$, па мора бити $a(X) = 1$, или $a(X) = -1$. То би значило да је $1 = 2p(X) + Xq(X)$ за неке полиноме $p(X), q(X) \in \mathbb{Z}[X]$. Но, заменом 0 уместо X добијамо да је тада $1 = 2p(0)$, те би следило да $\frac{1}{2} \in \mathbb{Z}$. Закључујемо да наведени идеал није главни. ♣

У прстену са више неодређених, чак и када су коефицијенти у пољу, није сваки идеал главни. Нека

$$f_1(X_1, \dots, X_n), \dots, f_k(X_1, \dots, X_n) \in K[X_1, \dots, X_n].$$

Тада је идеал $\langle f_1, \dots, f_k \rangle$, генерисан полиномима f_i :

$$\langle f_1, \dots, f_k \rangle = \{a_1 f_1 + \dots + a_k f_k : a_i \in K[X_1, \dots, X_n]\}.$$

Идеал $\langle X, Y \rangle \triangleleft K[X, Y]$ није главни. У супротном, претпоставимо да је $\langle X, Y \rangle = \langle a(X, Y) \rangle$, за неки полином $a(X, Y)$. Како је тада $X \in \langle a(X, Y) \rangle$, то је $X = a(X, Y)b(X, Y)$ за неки полином $b(X, Y) \in K[X, Y]$. Но, то би значило да је $a(X, Y)$ полином различит од нула полинома у коме се не појављује Y . На сличан начин се добија да се не појављује ни X , те је $a(X, Y)$ константан полином који није 0 . Но, тада је то инвертибилан елемент у прстену $K[X, Y]$, те је $\langle a(X, Y) \rangle = K[X, Y]$.

Оно што јесте тачно је да је сваки идеал у прстену $K[X_1, \dots, X_n]$, где је K поље, коначно генерисан, тј. за сваки идеал $I \triangleleft K[X_1, \dots, X_n]$, постоје $f_1, \dots, f_k \in I$ тако да је $I = \langle f_1, \dots, f_k \rangle$. Ово ћемо доказати нешто касније, сада ћемо се позабавити питањем како се одређује генератор за $\langle f_1(X), \dots, f_k(X) \rangle \neq \{0\}$ пошто знамо да овај идеал јесте генерисан једним елементом. Уколико је међу полиномима f_i неки нула полином, њега можемо избацити без последица из скупа генератора те ћемо у даљем претпоставити да су сви различити од нуле.

Појам највећег заједничког делиоца више од два полинома дефинише се на аналогни начин: то је полином који дели све њих, а и дељив је сваким полиномом који их дели. Напишите дефиницију у ‘духу’ дефиниције за два полинома. Размислите и зашто за коначан скуп полинома из $K[X]$ постоји њихов највећи заједнички делилац.

Став 32 Нека је K поље и $f_1(X), \dots, f_k(X) \in K[X] \setminus \{0\}$. Тада је

$$\langle f_1(X), \dots, f_k(X) \rangle = \langle \text{NZD}(f_1(X), \dots, f_k(X)) \rangle.$$

Доказ. Није тешко доказати (докажите то за вежбу) да је

$$\text{NZD}(f_1(X), \dots, f_{k-1}(X), f_k(X)) = \text{NZD}(\text{NZD}(f_1(X), \dots, f_{k-1}(X)), f_k(X)),$$

за $k \geq 2$ и произвољне полиноме $f_i(X) \in K[X] \setminus \{0\}$. Из једнакости (1) закључује се да највећи заједнички делилац свака два полинома припада идеалу који ти полиноми генеришу. Стога се индукцијом може доказати да

$$\text{NZD}(f_1(X), \dots, f_{k-1}(X), f_k(X)) \in \langle f_1(X), \dots, f_k(X) \rangle.$$

Но, како $\text{NZD}(f_1(X), \dots, f_{k-1}(X), f_k(X)) \mid f_i(X)$, за све i , добијамо да, $f_i(X) \in \langle \text{NZD}(f_1(X), \dots, f_k(X)) \rangle$, за све i , што и завршава доказ. \square

Количнички прстени

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

Дефиниција 33 Нека је $I \triangleleft A$. На A дефинишемо релацију конгруенције по модулу I са:

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

Проверимо да је ова релација заиста конгруенција.

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

Симетричност. Нека је $a \equiv b \pmod{I}$. То значи да $a - b \in I$, но, множењем са (-1) добијамо да $b - a = (-1)(a - b)$ припада I , па је $b \equiv a \pmod{I}$.

Транзитивност. Нека је $a \equiv b \pmod{I}$ и $b \equiv c \pmod{I}$. Дакле, $a - b \in I$ и $b - c \in I$. Но, тада је и

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

те је $a \equiv c \pmod{I}$.

Слагање са $+$. Нека је $a \equiv a' \pmod{I}$ и $b \equiv b' \pmod{I}$. Дакле, $a - a' \in I$ и $b - b' \in I$. Добијамо да је

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

Слагање са \cdot . Нека је $a \equiv a' \pmod{I}$ и $b \equiv b' \pmod{I}$. Дакле, $a - a' \in I$ и $b - b' \in I$. Добијамо да је

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

Приметимо да је класа еквиваленције елемента a заправо скуп

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

Скуп класа еквиваленције означавамо са A/I . На основу претходног добијамо да је структура $(A/I, +, \cdot)$ један комутативан прстен са јединицом где су операције $+$ и \cdot дефинисане са:

$$(a + I) + (b + I) := (a + b) + I, \quad (a + I) \cdot (b + I) := (a \cdot b) + I.$$

Наравно да неке од ових заграда нећемо увек записивати. Прстен A/I назива се КОЛИЧНИЧКИ ПРСТЕН ПРСТЕНА A ПО ИДЕАЛУ I .

Као и у случају група, важе и теореме о изоморфизмима за прстене. Наводимо само једну.

Теорема 34 (Теорема о изоморфизмима за прстене) Нека је $f: A \rightarrow B$ хомоморфизам комутативних прстена са јединицом. Тада је $\tilde{f}: A/\text{Ker}(f) \rightarrow \text{Im}(f)$ задато са:

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

изоморфизам комутативних прстена са јединицом.

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

Проверимо да је \tilde{f} хомоморфизам.

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

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

Јасно је да је \tilde{f} „на”. Остаје да се провери да је \tilde{f} „1-1”.

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

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

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

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

Пример 35 Нека је $I \triangleleft A$. Тада је $p: A \rightarrow A/I$ један епиморфизам. ♣

Пример 36 За све $n \geq 1$ важи: $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

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

Директан производ прстена; Кинеска теорема о остацима

Важна конструкција је и ДИРЕКТАН ПРОИЗВОД ПРСТЕНА. Она је наведена у следећој дефиницији.

Дефиниција 37 Нека су $(A_1, +^1, \cdot^1), \dots, (A_n, +^n, \cdot^n)$ комутативни прстени са јединицом. На Декартовом производу

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

задајемо структуру комутативног прстена са јединицом са:

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) := (a_1 +^1 b_1, \dots, a_n +^n b_n)$$

$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) := (a_1 \cdot^1 b_1, \dots, a_n \cdot^n b_n)$$

Приметимо да је $0_A = (0_{A_1}, \dots, 0_{A_n})$ и $1_A = (1_{A_1}, \dots, 1_{A_n})$.

Искористимо конструкцију директног производа за добијање неких нових занимљивих примера.

Пример 38 Посматрајмо полином $f(X) = X^2 + (5, 5)X + (6, 6) \in (\mathbb{Z} \times \mathbb{Z})[X]$. Он има следеће четири нуле: $(-2, -2), (-2, -3), (-3, -2), (-3, -3)$ што се може лако проверити. На пример:

$$\begin{aligned} (-2, -3)^2 + (5, 5)(-2, -3) + (6, 6) \\ = (4, 9) + (-10, -15) + (6, 6) = (0, 0) = 0_{\mathbb{Z} \times \mathbb{Z}} \quad \clubsuit \end{aligned}$$

Пример 39 Додатном модификацијом претходног примера можемо добити полином степена 2 који има бесконачно много нула. Посматрајмо полином: $g(X) = (1, 0)X^2 + (5, 0)X + (6, 0) \in (\mathbb{Z} \times \mathbb{Z})[X]$. Лако је проверити да је сваки елемент облика $(-2, m) \in \mathbb{Z} \times \mathbb{Z}$ нула овог полинома:

$$\begin{aligned} (1, 0)(-2, m)^2 + (5, 0)(-2, m) + (6, 0) \\ = (1, 0)(4, m^2) + (-10, 0) + (6, 0) = (4, 0) + (-10, 0) + (6, 0) = (0, 0). \quad \clubsuit \end{aligned}$$

Кренимо сада ка доказу Кинеске теореме о остацима.

Став 40 Нека су m_1, \dots, m_n позитивни цели бројеви за које је: $\text{NZD}(m_i, m_j) = 1$ за све $i \neq j$. Тада је

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

Доказ. Дефинишимо хомоморфизам

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

са:

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

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

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

Добијамо да је

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

Но, како је $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$, то је

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

Закључујемо да f мора бити „на”. Тиме смо добили тражени изоморфизам. \square

Последица 41 (Кинеска теорема о остацима) Нека су m_1, \dots, m_n позитивни цели бројеви који су пар по пар узајамно прости и x_1, \dots, x_n произвољни цели бројеви. Тада постоји цео број x такав да је

$$x \equiv x_1 \pmod{m_1}$$

$$x \equiv x_2 \pmod{m_2}$$

.....

$$x \equiv x_n \pmod{m_n}$$

Ако је x' неки други цео број који задовољава наведени систем конгруенција, онда је

$$x \equiv x' \pmod{m_1 \cdots m_n}.$$

Доказ. Посматрајмо елемент

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

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

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

но, то управо значи да је

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

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

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

као што је и тврђено. □

Став 42 Ако су прстени A и B изоморфни, онда је $(U(A), \cdot) \cong (U(B), \cdot)$

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

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

Став 43 Важи једнакост: $U(A_1 \times \cdots \times A_n) = U(A_1) \times \cdots \times U(A_n)$.

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

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

□

Теорема 44 Ако су m_1, \dots, m_n пар по пар узајамно прости позитивни цели бројеви, онда је

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

и

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

где је φ Ојлерова функција.

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

У произвољном прстену могуће је формулисати Кинеску теорему о остацима. Потребна нам је најпре једна дефиниција.

Дефиниција 45 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 **ако** су m и n узајамно прости. Отуд и терминологија.

Став 46 За копросте идеале I и J важи следећа једнакост: $I \cdot J = I \cap J$.

Доказ. Увек је $I \cdot J \subseteq I \cap J$. Наиме, ако је $a \in I$ и $b \in J$, онда $a \cdot b \in I$ пошто $a \in I$, а $a \cdot b \in J$, јер $b \in J$. Одатле следи да и сума таквих производа лежи у идеалу $I \cap J$. Дакле, потребно је доказати само обратну инклузију. Како су I и J копрости, то постоје $x \in I$ и $y \in J$ тако да важи $x + y = 1$. Нека је $z \in I \cap J$ произвољан елемент. Тада је

$$z = z \cdot 1 = z \cdot (x + y) = z \cdot x + z \cdot y.$$

Како $x \in I$ и $z \in J$, то је $z \cdot x \in I \cdot J$ (радимо са комутативним прстенима, па је $z \cdot x = x \cdot z$). Такође и $z \cdot y \in I \cdot J$, па закључујемо да и z припада пресеку $I \cap J$. \square

У \mathbb{Z} важи: $\langle m \rangle \cdot \langle n \rangle = \langle m \cdot n \rangle$, а $\langle m \rangle \cap \langle n \rangle = \langle \text{NZS}(m, n) \rangle$. Једнакост важи уколико су m и n узајамно прости, сасвим у складу са овим ставом.

Лема 47 Нека су идеали I и J копрости, као и идеали I и K . Тада су и идеали I и $J \cdot K$ копрости.

Доказ. Како су I и J копрости, тј. $I + J = A$, то постоје $x_1 \in I$ и $y \in J$ такви да је $x_1 + y = 1$. Слично, како су I и K копрости, постоје $x_2 \in I$ и $z \in K$ такви да је $x_2 + z = 1$. Множењем ове две једнакости добијамо $(x_1 + y) \cdot (x_2 + z) = 1$, тј.

$$x_1x_2 + x_1z + yx_2 + yz = 1.$$

Но, како $x_i \in I$, то $x_1x_2, x_1z, yx_2 \in I$, те и $x_1x_2 + x_1z + yx_2 \in I$, док из $y \in J, z \in K$, следи да $yz \in J \cdot K$. Дакле,

$$1 = \underbrace{x_1x_2 + x_1z + yx_2}_{\in I} + \underbrace{yz}_{\in J \cdot K} \in I + J \cdot K.$$

Како $1 \in I + J \cdot K$, то је $I + J \cdot K = A$. \square

Теорема 48 (Кинеска теорема о остацима) Нека су идеали I_1, \dots, I_n комутативног прстена са јединицом A пар по пар узајамно прости. Тада важи изоморфизам:

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

Доказ. Доказ је нешто тежи него у случају прстена целих бројева. Посматрамо хомоморфизам $f: A \rightarrow A/I_1 \times \dots \times A/I_n$ дефинисан са:

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

Није тешко проверити да је ова функција заиста један хомоморфизам. Наиме:

$$\begin{aligned} f(x+y) &= ((x+y) + I_1, \dots, (x+y) + I_n) \\ &= ((x + I_1) + (y + I_1), \dots, (x + I_n) + (y + I_n)) \\ &= (x + I_1, \dots, x + I_n) + (y + I_1, \dots, y + I_n) \\ &= f(x) + f(y). \end{aligned}$$

На сличан начин се проверава да је $f(x \cdot y) = f(x) \cdot f(y)$. Такође је $f(1_A) = (1_A + I_1, \dots, 1_A + I_n) = (1_{A/I_1}, \dots, 1_{A/I_n}) = 1_{A/I_1 \times \dots \times A/I_n}$.

Јасно је да је језгро овог хомоморфизма пресек свих идеала. Једино треба проверити да је f „на”.

Из леме 47 следи да је за свако $i = \overline{1, n}$ испуњено:

$$I_i \text{ и } \prod_{j \neq i} I_j \text{ су копрости.}$$

Наравно са $\prod_{j \neq i} I_j$ смо означили производ свих идеала I_j за $j \neq i$.

Дакле, за $i = \overline{1, n}$, постоје $a_i \in I_i$ и $b_i \in \prod_{j \neq i} I_j$ такви 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 $j \neq i$.

Докажимо сада да је f „на”. Нека је $(x_1 + I_1, \dots, x_n + I_n)$ произвољни елемент из $A/I_1 \times \dots \times A/I_n$. Уочимо елемент $x = b_1 x_1 + \dots + b_n x_n$, где су b_i претходно изабрани елементи. Тада је, за све i :

$$x = b_1 x_1 + \dots + b_i x_i + \dots + b_n x_n \equiv 0 \cdot x_1 + \dots + 1 \cdot x_i + \dots + 0 \cdot x_n \pmod{I_i}.$$

Дакле, за све $i = \overline{1, n}$: $x \equiv x_i \pmod{I_i}$, а то управо значи да је

$$f(x) = (x_1 + I_1, \dots, x_n + I_n).$$

Закључујемо да је f заиста „на”. □

С обзиром да је $I \cdot J = I \cap J$ за копросте I, J , индукцијом се може показати да је за пар по пар копростих I_1, \dots, I_n : $I_1 \cap \dots \cap I_n = I_1 \cdot \dots \cdot I_n$. Дакле, у том случају имамо да је $A/I_1 \cdot \dots \cdot I_n \cong A/I_1 \times \dots \times A/I_n$.

Прости и максимални идеали

Започнимо ову тему следећим ставом.

Став 49 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 је $I \subseteq P$ или је $J \subseteq P$.
2. За $a, b \in A$ важи: ако $ab \in P$, онда $a \in P$ или $b \in P$.
3. Прстен A/P је област целих (домен).

Доказ. Подсетимо се најпре да се област целих дефинише као комутативан прстен са јединицом у коме нема правих делитеља нуле, тј. у коме важи: ако је $ab = 0$, онда је $a = 0$ или $b = 0$.

$1 \implies 2$. Уочимо идеале $I = \langle a \rangle$, $J = \langle b \rangle$. Како је $I \cdot J = \langle ab \rangle$ и $ab \in P$, то $I \cdot J \subseteq P$. На основу 1. следи да $I \subseteq P$, или $J \subseteq P$, тј. $a \in P$, или $b \in P$.

$2 \implies 3$. Претпоставимо да за елементе $x, y \in A/P$ важи: $xy = 0_{A/P}$. Наравно, $0_{A/P} = P$. Како су x и y елементи из количничког прстена, то постоје $a, b \in A$ такви да је $x = a + P$ и $y = b + P$ и да важи: $(a + P)(b + P) = P$. Ова једнакост се своди на $ab + P = P$, тј. на $ab \in P$. На основу 2. добијамо да $a \in P$, или $b \in P$, односно $a + P = P$ или $b + P = P$, тј. $x = 0$, или $y = 0$.

$3 \implies 1$. Нека су идеали I, J прстена A такви да је $I \cdot J \subseteq P$, а да $I \not\subseteq P$ и $J \not\subseteq P$. То значи да постоји $a \in I \setminus P$ и $b \in J \setminus P$. Но, $ab \in I \cdot J \subseteq P$, па је $(a + P)(b + P) = ab + P = P$. Како је A/P област целих, следи да је $a + P = P$, или $b + P = P$, односно $a \in P$ или $b \in P$. Ова контрадикција завршава доказ. \square

Дефиниција 50 Идеал $P \triangleleft A$ је прост уколико испуњава неко од претходна три еквивалентна својства.

Пример 51 Идеал $\langle 2, 1 - \sqrt{-5} \rangle \triangleleft \mathbb{Z}[\sqrt{-5}]$ је прост идеал.

Покажимо да је $\mathbb{Z}[\sqrt{-5}] / \langle 2, 1 - \sqrt{-5} \rangle \cong \mathbb{Z}_2$. Приметимо да је сваки елемент у прстену $\mathbb{Z}[\sqrt{-5}]$ облика $m + n\sqrt{-5}$ за неке целе бројеве m и n . Дефинишимо пресликавање $f: \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{Z}_2$ са:

$$f(m + n\sqrt{-5}) = \rho(m + n, 2).$$

Покажимо да је ово пресликавање хомоморфизам прстена.

$$\begin{aligned} f((m + n\sqrt{-5}) + (r + s\sqrt{-5})) &= f((m + n) + (r + s)\sqrt{-5}) \\ &= \rho((m+n) + (r+s), 2) = \rho(m+n, 2) +_2 \rho(r+s, 2) = f(m+n\sqrt{-5}) +_2 f(r+s\sqrt{-5}). \end{aligned}$$

$$\begin{aligned}
f((m+n\sqrt{-5})(r+s\sqrt{-5})) &= f(mr-5ns+(ms+nr)\sqrt{-5}) \\
&= \rho(mr-5ns+ms+nr, 2) = \rho(mr+ns+ms+nr, 2) = \rho((m+n)(r+2), 2) \\
&= \rho(m+n, 2) \cdot_2 \rho(r+s, 2) = f(m+n\sqrt{-5}) \cdot_2 f(r+s\sqrt{-5}).
\end{aligned}$$

Наравно, $f(1) = 1$. Јасно је да је f „на”. Треба одредити језгро овог хомоморфизма. Но, $m+n\sqrt{-5} \in \text{Ker } f$ **ако** $2 \mid (m+n)$. Но,

$$m+n\sqrt{-5} = m-n(-\sqrt{-5}) = m-n(1-\sqrt{-5}-1) = (m+n) - n(1-\sqrt{-5}).$$

Стога, ако је $m+n$ паран број, онда је $m+n = 2t$ за неко $t \in \mathbb{Z}$ и на основу горње једнакости $m+n\sqrt{-5} \in \langle 2, 1-\sqrt{-5} \rangle$. Обратно, ако $m+n\sqrt{-5} \in \langle 2, 1-\sqrt{-5} \rangle$, онда је

$$\begin{aligned}
m+n\sqrt{-5} &= (a+b\sqrt{-5}) \cdot 2 + (c+d\sqrt{-5}) \cdot (1-\sqrt{-5}) \\
&= 2a+2b\sqrt{-5}+c-c\sqrt{-5}+d\sqrt{-5}+5d = (2a+c+5d) + (2b-c+d)\sqrt{-5},
\end{aligned}$$

за неке $a, b, c, d \in \mathbb{Z}$. Тада је

$$m+n = 2a+c+5d+2b-c+d = 2a+2b+6d,$$

па је $m+n$ паран број. Добили смо да је $\text{Ker } f = \langle 2, 1-\sqrt{-5} \rangle$ и на основу теореме о изоморфизму прстена добијамо тражени изоморфизам. Како је \mathbb{Z}_2 област целих, закључујемо да је идеал $\langle 2, 1-\sqrt{-5} \rangle$ прост. ♣

Приметимо да, 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 $i \in \{1, \dots, n\}$ (што се лако доказује индукцијом по n).

Пређимо сада на појам максималног идеала.

Дефиниција 52 Идеал M прстена A је максималан, уколико не постоји идеал I прстена A за који важи: $M \subset I \subset A$.

Дакле, максималан идеал је прави идеал за који не постоји прави идеал, различит од њега, који га садржи као свој подскуп.

Став 53 Нека је M прави идеал прстена A . Тада је M максималан идеал ако и само ако је A/M поље.

Доказ. Претпоставимо да је M максималан идеал и $a+M \neq M$. Треба показати да $a+M$ има инверз у прстену A/M . Посматрамо идеал $\langle a \rangle + M$. Како $a \notin M$, то је M прави подскуп од $\langle a \rangle + M$. Но, с обзиром да је M максималан идеал, мора бити $\langle a \rangle + M = A$. То значи да постоје $b \in A$ и $t \in M$ за које је $ab+t = 1$. Дакле, $ab-1 = t \in M$, па је $ab+M = 1+M$, те је $b+M$ тражени инверз елемента $a+M \in M$.

Обратно, претпоставимо да је A/M поље. Нека је M прави подскуп идеала I . Дакле, постоји $a \in I \setminus M$. Стога је $a+M \neq M$ у количничком прстену A/M . Како је овај прстен по претпоставци поље, то постоји

$b \in M$ тако да је $(a + M)(b + M) = 1 + M$, односно, $ab - 1 \in M$. Дакле, за неко $m \in M$ важи: $ab - 1 = m$, тј. $1 = ab - m$. Како и a и m припадају идеалу I , то и $1 \in I$, па мора бити $I = A$. Закључујемо да је M заиста максималан идеал у A . \square

Напомена 54 Видимо да из овог става следи да је сваки максималан идеал уједно и прост идеал, пошто у пољу нема правих делитеља нуле. \diamond

У основној школи смо научили да је природан број прост уколико нема других делилаца сем 1 и њега самог (ово такође важи и за број 1, али се он не сматра простим бројем). Но, у произвољној области целих разликује се појам простог и нерастављивог елемента. Подсетимо се да са $U(A)$ означавамо скуп свих инвертибилних елемената у прстену A .

Дефиниција 55 Нека је A област целих. Елемент $p \in A \setminus (U(A) \cup \{0\})$ је

- ПРОСТ, уколико за $a, b \in A$ важи: ако $p \mid ab$, онда $p \mid a$, или $p \mid b$;
- НЕРАСТАВЉИВ (АТОМ) уколико за $a, b \in A$ важи: ако је $p = ab$, онда је $a \in U(A)$, или $b \in U(A)$.

Веза између простих и нерастављивих елемената у произвољном прстену дата је следећим ставом.

Став 56 Нека је A домен. Тада је сваки прост елемент у A нерастављив.

Доказ. Претпоставимо да је p прост и да је $p = ab$. Посебно то значи да p дели производ ab . Како је p прост, то $p \mid a$, или $p \mid b$. Нека, на пример, $p \mid a$. То значи да постоји $c \in A$ за који је $a = pc$. Како је $p = ab$, то је $p = pcb$, тј. $p(1 - cb) = 0$, па мора бити $1 - cb = 0$, пошто је A област целих. Дакле, $cb = 1$, те је елемент b инвертибилан. \square

У произвољном домену, прости и нерастављиви елементи се разликују. Размотримо следећи пример.

Пример 57 У прстену $\mathbb{Z}[\sqrt{-5}]$ елемент 3 је нерастављив, али није прост.

Пре свега,

$$\mathbb{Z}[\sqrt{-5}] := \{p(\sqrt{-5}) : p \in \mathbb{Z}[X]\}.$$

Но, није тешко уверити се да из дефиниције следи да је

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Уверимо се најпре да је 3 нерастављив. Претпоставимо да је $3 = uv$. Уведимо ознаку $N(z) := z\bar{z}$, за $z \in \mathbb{Z}[\sqrt{-5}]$ (наравно да је $N(z)$ квадрат модула комплексног броја z). Јасно је да је $N(z_1 z_2) = N(z_1)N(z_2)$ за све z_1, z_2 . Добијамо да је $N(3) = N(u)N(v)$, односно $9 = N(u)N(v)$.

Ово је факторизација природног броја 9 у скупу природних бројева, то имамо две могућности:

1) један од $N(u)$, $N(v)$ једнак је 1, а други 9;

2) $N(u) = N(v) = 3$.

1) Претпоставимо, на пример, да је $N(u) = 1$. Уколико је $u = a + b\sqrt{-5}$, добијамо да је $1 = N(u) = u\bar{u} = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$. С обзиром да $a, b \in \mathbb{Z}$, ово је могуће једино ако је $b = 0$ и $a \in \{-1, 1\}$, тј. $u \in \{-1, 1\}$, те следи да је u инвертибилан (било би добро да читаоци сами покажу, за вежбу, да је $U(\mathbb{Z}[\sqrt{-5}]) = \{-1, 1\}$ користећи функцију N).

2) Поступамо на сличан начин. Уколико је $u = a + b\sqrt{-5}$, добијамо да је $3 = N(u) = a^2 + 5b^2$. С обзиром да $a, b \in \mathbb{Z}$, мора бити $b = 0$ и добијамо да је $3 = a^2$, за неко $a \in \mathbb{Z}$. Ово наравно није могуће, те закључујемо да се случај 2) и не појављује.

Дакле, из чињенице да је $3 = uv$, добијамо да је један од фактора инвертибилан, а то заправо значи да је 3 нерастављив.

Остаје да покажемо да 3 није прост. Посматрајмо факторизацију броја 9 у $\mathbb{Z}[\sqrt{-5}]$:

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Како је $9 = 3 \cdot 3$, то

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

Покажимо да 3 не дели ниједан од ових фактора. Из те чињенице ће следити да 3 није прост.

Нека $3 \mid (2 + \sqrt{-5})$ (аналогно се разматра и други случај). Дакле, за неки елемент $u \in \mathbb{Z}[\sqrt{-5}]$:

$$3 \cdot u = 2 + \sqrt{-5}.$$

Применом функције N добијамо

$$9 \cdot N(u) = 9.$$

Добијамо да је $N(u) = 1$, те је $u \in \{-1, 1\}$, тј. $3 = 2 + \sqrt{-5}$, или $3 = -(2 + \sqrt{-5})$. Ова контрадикција нам показује да 3 не дели $2 + \sqrt{-5}$, тј. 3 заиста није прост. ♣

Напомена 58 Приметимо да једнакост $3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ даје две различите факторизације броја 9 у производ нерастављивих. То је нешто са чиме се нисмо срели у случају целих бројева. Више ћемо о овоме рећи у наредним предавањима. ◇

Следећи став је помало и очекиван.

Став 59 Елемент је прост ако и само ако је идеал генерисан тим елементом прост идеал.

Доказ. Нека је p прост елемент у прстену A и $\langle p \rangle$ идеал генерисан тим елементом. Уколико $ab \in \langle p \rangle$, онда је $ab = pc$ за неки $c \in A$, тј. $p \mid ab$. Како је елемент p прост, то $p \mid a$, или $p \mid b$, односно, $a \in \langle p \rangle$, или $b \in \langle p \rangle$, те закључујемо да је $\langle p \rangle$ прост идеал.

Обратно, претпоставимо да је $\langle p \rangle$ прост идеал и нека $p \mid ab$. То значи да $ab \in \langle p \rangle$, те следи да $a \in \langle p \rangle$, или $b \in \langle p \rangle$, односно $p \mid a$, или $p \mid b$. \square

Претходни део је за први колоквијум.

Напомена 60 Као што смо доказали да 3 није прост, можемо доказати да ни 2 није прост. Стога идеал $\langle 2 \rangle$ није прост. Но, важи једнакост

$$\langle 2 \rangle = \langle 2, 1 - \sqrt{-5} \rangle \langle 2, 1 + \sqrt{-5} \rangle.$$

Наиме, лако је видети да је генерално тачно да је $\langle a, b \rangle \langle c, d \rangle = \langle ac, ad, bc, bd \rangle$. Стога је

$$\langle 2, 1 - \sqrt{-5} \rangle \langle 2, 1 + \sqrt{-5} \rangle = \langle 4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6 \rangle,$$

но, 2 припада овом идеалу као разлика $6 - 4$, а сви остали елементи су умношци од 2. Стога је тај идеал заправо $\langle 2 \rangle$. Као што смо доказали да је идеал $\langle 2, 1 - \sqrt{-5} \rangle$ прост идеал, може се доказати да је то и идеал $\langle 2, 1 + \sqrt{-5} \rangle$. Дакле, мада идеал $\langle 2 \rangle$ није прост, он ипак има факторизацију на производ простих идеала. Заправо, тачно је, мада ми нећемо то овде доказивати, да сваки идеал у прстену $\mathbb{Z}[\sqrt{-5}]$ има јединствену, до на редослед фактора, факторизацију у облику простих идеала! Према томе, мада елементи немају јединствену факторизацију, преласком на идеале добијамо јединствену факторизацију. Посебно то важи за главне идеале. Видимо сада зашто нам је корисна аритметика идеала. \diamond

Веза између нерастављивих елемената и максималних идеала дата је следећим ставом.

Став 61 Елемент $a \in A$ је нерастављив ако и само ако је идеал $\langle a \rangle$ максималан у скупу свих главних идеала прстена A .

Доказ. Претпоставимо да је $a \in A$ нерастављив и нека је $\langle a \rangle \subseteq \langle b \rangle$. Треба да покажемо да је $\langle a \rangle = \langle b \rangle$ или $\langle b \rangle = A$. Како је $\langle a \rangle \subseteq \langle b \rangle$, то $a \in \langle b \rangle$, па постоји $c \in A$ тако да је $a = bc$. Како је a нерастављив, то $b \in U(A)$, или $c \in U(A)$. Уколико $b \in U(A)$, онда је $\langle b \rangle = A$, а ако $c \in U(A)$, онда је $\langle a \rangle = \langle b \rangle$.

Обратно, претпоставимо да је $\langle a \rangle$ максималан у скупу свих главних идеала прстена A . Нека је $a = bc$ и претпоставимо да $c \notin U(A)$. То значи да је $a \in \langle b \rangle$, али да $b \notin \langle a \rangle$ (зашто?), тј. да је $\langle a \rangle$ прави подскуп

идеала $\langle b \rangle$. Како је $\langle a \rangle$ максималан у скупу свих главних идеала, то мора бити $\langle b \rangle = A$, тј. постоји $c \in A$ тако да је $bc = 1$, те закључујемо да је b инвертибилан. \square

Максималан идеал у сваком комутативном прстену са јединицом постоји. Заправо, важи следећа теорема, коју нећемо доказивати.

Теорема 62 Нека је I прави идеал у комутативном прстену са јединицом A . Тада постоји максималан идеал M за који је $I \subseteq M$.

Посебно је занимљив случај прстена у којима постоји тачно један максимални идеал.

Став 63 У комутативном прстену са јединицом A постоји тачно један максималан идеал ако и само ако је $A \setminus U(A)$ идеал.

Доказ. Приметимо да важи следеће. Идеал $I \triangleleft A$ је прави ако I не садржи ниједан инвертибилан елемент (видети пример 15).

Претпоставимо да у прстену постоји тачно један максималан идеал M . Према претходном је $U(A) \subseteq A \setminus M$. Но, ако постоји $a \in A \setminus M$ који није инвертибилан, онда је идеал $\langle a \rangle$ прави, па је према теорему 62 $\langle a \rangle$ садржан у неком максималном, а како је M једини такав, то је $\langle a \rangle \subseteq M$, што није могуће, јер $a \notin M$.

Обратно, нека у прстену A сви неинвертибилни елементи чине идеал M : $A \setminus U(A) = M$. Но, тада је и сваки други идеал I садржан у M , јер је $I \cap U(A) = \emptyset$, као што смо горе приметили. Стога је M максималан идеал и то једини такав. \square

Дефиниција 64 Комутативан прстен са јединицом у коме постоји тачно један максимални идеал назива се ЛОКАЛНИ ПРСТЕН.

Пример 65 Нека је $p \in \mathbb{N}$ прост број. Тада је прстен $\mathbb{Z}_{(p)}$ дефинисан са:

$$\mathbb{Z}_{(p)} := \left\{ \frac{a}{b} : p \nmid b \right\}$$

локални.

Треба само показати да неинвертибилни елементи чине идеал. Приметимо да $\frac{a}{b} \in U(\mathbb{Z}_{(p)})$ **ако** $p \nmid a$. Дакле, $\frac{a}{b} \notin U(\mathbb{Z}_{(p)})$ **ако** $p \mid a$. Но, то управо значи да је скуп свих неинвертибилних елемената у овом прстену скуп свих умножака броја p , тј. идеал генерисан са p . \clubsuit

Пример 66 Нека је A задат са:

$$A = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} : a, b \in \mathbb{Q} \right\}.$$

Показати да је A комутативни прстен са јединицом у односу на множење и сабирање матрица и да је A пример локалног прстена.

Није тешко проверити да је A комутативан прстен са јединицом, као и да је матрица из $\begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \in A$ инвертибилна **акко** је $a \neq 0$. Дакле,

$$A \setminus U(A) = \left\{ \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix} : b \in \mathbb{Q} \right\}.$$

Но,

$$\left\langle \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \right\rangle = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Q} \right\} = \left\{ \begin{bmatrix} 0 & a \\ 0 & 0 \end{bmatrix} : a, b \in \mathbb{Q} \right\} = A \setminus U(A).$$

Дакле, неинвертибилни елементи чине главни идеал генерисан матрицом $\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$. ♣

Факторизација; локализација

Подсетимо се да је област целих (домен) комутативан прстен са јединицом у коме нема правих делитеља нуле, тј. у којима важи: за све $a, b \in A$ из $ab = 0$ следи $a = 0$, или $b = 0$. Сви прстени којима ћемо се бавити у овој лекцији биће домени.

Дефиниција 67 Два елемента $a, b \in A$ су ПРИДРУЖЕНА уколико постоји елемент $u \in U(A)$ такав да је $a = ub$.

Јасно је да је придруженост елемената једна релација еквиваленције. Приметимо да ако је p нерастављив онда је то и сваки њему придружен елемент. Исто то важи и за просте елементе у домену.

Дефиниција 68 Домен A је домен са једнозначном факторизацијом уколико су испуњени следећи услови.

1. За сваки елемент из $a \in A \setminus (U(A) \cup \{0\})$ постоје нерастављиви елементи p_1, \dots, p_r такви да је $a = p_1 p_2 \cdots p_r$.
2. Ако је за нерастављиве елементе p_i, q_j :

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

онда је $r = s$ и постоји пермутација $\sigma \in \mathbb{S}_r$ тако да је за све $i = \overline{1, r}$ елемент p_i придружен елементу $q_{\sigma(i)}$.

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

Став 69 Домен A је домен са једнозначном факторизацијом акко се сваки елемент $a \in A \setminus (U(A) \cup \{0\})$ може приказати у облику производа простих елемената. Посебно, то значи да је сваки нерастављив елемент прост.

Доказ. Претпоставимо да се сваки неинвертибилан, ненула елемент може приказати у облику производа простих. Како су прости нерастављиви, потребно је само доказати да је приказ у облику производа јединствен (у горенаведеном смислу). Докажимо најпре да је, у овом случају, сваки нерастављив елемент прост.

Нека је q нерастављив елемент. По претпоставци, он се може написати у облику производа простих елемената: $q = p_1 \cdots p_r$, где су p_i прости. Но, како је q нерастављив, мора бити $r = 1$, тј. и сам q је прост.

Докажимо сада јединственост разлагања у облику производа нерастављивих елемената. Нека је

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

Доказ изводимо индукцијом по r . Случај $r = 1$ је тривијалан. Претпоставимо да је у горњој једнакости $r > 1$ и да су p_i, q_j нерастављиви. Према доказаном, p_1 је прост, па постоји $j_1 \in \{1, \dots, s\}$ тако да $p_1 \mid q_{j_1}$. Како је q_{j_1} нерастављив, добијамо да су p_1 и q_{j_1} придружени, тј. да постоји $u_1 \in U(A)$ за који је $q_{j_1} = u_1 p_1$. Горњу једнакост можемо скратити са p_1 и добити

$$p_2 \cdots p_r = q'_2 q_3 \cdots q_s,$$

где је $q'_2 = q_2 u_1$, који је такође нерастављив. Индуктивна хипотеза завршава доказ.

Обратно, претпоставимо да је A домен за једнозначном факторизацијом. Довољно је показати да је сваки нерастављив елемент прост. Нека је p нерастављив и нека $p \mid ab$. Треба показати да $p \mid a$, или $p \mid b$. Претпоставимо да p не дели ни a ни b . Нека је $a = p_1 \cdots p_r$ факторизација a на нерастављиве елементе и $b = q_1 \cdots q_s$ факторизација b на нерастављиве. Тада је

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

факторизација ab на нерастављиве. Како p дели ab , то је $ab = pc$ за неко c . И c има факторизацију на нерастављиве елементе, па је $c = z_1 \cdots z_l$ за неке нерастављиве z_1, \dots, z_l . Добијамо да је

$$p_1 \cdots p_r q_1 \cdots q_s = p z_1 \cdots z_l,$$

где су сви p_i, q_j, z_k и p нерастављиви. Како је, по претпоставци, A домен са једнозначном факторизацијом, то је p придружен неком од елемената из скупа $\{p_1, \dots, p_r, q_1, \dots, q_s\}$. Уколико је p придружен елементу p_i (за неко i), добијамо да $p \mid a$, а ако је p придружен неком q_j онда $p \mid b$. Наиме, лако се показује да важи следеће: ако је p придружен елементу q и ако $q \mid c$, онда и $p \mid c$. Овим је доказ завршен. \square

Знамо да је \mathbb{Z} домен за једнозначном факторизацијом. Показаћемо сада да је сваки главноидеалски домен уједно и домен са једнозначном факторизацијом.

Став 70 Доказати да у сваком главноидеалском домену за свака два елемента постоји њихов највећи заједнички делилац.

Доказ. Нека A један главноидеалски домен и $a, b \in A$. Уочимо идеал $\langle a, b \rangle$ генерисан елементима a и b . Како је у A сваки идеал главни, то је и $\langle a, b \rangle = \langle d \rangle$, за неки $d \in A$. Докажимо да је d један највећи заједнички делилац елемената a и b (највећи заједнички делилац није једнозначно одређен, али су свака два највећа заједничка делиоца придружени један другом).

Најпре, $a, b \in \langle d \rangle$. То значи да постоје a_1, b_1 за које је $a = da_1$ и $b = db_1$, тј. $d \mid a$ и $d \mid b$, те d јесте заједнички делилац од a и b .

Претпоставимо да $d_1 \mid a$ и $d_1 \mid b$, тј. да је d_1 неки заједнички делилац од a и b . Треба доказати да $d_1 \mid d$. Како $d_1 \mid a$ и $d_1 \mid b$, то постоје a_1 и b_1 тако да је $a = d_1a_1$ и $b = d_1b_1$. С обзиром да $d \in \langle a, b \rangle$, постоје p, q такви да је $d = ap + bq$. Добијамо да је $d = d_1a_1p + d_1b_1q = d_1(a_1p + b_1q)$, те следи да $d_1 \mid d$. \square

Заправо је у овом ставу доказано не само да свака два елемента a и b имају највећи заједнички делилац d , но и да постоје p и q за које је $d = ap + bq$ (Безуова релација). Из ове релације се, на стандардан начин, изводи следеће својство: ако $a \mid bc$ и ако је $\text{NZD}(a, b)$ придружен јединици, онда $a \mid c$ (наравно, уместо да пишемо да је $\text{NZD}(a, b)$ придружен јединици, писаћемо да је $\text{NZD}(a, b) = 1$, имајући на уму шта то значи). Нека читаоци ово сами докажу.

Теорема 71 Сваки главноидеалски домен је и домен са једнозначном факторизацијом.

Доказ. Нека је A главноидеалски домен. Докажимо најпре да је сваки нерастављив елемент у A прост. Нека је q нерастављив и нека $q \mid ab$. Уколико q не дели a , мора бити $\text{NZD}(q, a) = 1$. Наиме, ако је $d = \text{NZD}(q, a)$, то значи да је $q = dz$ за неко z . Како је q нерастављив, мора бити $d \in U(A)$, или $z \in U(A)$. Но, ако је $z \in U(A)$, онда из чињенице да $d \mid a$ следи да и $q \mid a$, што противречи претпоставци. Закључујемо да $d \in U(A)$, тј. $\text{NZD}(q, a) = 1$ (погледајте ранију напомену у загради). Но, тада из горенаведеног својства следи да $q \mid b$, те закључујемо да је q прост.

Да бисмо доказали да је A домен са једнозначном факторизацијом, остаје само да покажемо да се сваки елемент из $A \setminus (U(A) \cup \{0\})$ може приказати у облику производа нерастављивих елемената (видети став 69).

Докажимо најпре да сваки непразан скуп идеала у A има максималан елемент. Претпоставимо да то није тако и нека је \mathcal{I} неки непразан скуп идеала који не садржи максималан елемент. Нека је $I_1 \in \mathcal{I}$ произвољан идеал из \mathcal{I} . Како он није максималан у \mathcal{I} , то постоји $I_2 \in \mathcal{I}$ за који је $I_1 \subset I_2$. Слично, постоји и $I_3 \in \mathcal{I}$ такав да је $I_2 \subset I_3$. Заправо добијамо стриктно растући ланац идеала

$$I_1 \subset I_2 \subset I_3 \subset \dots$$

из \mathcal{I} . Унија $J = \bigcup_{i=1}^{\infty} I_i$ је идеал као што се лако може проверити (проверите!). Но, с обзиром да је A главноидеалски, то је $J = \langle x \rangle$ за неки $x \in A$. Како је $x \in \bigcup_{i=1}^{\infty} I_i$, то $x \in I_{i_0}$ за неки i_0 . Но, одавде следи да је $J = I_{i_0}$, па је и $I_i = I_{i_0}$ за све $i \geq i_0$, те бесконачан стриктно растући ланац идеала и не постоји. Закључујемо да у \mathcal{I} постоји максималан елемент.

Претпоставимо да у $A \setminus (U(A) \cup \{0\})$ има елемената који немају факторизацију на нерастављиве елементе. Уочимо скуп идеала \mathcal{J} задат са:

$$\mathcal{J} = \{ \langle a \rangle : a \in A \setminus (U(A) \cup \{0\}) \text{ и } a \text{ нема факторизацију на нерастављиве} \}.$$

Према управо доказаном резултату, у \mathcal{J} постоји максималан елемент $\langle x \rangle$. Како x нема факторизацију на нерастављиве, то он сам није нерастављив, па постоје a, b такви да је $x = ab$, при чему $a, b \in A \setminus (U(A) \cup \{0\})$. Стога је $\langle x \rangle \subset \langle a \rangle$ и $\langle x \rangle \subset \langle b \rangle$ (зашто?), па a и b имају факторизацију на нерастављиве ($\langle x \rangle$ је максималан елемент у \mathcal{J}). Но, ако су то факторизације $a = p_1 \cdots p_r$ и $b = q_1 \cdots q_s$, онда је $x = ab = p_1 \cdots p_r q_1 \cdots q_s$ једна факторизација x на нерастављиве, што противречи избору елемента x . Ова контрадикција завршава доказ. \square

Дакле, домен са једнозначном факторизацијом се карактерише тиме да се у њему прости и нерастављиви елементи подударају и да се сваки ненула, неинвертибилан елемент a може представити у облику

$$a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}, \quad (2)$$

где је u инвертибилан елемент и p_i нерастављиви, при чему за $i \neq j$ елементи p_i и p_j нису придружени, док је $\alpha_i \in \mathbb{N}$. Осим тога, ако је

$$a = vq_1^{\beta_1} \cdots q_l^{\beta_l},$$

где је v инвертибилан, q_j нерастављиви и q_i, q_j нису придружени за $i \neq j$, онда је $k = l$ и за неку пермутацију $\sigma \in \mathbb{S}_k$ $\alpha_i = \beta_{\sigma(i)}$ и p_i је придружен елементу $q_{\sigma(i)}$.

Напомена 72 Читалац се можда пита зашто се појављује инвертибилан елемент u у представљању елемента a у облику производа, када се тако нешто не појављује у самој дефиницији домена са једнозначном

факторизацијом. Разлог лежи у томе што нерастављиви елементи p_i нису међусобно придружени и онда је неопходно издвојити инвертибилан елемент u . На пример, елемент $-36 \in \mathbb{Z}$ се може записати у облику $-36 = (-1)2^23^2$, или у облику $-36 = (-1)2^2(-3)^2$, али се (-1) мора појавити у овим записима. Презентација $-36 = 2(-2)3^2$ не задовољава услов да за различите индексе прости елементи нису придружени. \diamond

Пређимо сада на важан метод локализације којим се од датог домена прелази на нови домен, а у коме су неки изабрани елементи из почетног домена инвертибилни у новом домену (ми смо се у основној школи упознали са овим – то је увођење разломака). Почнимо следећом дефиницијом.

Дефиниција 73 Нека је A домен и $S \subseteq A \setminus \{0\}$. За S кажемо да је мултипликативан ако $1 \in S$ и ако из $s, t \in S$ следи да $st \in S$.

Пример 74 Следећи подскупови од $A \setminus \{0\}$ су мултипликативни:

1. $A \setminus \{0\}$;
2. $\{f^n : n \in \mathbb{N}\}$, за ма који елемент $f \in A \setminus \{0\}$;
3. $A \setminus P$ за ма који прост идеал $P \triangleleft A$.

1. Ово је јасно.

2. Подсетимо се да $0 \in \mathbb{N}$, па $1 \in S$. Осим тога, како је $f^m f^n = f^{m+n}$ и други услов је испуњен.

3. Јасно је да $1 \in A \setminus P$. Осим тога, ако $a \notin P$ и $b \notin P$, онда и $ab \notin P$, пошто је P прост идеал (појасните себи ово!). \clubsuit

Нека је A домен и S ма који мултипликативан подскуп од A . На скупу $A \times S$ дефинишемо релацију \sim са:

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

Докажимо да је \sim једна релација еквиваленције.

Рефлексивност. Ово је јасно пошто је $sa = sa$, па је $(a, s) \sim (a, s)$.

Симетричност. И ово је јасно, јер из $(a, s) \sim (b, t)$, следи да је $ta = sb$, тј, $sb = ta$, а то управо значи да је $(b, t) \sim (a, s)$.

Транзитивност. Нека је $(a, s) \sim (b, t)$ и $(b, t) \sim (c, r)$. То значи да је $ta = sb$ и $rb = tc$. Добијамо да је

$$rta = rsb = stc.$$

Како је A домен, то је $ra = sc$, па је $(a, s) \sim (c, r)$.

Са $S^{-1}A$ означавамо скуп свих класа еквиваленције, а са $\frac{a}{s}$ класу еквиваленције елемента (a, s) . Дефинишемо операције $+$ и \cdot на $S^{-1}A$ са:

$$\frac{a}{s} + \frac{b}{t} := \frac{ta + sb}{st};$$

$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

Како је скуп S мултипликативан, то за $s, t \in S$ и $st \in S$, па ови записи имају смисла. Треба још да проверимо да су ове операције добро дефинисане.

Нека је $\frac{a}{s} = \frac{a'}{s'}$ и $\frac{b}{t} = \frac{b'}{t'}$. То заправо значи да је $(a, s) \sim (a', s')$ и $(b, t) \sim (b', t')$. Треба проверити да је $(ta + sb, st) \sim (t'a' + s'b', s't')$ и $(ab, st) \sim (a'b', s't')$. Рачунамо:

$$s't'(ta + sb) = s't'ta + s't'sb = t'tsa' + s'stb' = st(t'a' + s'b'),$$

па је заиста $(ta + sb, st) \sim (t'a' + s'b', s't')$. На сличан начин се проверава и добра дефинисаност операције множења.

Није тешко проверити да је структура $(S^{-1}A, +, \cdot)$ један комутативан прстен са јединицом (урадите то за вежбу: $0_{S^{-1}A} = \frac{0}{1}$, $1_{S^{-1}A} = \frac{1}{1}$). Овај прстен назива се локализација домена A у односу на мултипликативан скуп S . Основно својство локализације дато је следећим ставом.

Став 75 Нека је A домен и S неки мултипликативан подскуп од A .

- а) Са $i(a) = \frac{a}{1}$ задат је један мономорфизам $i: A \rightarrow S^{-1}A$,
 б) Ако је B ма који комутативан прстен и $f: A \rightarrow B$ хомоморфизам такав да за све $s \in S$ важи: $f(s) \in U(B)$, онда постоји тачно један хомоморфизам $\tilde{f}: S^{-1}A \rightarrow B$ за који је $\tilde{f} \circ i = f$.

Доказ.

а) Како је $i(a + b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)$ и $i(ab) = \frac{ab}{1} = \frac{a}{1} \frac{b}{1}$, то је i заиста хомоморфизам. Но, $a \in \text{Ker}(i)$ ако и само ако је $\frac{a}{1} = \frac{0}{1}$, што је еквивалентно са $a = 0$, па је i мономорфизам.

б) Тражени хоморфизам \tilde{f} дефинишемо са: $\tilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$. Како је, за све $s \in S$, $f(s)$ инвертибилан, ова дефиниција има смисла. Остављамо читаоцима да провере да је ово заиста један добро дефинисан хомоморфизам и да важи: $\tilde{f} \circ i = f$. \square

Уколико је $S = A \setminus P$ за неки прост идеал P , онда се уместо $(A \setminus P)^{-1}A$ краће пише: A_P . Важи следећа теорема.

Теорема 76 За сваки прост идеал $P \triangleleft A$, прстен A_P је локални прстен.

Доказ. Доказаћемо да је скуп свих неинвертибилних елемената идеал. Одредимо најпре $U(A_P)$:

$$\frac{a}{s} \in U(A_P) \text{ ако постоје } b \in A \text{ и } t \in A \setminus P \text{ тако да је } \frac{a}{s} \cdot \frac{b}{t} = \frac{1}{1}.$$

Другим речима, $\frac{a}{s}$ је инвертибилан акко постоји $b \in A$ и $t \notin P$ за које је $ab = st$. Уколико $a \in P$, онда и $st = ab \in P$, па како је P прост идеал, следи да $s \in P$, или $t \in P$, што није могуће на основу избора s и t . А уколико $a \notin P$, онда је $\frac{s}{a} (\in A_P)$ инверз елемента $\frac{a}{s}$. Дакле,

$$A_P \setminus U(A_P) = \left\{ \frac{a}{s} \in A_P : a \in P \right\}.$$

Уверимо се да је ово заиста идеал у A_P .

Нека су x, y неинвертибилни елементи из A_P . То значи да постоје елементи $a, b \in P$ и $s, t \notin P$ за које је $x = \frac{a}{s}$ и $y = \frac{b}{t}$. Тада је $x + y = \frac{a}{s} + \frac{b}{t} = \frac{ta + sb}{st}$, но, како је P идеал, $ta + sb \in P$, па је заиста и елемент $x + y$ неинвертибилан. На сличан начин се показује да ако $x \in A_P$ нема инверз и ако је $z \in A_P$ произвољан, ни елемент zx нема инверз. Закључујемо да је $A_P \setminus U(A_P)$ заиста идеал, па је и прстен A_P локални прстен. \square

За крај напоменимо да, уколико је $S = A \setminus \{0\}$, у прстену $S^{-1}A$ је сваки елемент различит од нуле инвертибилан, те је, у овом случају, $S^{-1}A$ једно поље. Ово поље се назива поље разломака домена A и означава са $Q(A)$. На овај начин смо показали да се сваки домен може утопити у неко поље. Као што видимо, ова је конструкција у потпуности аналогна конструкцији рационалних бројева као разломака над целим бројевима. Други важан пример имамо у случају прстена полинома, али ћемо се прво позабавити више овим прстеном.

Једнозначна факторизација у прстену полинома

У овом одељку, прстен A је прстен са једнозначном факторизацијом. Главни резултат у овом делу биће следећа теорема.

Теорема 77 Ако је A домен са једнозначном факторизацијом, онда је и $A[X]$ домен са једнозначном факторизацијом.

Но, ово није тако лако доказати, биће нам потребни неки припремни резултати. У даљем ћемо поље разломака домена A , тј. прстен $Q(A)$ означавати са K . То је заправо $S^{-1}A$, за $S = A \setminus \{0\}$.

Докажимо најпре следећу лему.

Лема 78 Ако је p прост елемент у A , онда је $\langle p \rangle \triangleleft A[X]$ прост идеал.

Доказ. Неопходно је да разликујемо идеал pA прстена A генерисан са p и идеал $pA[X]$ који је идеал у прстену $A[X]$. Овај потоњи идеал је горенаведени идеал $\langle p \rangle$. Пошто је p прост елемент у A , онда је, по ранијим резултатима, pA прост идеал у A и A/pA је домен. Ми

треба да докажемо 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 са \bar{a} означен елемент $a + pA$ прстена A/pA . С обзиром да је пресликавање $a \mapsto \bar{a}$ епиморфизам (хомоморфизам који је „на” прстена A на прстен A/pA), лако се проверава да је φ такође један епиморфизам. Но, $a_0 + a_1X + \cdots + a_nX^n \in \text{Ker}(\varphi)$ **ако** је $a_i = 0_{A/pA}$ за све i , тј. **ако** $p \mid a_i$ за све i . Но, у том случају је $a_i = pb_i$, за неке b_i , па је $a_0 + a_1X + \cdots + a_nX^n = p(b_0 + b_1X + \cdots + b_nX^n)$. Но, ово нам показује да је $\text{Ker}(\varphi) = pA[X]$, те имамо изоморфизам $A[X]/pA[X] \cong (A/pA)[X]$. Но, како је A/pA домен, то је и $(A/pA)[X]$ такође домен, те закључујемо да је $pA[X]$ заиста прост идеал. \square

Дефиниција 79 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 80 (Гаусова лема) Ако су $f, g \in A[X]$ примитивни, онда је и $f \cdot g$ примитиван.

Доказ. 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 полинома $f \cdot g$. То значи да је онда

$$\varphi(f \cdot g) = 0 \in (A/pA)[X], \quad (3)$$

где је φ горенаведени епиморфизам. Но, како је f примитиван, онда p не може да дели све његове коефицијенте, тј. $\varphi(f) \neq 0$. Из истих разлога је $\varphi(g) \neq 0$. Но, како је $(A/pA)[X]$ домен, то је $\varphi(f) \cdot \varphi(g) \neq 0$, а $\varphi(f \cdot g) = \varphi(f) \cdot \varphi(g)$. Једначина (3) даје контрадикцију која завршава доказ. \square

Лема 81 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 $u \in U(A)$.

Доказ. а) Нека је

$$f = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \cdots + \frac{a_n}{b_n}X^n,$$

где $a_i, b_i \in A$. Ако је $d = b_0b_1 \cdots b_n$, онда је јасно 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 примитивни. Уколико је $c_1 = \frac{p_1}{q_1}$, $c_2 = \frac{p_2}{q_2}$ 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 $q_1p_2f_2$. С обзиром да су ово једнаки полиноми, закључујемо да су q_2p_1 и q_1p_2 придружени елементи прстена A , 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 $f = c(f)f_0$ и $g = c(g)g_0$, $h = f \cdot g = c(f \cdot g)h_0$, $f_0, g_0, h_0 \in A[X]$ примитивни полиноми. Тада је $f \cdot g = c(f)c(g)f_0g_0$, где је f_0g_0 примитиван по Гаусовој лемии. Дакле,

$$c(f)c(g)f_0g_0 = c(h)h_0.$$

На основу а) добијамо да је $c(f \cdot g) = u \cdot c(f) \cdot c(g)$, за неки $u \in U(A)$. \square

Лема 82 Прости елементи у $A[X]$ су или прости елементи у A или примитивни полиноми из $A[X]$ који су нерастављиви у $K[X]$.

Доказ. Нека је $f \in A[X]$ прост елемент. Ако је $\deg f = 0$, онда је f прост елемент у A . Ако је $\deg f > 0$, онда f мора бити примитиван полином. Наиме, ако постоји p који је прост у A и који дели све коефицијенте полинома f , онда је $f = a_0 + a_1X + \dots + a_nX^n = p(b_0 + b_1X + \dots + b_nX^n)$ и f не би био нерастављив, па тиме ни прост. Поставља се питање: може ли f бити растављив у $K[X]$. Уколико би то било тако, тј. уколико би постојали неконстантни полиноми g и h тако да је $f = g \cdot h$, онда би, на основу претходне 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 само инвертибилан у A , што не мења ништа) и имали бисмо да је $c(g) \cdot c(h) \in U(A)$. Тада је

$$f = c(g)g_0 \cdot c(h)h_0 = \underbrace{c(g) \cdot c(h)}_{\in U(A)} g_0h_0$$

и добили бисмо да је f растављив 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 константа, онда је он примитиван и нерастављив у $K[X]$.

Докажимо сада и други смер. Ако је f прост елемент у A , онда из леме 78 следи да је он прост и у $A[X]$. Претпоставимо сада да је f примитиван полином у $A[X]$ који је нерастављив у $K[X]$. Треба доказати 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 ово јесте прстен 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 81 имамо да је $c(g) = c(k) \cdot c(f) \cdot u$, где је $u \in U(A)$. Како је f примитиван, то је $c(f) = 1$, па је $c(k) = c(g) \cdot u^{-1} \in A$, па је заправо $k \in A[X]$ и $f \mid g$ у $A[X]$, те је f прост елемент у $A[X]$. \square

Сада најзад можемо доказати теорему 77.

Доказ теореме 77. Знамо да је довољно доказати да се сваки елемент у $A[X] \setminus (U(A[X]) \cup \{0\})$ може приказати у облику производа простих елемената. Наравно, $U(A[X]) = U(A)$. Можемо наћи растав од f на нерастављиве у $K[X]$ за који знамо да постоји: $f = f_1 \cdots f_k$. Но, $f_i = c(f_i)g_i$ где је $c(f_i) \in K$, а g_i примитивни (а наравно да су нерастављиви у $K[X]$) јер су такви f_i . Дакле,

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

Како су g_i примитивни у $A[X]$ и нерастављиви у $K[X]$, онда су они прости елементи у $A[X]$. Но, из горње једнакости следи да $c(f_1) \cdots c(f_k) \in A$, а како је A прстен са једнозначном факторизацијом, могуће је наћи d_1, \dots, d_r који су прости у A (а тиме и прости у $A[X]$) такве да је $c(f_1) \cdots c(f_k) = d_1 \cdots d_r$ те смо најзад 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 $A[X]$. \square

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

Приметимо да ако је $f \in A[X]$, онда $c(f) \in A$.

Став 83 Нека је A прстен 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 $K[X]$.

Доказ. Пре свега, знамо да је $A[X]$ прстен са једнозначном факторизацијом, те 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 $K[X]$, а тада и $\text{NZD}(c(f), c(g)) \cdot d \mid f$ у $K[X]$ то је $f = \text{NZD}(c(f), c(g)) \cdot d \cdot q$ 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 примитивни 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 $K[X]$. 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 $Q \in K[X]$ и D дели наведени полином у $A[X]$. Стога он испуњава оба услова за највећи заједнички делилац и то завршава доказ овог става. \square .

Уколико је A прстен са једнозначном факторизацијом, а K његово поље разломака, онда је поље разломака за прстен $A[X]$, заправо ПОЉЕ РАЦИОНАЛНИХ ФУНКЦИЈА у ознаци $K(X)$, дато са:

$$K(X) = \left\{ \frac{a(X)}{b(X)} : a(X), b(X) \in A[X], b(X) \neq 0 \right\}.$$

Наравно, овде је $\frac{a(X)}{b(X)}$ класа еквиваленције и

$$\frac{a(X)}{b(X)} = \frac{a_1(X)}{b_1(X)} \text{ ако је } a(X)b_1(X) = a_1(X)b(X).$$

Приметимо да је $K(X)$ истовремено и поље разломака за прстен $K[X]$. Наиме, инвертујући све не-нула полиноме из $A[X]$ ми смо инвертовали и све не-нуле елементе из A и тиме добили и K .

Илуструјмо став **83** примерима.

Пример 84 Наћи 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 $\mathbb{Z}[X]$.

Одредимо најпре $c(f)$ и $c(g)$ за наше полиноме.

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

и добијамо да је $\text{NZD}(c(f), c(g)) = 2$. Следеће што треба да урадимо је да нађемо највећи заједнички делилац ових полинома, али у $\mathbb{Q}[X]$. Потом, пошто знамо да је највећи делилац одређен но на инвертибилан

елемент, према ставу **83** 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 ненула цели бројеви су инвертибилни те је $\text{NZD}(ma(X), nb(X)) = \text{NZD}(a(X), b(X))$ за све целе бројеве m, n који нису једнаки нула. Поступак наравно изводимо Еуклидовим алгоритмом, али користећи ову идеју да бисмо поједноставили међурезултате. Како је $f(X) = 4(2X^5 + 2X^4 + X^3 + X^2 + X + 2)$, а $g(X) = 6(3X^4 + 4X^3 + 2X^2 - X - 2)$, то Еуклидов алггеоритам можемо применити на ове примитивне полиноме у заградама. Дакле, требало би 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 ћемо одмах добити разломак. Нема ничег лошег у разломцима, али ради лакше рачунице бисмо волели да их избегнемо. Видимо да то можемо ако први 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 ова два полинома једнака 1. Стога се у другом кораку може појавити разломак. Зато је погодно први 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 $5^2 = 25$.

Дакле, делимо полином $75X^4 + 100X^3 + 50X^2 - 25X - 50$ полиномом $5X^3 + 19X^2 + 19X + 14$. Добијамо количник $15X - 37$ и остатак $468X^2 + 468X + 468 = 468(X^2 + X + 1)$. Сада полином $5X^3 + 19X^2 + 19X + 14$ треба поделити полиномом $468(X^2 + X + 1)$, но наравно да ћемо га делити полиномом $X^2 + X + 1$. Када то урадимо, добијамо да је количник $5X + 14$, а остатак је једнак 0.

Еуклидов алгоритам нам за тражени највећи заједнички делилац даје последњи ненула остатак, а то је полином $468(X^2 + X + 1)$. Но, највећи заједнички делилац ће бити тада и полином $X^2 + X + 1$ и њега бирамо зато што је он примитиван полином у $\mathbb{Z}[X]$.

Коначно, $\text{NZD}(f, g) = 2(X^2 + X + 1)$ на основу става **83**. ♣

Пример 85 Наћи највећи заједнички делилац полинома $f(X, Y) = X^3 + X^2Y - 2XY^2 + XY + 2Y^2$ и $g(X, Y) = X^4 + 2X^3Y + XY^2 + X + 2Y^3 + 2Y$ у прстену $\mathbb{Z}[X, Y]$.

Да бисмо применили став **83**, 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 :

$$P = X^3 + YX^2 + (-2Y^2 + Y)X + 2Y^2, Q = X^4 + 2YX^3 + (Y^2 + 1)X + 2Y^3 + 2Y.$$

Тада је $c(P) = \text{NZD}(1, Y, -2Y^2 + Y, 2Y^2) = 1$, а $c(Q) = \text{NZD}(1, 2Y, Y^1 + 1, 2Y^3 + 2Y) = 1$. Остаје да нађемо највећи заједнички делилац поли-

нома P и Q у $\mathbb{Q}(Y)[X]$ и да изаберемо такав који је примитиван полином у $\mathbb{Z}[Y][X]$ (поље разломака прстена $\mathbb{Z}[Y]$ је поље $\mathbb{Q}(Y)$).

Поделимо полином Q полиномом P . Добијамо количник $X + Y$ и остатак $(Y^2 - Y)X^2 + (2Y^3 - 2Y^2 + 1)X + 2Y$. Сада би полином P требало поделити овим остатком. Да би се избегли разломци, као у претходном, делићемо полином $(Y^2 - Y)^2 P$ тим остатком. После доста рачунања добијамо да је количник $(Y^2 - Y)X - Y^3 + Y^2 - 1$, а остатак $(Y^5 - 2Y^4 + 2Y^3 - Y^2 + 1)X + (2Y^6 - 4Y^5 + 4Y^4 - 2Y^3 + 2Y)$. Није тешко видети да је овај полином шестог степена по Y заправо производ полинома петог степена по Y и $2Y$, те је остатак $(Y^5 - 2Y^4 + 2Y^3 - Y^2 + 1)(X + 2Y)$ и у даљем рачуну можемо користити $X + 2Y$ (пошто је сваки ненула полином по Y инвертибилан у $\mathbb{Q}(Y)$).

Остало је да се полином $(Y^2 - Y)X^2 + (2Y^3 - 2Y^2 + 1)X + 2Y$ подели полиномом $X + 2Y$. Но, добијамо да је заправо $(Y^2 - Y)X^2 + (2Y^3 - 2Y^2 + 1)X + 2Y = (X + 2Y)((Y^2 - Y)X + 1)$. Дакле, последњи ненула остатак је $X + 2Y$ и добијамо да је то заправо највећи заједнички делилац датих полинома. ♣

Докажимо на крају овог дела и познати Ајзенштајнов критеријум за нерастављивост полинома из $\mathbb{Z}[X]$ у прстену \mathbb{Q} .

Став 86 (Ајзенштајнов критеријум) Нека је A прстен са једнозначном факторизацијом, K његово поље разломака и $f = a_0 + a_1X + \dots + a_nX^n \in A[X]$ 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. $p^2 \nmid a_0$,

онда је f нерастављив у $K[X]$.

Доказ. Претпоставимо да је $f = g \cdot h$ у $K[X]$, при чему је $\deg g, \deg h < \deg f$. 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 $f = c(g)g_0c(h)h_0 = g_1h_0$, при чему је $g_1 = c(g)c(h)g_0 \in A[X]$. Дакле, имамо факторизацију $f = g_1h_1$ и у $A[X]$.

Искористимо сада хомоморфизам φ из доказа леме **78**. Ако са \bar{a} означимо слику елемента a у $A/pA[X]$, онда имамо да је $\bar{f} = \bar{a}_nX^n$, а како је $f = g_1h_1$, онда је $\bar{a}_nX^n = \bar{g}_1\bar{h}_1$, из чега следи да је $\bar{g}_1 = \bar{c}X^k$, а $\bar{h}_1 = \bar{d}X^{n-k}$. Но, то значи да је сваки коефицијент полинома g_1 и h_1 , сем најстаријег, дељив са p . Посебно су и слободни чланови дељиви са p , па је a_0 дељив са p^2 што противречи претпоставци. Стога закључујемо да је f нерастављив у $K[X]$. □

Пример 87 Нека је p прост број. Доказати да је полином $a(X) = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Z}[X]$ нерастављив у $\mathbb{Q}[X]$.

Јасно је да је полином $a(X)$ нерастављив **акко** је нерастављив полином $a(X+1)$. Наиме, ако би полином $a(X+1)$ био растављив, онда би било

$a(X+1) = b(X)c(X)$, за неке полиноме $a(X)$ и $b(X)$, но из овога следи да је $a(X) = b(X-1)c(X-1) = a_1(X)b_1(X)$. Како је

$$(X-1)a(X) = X^p - 1,$$

то је

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

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 $p \nmid 1$, то је полином $a(X+1)$ нерастављив по Ајзенштајновом критеријуму. ♣

За испитивање нерастављивости је корисна и провера да ли полином из $A[X]$ има нулу у K . Ево става који нам у томе помаже.

Став 88 Нека је $f(X) = a_nX^n + \dots + a_1X + a_0 \in A[X]$, где је A прстен 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, онда је свака нула тог полинома која се налази у K заправо у A .

Доказ. Ако је $f(b/c) = 0$, онда имамо

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

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 $b \mid a_0c^n$, а $c \mid a_nb^n$. Из чињенице да је $\text{NZD}(b, c) = 1$ следи да је и $\text{NZD}(b, c^n) = 1$, те, као и раније, закључујемо да $b \mid a_0$. На аналоган начин добијамо да $c \mid a_n$. Ако је $f(X)$ моничан полином, тј. ако је $a_n = 1$, онда из $c \mid a_n$ следи да је $c \in U(A)$, те је $b/c \in A$. □

Раширења поља

Уколико је поље F садржано у пољу E , онда кажемо да је поље E РАШИРЕЊЕ поља F . Следећа важна теорема описује Кронекерову конструкцију којим се дато поље проширује до новог поља додавањем нула нерастављивог полинома. Пре даљег читања, препорука је да читаоци понове градиво из Линеарне алгебре – појам векторског простора, линеарне независности вектора, базе и димензије векторског простора.

Теорема 89 Нека је F поље и $a(X) \in F[X] \setminus \{0\}$ нерастављив полином.

- а) $E = F[X]/\langle a(X) \rangle$ је поље.
- б) Поље E садржи потпоље изоморфно пољу F .
- в) Полином $a(X)$ има бар једну нулу у пољу E .
- г) На основу а) можемо сматрати да је $F \subset E$. Тада се E може видети и као векторски простор над пољем F и димензија тог простора једнака је степену полинома $a(X)$.

Доказ. а) Како је $a(X)$ нерастављив, то је идеал $I = \langle a(X) \rangle$ максималан у скупу свих главних идеала. Но, у прстену $F[X]$ је сваки идеал главни, те је I максималан идеал. Стога је E поље.

б) Дефинишимо хомоморфизам $f: F \rightarrow E$ са $f(\alpha) = \alpha + I$ за $\alpha \in F$. Лако је проверити да ово јесте један хомоморфизам. Како су једини идеали у ма ком пољу $\{0\}$ и цело поље, то закључујемо да је $\text{Ker}(f) = \{0\}$ (језгро је увек идеал, али не може бити једнако целом пољу пошто се при хомоморфизму јединица слика у јединицу, а не у нулу). Дакле, хомоморфизам f успоставља изоморфизам између F и слике од f , која је потпоље од E . У даљем идентификујемо F и слику $f[F]$, ради једноставнијег писања, тако да ћемо, између осталог, уместо $a + I$, за $a \in F$ писати само a .

в) Уочимо елемент $X + I$ у E . Означимо га са \tilde{X} . Уколико је $a(X) = a_0 + a_1X + \dots + a_nX^n$, добијамо да је

$$\begin{aligned} a(\tilde{X}) &= a_0 + a_1\tilde{X} + a_2\tilde{X}^2 + \dots + a_n\tilde{X}^n = a_0 + a_1(X+I) + a_2(X+I)^2 + \dots + a_n(X+I)^n, \\ &= (a_0 + a_1X + a_2X^2 + \dots + a_nX^n) + I = a(X) + I = I, \end{aligned}$$

те добијамо да \tilde{X} заиста анулира полином $a(X)$.

г) Како E садржи потпоље F' изоморфно са F , заиста са алгебарске тачке можемо сматрати да је $F \subset E$. У овом случају кажемо и да је поље E једно РАШИРЕЊЕ поља F . Наравно да елементе поља E можемо сабирати, али, с обзиром да је $F \subset E$, можемо их и множити елементима из F . На основу својстава операција у пољу E добијамо да је E заиста векторски простор над F . Димензију тог простора зовемо и СТЕПЕН РАШИРЕЊА поља E над F и означавамо са $[E : F]$. Наш задатак је да докажемо да је $[E : F] = \deg a(X)$. Доказаћемо заправо да је

$$[1 + I, X + I, \dots, X^{n-1} + I]$$

једна база простора E уколико је полином $a(X)$ степена n .

$\{1 + I, X + I, \dots, X^{n-1} + I\}$ је генератриса. Уочимо ма који елемент $p(X) + I \in E$. Тада је

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

где је $r(X) = 0$, или је $\deg r(X) < \deg a(X) = n$. Дакле,

$$r(X) = r_0 + r_1X + \cdots + r_{n-1}X^{n-1},$$

где наравно неки, па и сви, коефицијенти $r_i \in F$ могу бити једнаки 0. Но, тада је

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

те је

$$p(X) + I = r_0(1 + I) + r_1(X + I) + \cdots + r_{n-1}(X^{n-1} + I).$$

Закључујемо да $1 + I, \dots, X^{n-1} + I$ заиста генеришу E .

Линеарна независност. Нека је

$$c_0(1 + I) + c_1(X + I) + \cdots + c_{n-1}(X^{n-1} + I) = 0 + I,$$

за неке $c_i \in F$. Тада је

$$(c_0 + c_1X + \cdots + c_{n-1}X^{n-1}) + I = I,$$

те

$$c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in I = \langle a(X) \rangle.$$

Но, полином $a(X)$ је степена n и он може да дели полином $c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$ једино ако је $c_0 + c_1X + \cdots + c_{n-1}X^{n-1} = 0$. Но, то управо значи да је $c_0 = c_1 = \cdots = c_{n-1} = 0$, те закључујемо да су $1 + I, \dots, X^{n-1} + I$ заиста линеарно независни. \square

Напомена 90 Приметимо да је, као векторски простор над пољем F , поље E из претходне теореме изоморфно са F^n : $E \cong F^n$. Но, директан производ поља никада није поље, јер ту увек имамо делитеље нуле: $(1, 0) \cdot (0, 1) = (0, 0)$. Ради се о томе што овде на F^n операцију сабирања заиста дефинишемо по координатама, али је операција множења задата на другачији начин – ту користимо полином $a(X)$. Наиме, да бисмо нашли производ n -торки $(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \cdot (\beta_0, \beta_1, \dots, \beta_{n-1})$ из F^n , ми налазимо остатак при дељењу полинома $(\alpha_0 + \alpha_1X + \cdots + \alpha_{n-1}X^{n-1}) \cdot (\beta_0 + \beta_1X + \cdots + \beta_{n-1}X^{n-1})$ полиномом $a(X)$ и ако је тај остатак полином $\gamma_0 + \gamma_1X + \cdots + \gamma_{n-1}X^{n-1}$, тада је

$$(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \cdot (\beta_0, \beta_1, \dots, \beta_{n-1}) = (\gamma_0, \gamma_1, \dots, \gamma_{n-1}). \quad \diamond$$

Искористимо управо доказану теорему да конструишемо поље од 4 елемента. Приметимо да \mathbb{Z}_4 јесте комутативан прстен, али наравно да да није поље пошто у \mathbb{Z}_4 важи: $2 \cdot 2 = 0$, а $2 \neq 0$.

Пример 91 Конструисати поље, које има тачно 4 елемента.

Како ово извести? Пре свега, ми знамо да је \mathbb{Z}_2 поље и да има 2 елемента. Претходна теорема нам каже да ако нађемо нерастављив полином $a(X) \in \mathbb{Z}_2[X]$, који је степена n онда ће $\mathbb{Z}_2[X]/\langle a(X) \rangle$ бити поље, које је истовремено векторски простор над \mathbb{Z}_2 димензије n . Дакле, то поље је као векторски простор над \mathbb{Z}_2 изоморфно \mathbb{Z}_2^n , те има 2^n елемената. Нама је потребно поље са 4 елемента, тј. потребан нам је нерастављив полином из $\mathbb{Z}_2[X]$ степена 2. Такав полином наравно није тешко наћи. То је полином $a(X) = 1 + X + X^2$. Како је то полином другог степена, он је нерастављив ако и само ако нема ниједну нулу у \mathbb{Z}_2 , а како је $a(0) = 1$ и $a(1) = 1$, то је заиста испуњено. Дакле, наше поље \mathbb{F}_4 је дато са

$$\mathbb{F}_4 = \mathbb{Z}_2[X]/\langle X^2 + X + 1 \rangle.$$

Означимо са η елемент $X + \langle X^2 + X + 1 \rangle$ у овом пољу. Добијамо да је

$$\mathbb{F}_4 = \{0, 1, \eta, 1 + \eta\}.$$

Како у пољу \mathbb{F}_4 важи: $\eta^2 = 1 + \eta$ (зашто?), можемо написати и таблице сабирања и множења у том пољу.

+	0	1	η	$1 + \eta$	·	0	1	η	$1 + \eta$
0	0	1	η	$1 + \eta$	0	0	0	0	0
1	1	0	$1 + \eta$	η	1	0	1	η	$1 + \eta$
η	η	$1 + \eta$	0	1	η	0	η	$1 + \eta$	1
$1 + \eta$	$1 + \eta$	η	1	0	$1 + \eta$	0	$1 + \eta$	1	η

Уколико, пак, желимо да прикажемо поље \mathbb{F}_4 као структуру коју чине уређени парови из \mathbb{Z}_2 , онда имамо, на основу претходне напомене, да су операције задате на следећи начин:

$$\begin{aligned} (\alpha_0, \alpha_1) + (\beta_0, \beta_1) &= (\alpha_0 + \beta_0, \alpha_1 + \beta_1) \\ (\alpha_0, \alpha_1) \cdot (\beta_0, \beta_1) &= (\alpha_0\beta_0 + \alpha_1\beta_1, \alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_1\beta_1), \end{aligned}$$

јер је остатак дељења полинома $(\alpha_0 + \alpha_1 X) \cdot (\beta_0 + \beta_1 X)$ полиномом $X^2 + X + 1$ једнак $\alpha_0\beta_0 + \alpha_1\beta_1 + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_1\beta_1)X$. Овде смо наравно користили да је $1 = -1$ у \mathbb{Z}_2 . ♣

Вратимо се поново на теорему. Претпоставимо да нам је дат неки полином $a(X) \in F[X]$ где је F неко поље. Тај полином наравно не мора имати линеарну факторизацију над пољем F . Поставља се питање: да ли постоји неко поље E које садржи поље F и у коме се полином $a(X)$ факторише на линеарне факторе? То заиста јесте тачно и претходна теорема нам показује и пут доказа.

Последица 92 Нека је F поље и $a(X) \in F[X]$. Тада постоји раширење E поља F у коме се полином $a(X)$ факторише на линеарне факторе.

Доказ. Јасно је да можемо да претпоставимо да је полином $a(X)$ нерастављив, пошто бисмо у супротном његову факторизацију добили тако

што бисмо нашли раширење у коме сви његови фактори имају линеарну факторизацију.

На основу доказане теореме, постоји поље E' , које је раширење поља F , а у коме полином $a(X)$ има бар једну нулу, назовимо је α . То значи да у $E'[X]$ важи факторизација

$$a(X) = (X - \alpha)b(X),$$

где је $b(X) \in E'[X]$ и $\deg b(X) = n - 1$. Уколико сада $b(X)$ раставимо на нерастављиве факторе у $E'[X]$, на њих можемо применити претходно закључивање. Тако процес настављамо све док не дођемо до линеарне факторизације. Јасно је да се процес мора завршити пошто у сваком кораку добијамо бар једну нову нулу почетног полинома, а он ни у једном пољу не може имати више од n нула. \square

Нека је B комутативни прстен са јединицом, A његов потпрстен (са јединицом наравно) и $b \in B \setminus A$. Како одредити најмањи потпрстен од B који садржи и A (као подскуп) и b као елемент? Очигледно је да такав прстен мора да садржи и све степене од b , као и све елементе облика $a_0 + a_1b + a_2b^2 + \dots + a_nb^n$ где $a_i \in A$. Дакле, мора да садржи све елементе облика $p(b)$, где $p(X) \in A[X]$. Но, то је заправо и довољно, тј. тражени најмањи потпрстен је

$$A[b] := \{p(b) : p(X) \in A[X]\}.$$

Наиме, $A[b]$, овако дефинисан, је заиста потпрстен од B (очигледно је да је $A \subset A[b]$ и $b \in A[b]$):

$$\begin{aligned} p(b), q(b) \in A[b] &\implies p(b) - q(b) = (p - q)(b) \in A[b]; \\ p(b), q(b) \in A[b] &\implies p(b)q(b) = (pq)(b) \in A[b]. \end{aligned}$$

Уколико је F потпоље од E и $\alpha \in E \setminus F$, онда са $F[\alpha]$ означавамо најмањи потпрстен који садржи F и α , а са $F(\alpha)$ најмање потпоље које садржи (као своје потпоље) F и α (као свој елемент). Поставља се природно питање: када је $F[\alpha] = F(\alpha)$? Другим речима, интересује нас у ком је случају прстен $F[\alpha]$ поље. Није тешко наћи један потребан услов за то. Наиме, како је

$$F[\alpha] = \{p(\alpha) : p(X) \in F[X]\},$$

а сваки елемент поља, који је различит од нуле има инверз, то и елемент $\alpha \in F[\alpha]$ има инверз у $F[\alpha]$, тј. постоји $a(\alpha) \in F[X]$ такав да је $\alpha \cdot a(\alpha) = 1$. Ако је $a(X) = a_0 + a_1X + \dots + a_nX^n$, то добијамо да је

$$a_n\alpha^{n+1} + \dots + a_1\alpha^2 + a_0\alpha - 1 = 0,$$

тј. постоји полином $p(X) \in F[X]$ такав да је $p(\alpha) = 0$.

Дефиниција 93 Нека је F потпоље од E и $\alpha \in E$. Тада је α алгебарски над F уколико постоји полином $p(X) \in F[X]$ за који је $p(\alpha) = 0$.

Дакле, видели смо да је потребан услов да прстен $F[\alpha]$ буде поље да је α алгебарски над F . Но, то је и довољан услов.

Став 94 Нека је F потпоље од E и $\alpha \in E$. Тада је $F[\alpha]$ поље ако и само ако је α алгебарски над F .

Доказ. Један смер смо већ доказали. Остало је да се покаже да из чињенице да је α алгебарски над F следи да је $F[\alpha]$ поље. Како је α алгебарски над F , посматрајмо идеал $I \triangleleft F[X]$ дефинисан са:

$$I = \{a(X) \in F[X] : a(\alpha) = 0\}.$$

Није тешко проверити да је I заиста идеал. Како је сваки идеал у $F[X]$ главни, то постоји моничан полином $\mu_\alpha(X)$ за који је $I = \langle \mu_\alpha \rangle$.

Приметимо да је полином $\mu_\alpha(X)$ нерастављив. У супротном, нека је $\mu_\alpha(X) = a(X)b(X)$ за неке неконстантне полиноме $a(X), b(X)$ из $F[X]$. Но, тада је $a(\alpha)b(\alpha) = \mu_\alpha(\alpha) = 0$, па следи да је $a(\alpha) = 0$ или $b(\alpha) = 0$. Уколико је нпр. $a(\alpha) = 0$, добили бисмо да $a(X) \in I$, те се добија да $\mu_\alpha(X) \mid a(X)$, што није могуће јер је $a(X)$ полином степена мањег од степена полинома $\mu_\alpha(X)$. Слично се добија и у случају да је $b(\alpha) = 0$.

Сада посматрамо хомоморфизам

$$f: F[X] \rightarrow F[\alpha]$$

дефинисан са $f(p(X)) = p(\alpha)$. Хомоморфизам f је очигледно „на”, а $\text{Ker}(f) = I$. Стога добијамо да је

$$F[X]/I \cong F[\alpha].$$

Но, како је $\mu_\alpha(X)$ нерастављив полином, $F[X]/I$ је поље, па је и $F[\alpha]$ такође поље. \square

Приметимо да смо у оквиру доказа овог става добили и да је

$$[F(\alpha) : F] = \deg \mu_\alpha(X).$$

Полином $\mu_\alpha(X)$ из овог става зове се и **минимални полином** елемента α . Базу за $F(\alpha)$ над F чине елементи $1, \alpha, \dots, \alpha^{n-1}$ уколико је $n = \deg \mu_\alpha(X)$.

Пример 95 Нека је $\alpha = \sqrt{2} + \sqrt{3}$.

- а) Показати да је α алгебарски над \mathbb{Q} .
- б) Наћи минимални полином за α над \mathbb{Q} .

в) Одредити $\frac{1}{\alpha+3}$ у облику $p(\alpha)$ за неки полином $p(X) \in \mathbb{Q}[X]$.

а) Нађимо полином који елемент α анулира. Како је $\alpha - \sqrt{2} = \sqrt{3}$, то је

$$\begin{aligned}(\alpha - \sqrt{2})^2 &= 3 \\ \alpha^2 - 2\alpha\sqrt{2} + 2 &= 3 \\ \alpha^2 - 1 &= 2\alpha\sqrt{2} \\ (\alpha^2 - 1)^2 &= (2\alpha\sqrt{2})^2 \\ \alpha^4 - 2\alpha^2 + 1 &= 8\alpha^2 \\ \alpha^4 - 10\alpha^2 + 1 &= 0.\end{aligned}$$

б) Покажимо да је минимални полином елемента α заиста полином $X^4 - 10X^2 + 1$. Означимо га са $\mu(X)$. Једино треба доказати је овај полином нерастављив над \mathbb{Q} . Како се ради о полиному четвртог степена, уколико је он растављив, он се раставља или на производ полинома првог степена и полинома трећег степена, или на производ два полинома другог степена.

$\mu(X)$ је производ полинома првог степена и полинома трећег степена над пољем \mathbb{Q} . То значи да $\mu(X)$ има нулу у \mathbb{Q} . Но, ако полином

$$a_n X^n + \dots + a_1 X + a_0$$

има рационалну нулу r/s (где је r/s нескратив разломак) онда $r \mid a_0$ и $s \mid a_n$. Како је у нашем случају $a_n = a_4 = 1$, то је $s = 1$, а како је $a_0 = 1$, то r може бити само 1 или -1 . Но, ни 1 ни -1 нису нуле полинома $\mu(X)$.

$\mu(X)$ је производ два полинома другог степена. Дакле,

$$\mu(X) = (X^2 + aX + b)(X^2 + cX + d)$$

(како је $\mu(X)$ моничан, можемо претпоставити да су и ти полиноми монични). Добијамо (изједначавањем одговарајућих коефицијената)

$$a + c = 0 \tag{4}$$

$$b + ac + d = -10 \tag{5}$$

$$ad + bc = 0 \tag{6}$$

$$bd = 1 \tag{7}$$

Из (4) добијамо да је $c = -a$. Тада из (6) следи да је $a(d - b) = 0$. Размотримо два случаја.

$a = 0$. Тада је и $c = 0$ и добијамо да се систем своди на две једначине

$$b + d = -10 \tag{8}$$

$$bd = 1 \tag{9}$$

Из (9) следи да је $d = 1/b$ (сигурно ни b ни d нису једнаки нули). Заменом у (8) и сређивањем добијамо квадратну једначину

$$b^2 + 10b + 1 = 0.$$

Решења ове једначине су дата са:

$$b_{1,2} = \frac{-10 \pm \sqrt{96}}{2}$$

По претпоставци $b \in \mathbb{Q}$. Како је $\sqrt{96} = 4\sqrt{6}$, добили бисмо да је $\sqrt{6} \in \mathbb{Q}$. Остављамо читаоцима да покажу да ово није могуће.

$a \neq 0$. У овом случају је $b = d$. Из једначине (7) добијамо да је $b \in \{1, -1\}$. Заменом у (5) (узимајући у обзир да је $c = -a$) добијамо да је $a^2 = 12$ или $a^2 = 8$. По претпоставци је $a \in \mathbb{Q}$ па би из $a^2 = 12$ следило да $\sqrt{3} \in \mathbb{Q}$, а из $a^2 = 8$ да је $\sqrt{2} \in \mathbb{Q}$. Како ни једно ни друго није тачно закључујемо да је $\mu(X)$ нерастављив.

в) За налажење $\frac{1}{\alpha+3}$ можемо користити метод неодређених коефицијената. Наиме, знамо да постоје a, b, c, d такви да је

$$\frac{1}{\alpha+3} = a + b\alpha + c\alpha^2 + d\alpha^3. \quad (10)$$

Потребно је одредити коефицијенте a, b, c, d . Из (10), множењем обе стране са $\alpha+3$, добијамо

$$1 = (\alpha+3)(a + b\alpha + c\alpha^2 + d\alpha^3). \quad (11)$$

Узимајући у обзир да је $\alpha^4 = 10\alpha^2 - 1$ и да су $1, \alpha, \alpha^2, \alpha^3$ линеарно независни над \mathbb{Q} , добијамо

$$\begin{array}{rcccc} 3a & & & -d & = & 1 \\ a & +3b & & & = & 0 \\ & b & +3c & +10d & = & 0 \\ & & c & +3d & = & 0 \end{array}$$

Као решење се добија: $(a, b, c, d) = (\frac{3}{8}, -\frac{1}{8}, -\frac{3}{8}, \frac{1}{8})$.

Ми смо заправо добили да је $\mathbb{Q}(\alpha) = \mathbb{Q}[X]/\langle X^4 - 10X^2 + 1 \rangle$. Стога је поље $\mathbb{Q}(\alpha)$ као векторски простор над \mathbb{Q} изоморфно са \mathbb{Q}^4 , а операција множења дата је са:

$$\begin{aligned} (\alpha_0, \alpha_1, \alpha_2, \alpha_3) \cdot (\beta_0, \beta_1, \beta_2, \beta_3) = & (\alpha_0\beta_0 - \alpha_1\beta_3 - \alpha_2\beta_2 - \alpha_3\beta_1 - 10\alpha_3\beta_3, \\ & \alpha_0\beta_1 + \alpha_1\beta_0 - \alpha_2\beta_3 - \alpha_3\beta_2, \alpha_0\beta_2 + \alpha_1\beta_1 + \alpha_2\beta_0 + 10\alpha_1\beta_3 + 10\alpha_2\beta_2 + 10\alpha_3\beta_1, \\ & \alpha_0\beta_3 + \alpha_1\beta_2 + \alpha_2\beta_1 + 10\alpha_1\beta_3 + 10\alpha_2\beta_2 + 10\alpha_3\beta_1 + 99\alpha_3\beta_3, \\ & \alpha_0\beta_3 + \alpha_1\beta_2 + \alpha_2\beta_1 + \alpha_3\beta_0 + 10\alpha_2\beta_3 + 10\alpha_3\beta_2). \end{aligned}$$

Јасно је да је из ове формуле веома тешко проверити да смо заиста добили поље! О налажењу инверза и да не говоримо. ♣

Дакле, видели смо да су од посебног значаја за теорију раширења поља они елементи који су алгебарски над датим пољем.

Дефиниција 96 За раширење E поља F кажемо да је алгебарско раширење ако је сваки елемент из E алгебарски над F .

За раширење E поља F кажемо да је коначно раширење уколико је E векторски простор над F , који је коначне димензије.

Став 97 Свако коначно раширење је алгебарско.

Доказ. Нека је $[E : F] = n$. То значи да је E n -димензионални простор над пољем F . Узмимо произвољни елемент $\alpha \in E$ и покажимо да је он алгебарски над F . Како је димензија простора једнака n , то је скуп вектора $\{1, \alpha, \dots, \alpha^n\}$ сигурно линеарно зависан скуп вектора. Наиме, ако међу њима има једнаких, тј. ако је $\alpha^k = \alpha^l$ за неке $1 \leq k < l \leq n$, онда је $\alpha^k - \alpha^l = 0$, те је $q(\alpha) = 0$ за полином $q(X) = X^k - X^l \in F[X]$. Ако су они сви различити, пошто их има више од $n = \dim_F E$, они морају бити линеарно зависни над F , па постоји $a_0, \dots, a_n \in F$ такви да је

$$a_0 1 + a_1 \alpha + \dots + a_n \alpha^n = 0,$$

но, то управо значи да је $p(\alpha) = 0$, где је $p(X) = a_0 + a_1 X + \dots + a_n X^n \in F[X]$. Дакле, елемент α је алгебарски над F . \square

Следећи став је користан.

Став 98 Нека је E коначно раширење поља F , а поље F коначно раширење поља G . Тада је поље E коначно раширење поља G и важи:

$$[E : G] = [E : F] \cdot [F : G].$$

Доказ. Нека је $[f_1, \dots, f_n]$ база за векторски простор F над поље G , а $[e_1, \dots, e_m]$ база за векторски простор E над пољем F . Покажимо да је $[e_1 f_1, \dots, e_m f_1, e_1 f_2, \dots, e_m f_n]$ база за векторски простор E над пољем G . То ће нам показати тражено.

Докажимо да је скуп $\mathcal{G} = \{e_i f_j : 1 \leq i \leq m, 1 \leq j \leq n\}$ генератриса са векторски простор E над пољем G . Нека је $e \in E$. Како је $[e_1, \dots, e_m]$ база за E над F , то је $e = \sum_{i=1}^m \alpha_i e_i$, за неке $\alpha_i \in F$. Како је $[f_1, \dots, f_n]$ база за F над G , то за свако $i \in \{1, \dots, m\}$ постоје $\beta_{ij} \in G$ за које је $\alpha_i = \sum_{j=1}^n \beta_{ij} f_j$. Тада имамо да је

$$e = \sum_{i=1}^m \sum_{j=1}^n \beta_{ij} f_j e_i = \sum_{1 \leq i \leq m, 1 \leq j \leq n} \beta_{ij} e_i f_j,$$

па имамо да је скуп \mathcal{G} једна генератриса за E над G . Да бисмо показали да је то линеарно независан скуп вектора, пођимо од релације

$$\sum_{1 \leq i \leq m, 1 \leq j \leq n} \beta_{ij} e_i f_j = 0_E.$$

Ако је $\alpha_i := \sum_{j=1}^n \beta_{ij} f_j \in F$, добијамо да је

$$\sum_{i=1}^m \alpha_i e_i = 0_E.$$

Како је $[e_1, \dots, e_m]$ база за E над F , онда имамо да је $\alpha_1 = \dots = \alpha_m = 0_F$. Из релације $\alpha_i = 0_F$ имамо да је $\sum_{j=1}^n \beta_{ij} f_j = 0_F$. Но, $[f_1, \dots, f_n]$ је база за F над G , па добијамо да је $\beta_{ij} = 0_G$ за све i, j те заиста елементи $e_j f_j$ чине базу за E над G . \square

Теорема о примитивном елементу

Дефиниција 99 Нека је A комутативни прстен са јединицом. Прстен A има карактеристику $n > 0$ уколико је n најмањи позитиван број за који је

$$n1_A = \underbrace{1_A + \dots + 1_A}_n = 0_A.$$

Уколико је $k1_A \neq 0_A$, за све $k > 0$ кажемо да је A карактеристике 0.

За поља чија је карактеристика неки позитиван цео број кажемо да су поља коначне карактеристике.

Став 100 Карактеристика сваког поља је или 0 или прост број.

Доказ. Нека је K поље коначне карактеристике n . Ако n не би био прост број, било би $n = a \cdot b$, за неке $a, b > 1$. Но, тада је

$$0_A = n1_A = (ab)1_A = (a1_A)(b1_A).$$

Но, како у пољу нема правих делитеља нуле (поновите основне ствари о пољима из Алгебре 1), следи да је $a1_A = 0_A$ или $b1_A = 0_A$. Но, како су и a и b позитивни бројеви мањи од n , то противречи чињеници да је K карактеристике n . Закључујемо да n мора бити прост број. \square

Приметимо да у пољу карактеристике 0 за целе бројеве r, s важи да је $r1_A = s1_A$ ако и само ако је $r = s$ (размислите зашто је ово тачо). Типичан пример поља карактеристике 0 је поље \mathbb{Q} , а поља карактеристике p је поље \mathbb{Z}_p . Но, нису ова поља само типични примери.

Став 101 Поље је карактеристике 0 ако и само ако садржи као своје потпоље поље изоморфно са \mathbb{Q} , док је поље карактеристике p ако и само ако садржи као своје потпоље поље изоморфно са \mathbb{Z}_p .

Доказ. Нека је K поље карактеристике 0. То значи да је $n1_K \neq 0_K$ за све позитивне целе бројеве n . Осим тога, за $m_1, m_2 \in \mathbb{Z}$ и $n_1, n_2 \in \mathbb{N} \setminus \{0\}$ важи:

$$\frac{m_1}{n_1} = \frac{m_2}{n_2} \text{ ако и само ако је } (m_1 1_K)(n_1 1_K)^{-1} = (m_2 1_K)(n_2 1_K)^{-1}.$$

Наиме, $\frac{m_1}{n_1} = \frac{m_2}{n_2}$ ако и само ако је $m_1 n_2 = m_2 n_1$. Но, с обзиром да је K поље карактеристике нула ово је еквивалентно са $(m_1 n_2) 1_K = (m_2 n_1) 1_K$, те и са $(m_1 1_K)(n_2 1_K) = (m_2 1_K)(n_1 1_K)$, што је коначно еквивалентно са $(m_1 1_K)(n_1 1_K)^{-1} = (m_2 1_K)(n_2 1_K)^{-1}$. То значи да је $f(\frac{m}{n}) := (m 1_K)(n 1_K)^{-1}$ добро задата функција $f: \mathbb{Q} \rightarrow K$ за коју се лако провери да је један хомоморфизам. Но, с обзиром да је \mathbb{Q} поље, језгро овог хомоморфизма је $\{0\}$ (језгро је увек идеал, а пошто су једини идеали у пољу тривијални, овај идеал је нула идеал), те је f изоморфизам између \mathbb{Q} и своје слике која је тражено потпоље од K .

Случај коначне карактеристике се на сличан начин може обрадити. Нека је K поље карактеристике p . Можемо задати хомоморфизам прстена $g: \mathbb{Z} \rightarrow K$ са $g(m) = m 1_K$ (уверите се да је ово заиста хомоморфизам). С обзиром да је карактеристика поља K једнака p , добија се да је језгро овог хомоморфизма идеал генерисан простим бројем p . Стога је $\mathbb{Z}/p\mathbb{Z}$ изоморфно слици хомоморфизма g што је и тражено потпоље од K изоморфно пољу \mathbb{Z}_p . \square

Већ смо се упознали са раширењима облика $F(\alpha)$. Но, ако $\beta \notin F(\alpha)$, може се формирати и раширење $F(\alpha)(\beta)$, које се краће означава са $F(\alpha, \beta)$. Општије, имамо и раширења $F(\alpha_1, \dots, \alpha_n)$.

Став 102 Нека E раширење поља F . Означимо са \overline{F} све елементе из E који су алгебарски над пољем F . Тада је \overline{F} потпоље поља E .

Доказ. Јасно је да је $1_E = 1_F \in \overline{F}$. Треба доказати да из чињенице да $\alpha, \beta \in \overline{F}$ следи да и $\alpha \pm \beta, \alpha \cdot \beta, \alpha \cdot \beta^{-1} \in \overline{F}$, при чему, наравно, за последњу релацију тражимо да је $\beta \neq 0$.

Како сви ови елементи припадају пољу $F(\alpha, \beta)$, то је, на основу става **97** довољно доказати да је $F(\alpha, \beta)$ коначно раширење поља F . Но,

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)] \cdot [F(\alpha) : F],$$

а $[F(\alpha) : F]$ је коначно, јер је α алгебарски над F , а $[F(\alpha, \beta) : F(\alpha)]$ је коначно, јер је β алгебарски над F , па тиме и над $F(\alpha)$. Ово завршава доказ. \square

Веома је занимљив следећи резултат.

Теорема 103 (Теорема о примитивном елементу) Свако коначно раширење E поља F , где је $F = \mathbb{Q}$ или је F коначно поље, је облика $F(\alpha)$, за неко $\alpha \in E$.

Елемент α је тај примитивни елемент раширења E .

Доказ за коначна поља. Пошто је поље F коначно, а E коначно раширење од F , то је, као векторски простор над F , поље E изоморфно са F^n , где је n степен раширења, па је и само коначно. Но, према теорема из Алгебре 1, која каже да је свака коначна подгрупа мултипликативне групе поља циклична, то је и $(E \setminus \{0\}, \cdot)$ циклична, па постоји $\alpha \in E$ такав да је $E \setminus \{0\} = \{0, \alpha, \alpha^2, \dots, \alpha^{q-1}\}$, где је $|E| = q$. Стога је $E = F(\alpha)$. \square

Приметимо да раширење поља има исту карактеристику као и само поље (зашто је то тако?).

Вишеструке нуле полинома

Као што смо видели, за сваки полином $f(X) \in F[X]$ постоји раширење E поља F у коме се он може факторисати у линеарне факторе. Но, да ли су ти фактори различити? Другим речима, да ли полином $f(X)$ у неком раширењу има вишеструке нуле? Сада ћемо се позабавити тим питањем.

Дефиниција 104 Полином $f \in F[X]$ има двоструку нулу $\alpha \in F$ уколико $(X - \alpha)^2 \mid f(X)$. На аналогни начин се дефинише и појам n -тоструке нуле за ма које $n \geq 2$.

Пре свега, извод полинома се може формално дефинисати, без икаквог граничног процеса и за полиноме над произвољним пољима (па и комутативним прстенима са јединицом) на следећи начин.

Дефиниција 105 Нека је $f(X) = a_0 + a_1X + \dots + a_nX^n \in F[X]$. Тада се извод полинома дефинише са:

$$f'(X) := a_1 + 2a_2X + \dots + na_nX^{n-1}.$$

Може се проверити да су уобичајена правила за изводе и овде испуњена. На пример, Лајбницово правило: $(fg)' = f'g + fg'$, а важи и следеће: $((X - \alpha)^n)' = n(X - \alpha)^{n-1}$. Добро би било да се у то читалац сам увери.

Докажимо најпре основни став.

Став 106 Полином $f \in F[X]$ има двоструку нулу $\alpha \in F$ ако $f(\alpha) = f'(\alpha) = 0$.

Доказ. \implies : Претпоставимо да је α двострука нула полинома f . Тада је $f(X) = (X - \alpha)^2 g(X)$ за неки полином $g(X) \in F[X]$. Добијамо да је

$$f'(X) = 2(X - \alpha)g(X) + (X - \alpha)^2 g'(X),$$

из чега следи да је и $f'(\alpha) = 0$.

\impliedby : Претпоставимо да је $f(\alpha) = f'(\alpha) = 0$. Поделитем еуклидски $f(X)$ полиномом $(X - \alpha)^2$. Добијамо

$$f(X) = (X - \alpha)^2 q(X) + a + bX,$$

за неке $a, b \in F$. Тада је

$$f'(X) = 2(X - \alpha)^2 q'(X) + (X - \alpha)^2 q'(X) + b,$$

те је

$$f(\alpha) = a + b\alpha, \quad f'(\alpha) = b.$$

Стога је $0 = a + b\alpha$ и $0 = b$, па добијамо да је $a = b = 0$ те $(X - \alpha)^2 \mid f(X)$ што се и тражило. \square

Није тешко доказати ни генерализацију овог става: полином има n -тоструку нулу α ако и само ако је $f(\alpha) = f'(\alpha) = \dots = f^{(n-1)}(\alpha) = 0$.

Став 107 Нека је $f(X) \in F[X]$. Тада f има вишеструку нулу у неком раширењу E поља F ако и само ако је $\text{NZD}(f(X), f'(X)) \neq 1$.

Доказ. \implies : Претпоставимо да постоји раширење E поља F и елемент $\alpha \in E$ такав да је $f(\alpha) = f'(\alpha) = 0$ (видети претходни став). Уколико би важило да је $\text{NZD}(f(X), f'(X)) = 1$, онда би постојали полиноми $p(X)$ и $q(X)$ такви да је

$$f(X)p(X) + f'(X)q(X) = 1.$$

Но, тада бисмо добили

$$f(\alpha)p(\alpha) + f'(\alpha)q(\alpha) = 1,$$

тј. $0 = 1$. Дакле, $\text{NZD}(f(X), f'(X)) \neq 1$.

\impliedby : Нека је $d(X) = \text{NZD}(f(X), f'(X)) \neq 1$. Како је $\deg d(X) > 0$, на основу ранијих резултата постоји раширење E поља F и елемент $\alpha \in E$ такав да је $d(\alpha) = 0$. С обзиром да $d(X) \mid f(X)$ и $d(X) \mid f'(X)$ добијамо да је и $f(\alpha) = 0$ и $f'(\alpha) = 0$, што показује да полином $f(X)$ у том раширењу поља F има вишеструку нулу. \square

Пажљив читалац је можда већ закључио да у произвољном пољу не мора важити следећа једнакост (која нам је позната из средње школе за реалне полиномске функције): $\deg f'(X) = \deg f(X) - 1$. На пример, за полином $f(X) = X^{15} + 3X^5 + 2 \in \mathbb{Z}_5[X]$ добијамо да је $f'(X) = 0$. Сада би следећи резултат требало да буде мало мање неочекиван.

Став 108 Нека је $f(X) \in F[X]$ нерастављив полином. Тада он има вишеструку нулу у неком раширењу E поља F ако и само ако је $f'(X) = 0$.

Доказ. На основу претходног става $f(X)$ има вишеструку нулу у неком раширењу ако и само ако је $\text{NZD}(f(X), f'(X)) \neq 1$. Но, с обзиром да $\text{NZD}(f(X), f'(X)) \mid f(X)$ и да је $f(X)$ нерастављив и моничан, добијамо да је $f(X) = \text{NZD}(f(X), f'(X))$. Дакле, $f(X) \mid f'(X)$. С обзиром на то да је $\deg f'(X) < \deg f(X)$, ово је могуће само ако је $f'(X) = 0$. \square

Пример 109 Нека је $F = \mathbb{Z}_3(t)$ и $a(X) = X^3 - t \in F[X]$. Показати да је $a(X)$ нерастављив полином и да он има троструку нулу у неком раширењу E поља F .

Пошто је $a(X)$ полином степена 3, он је растављив ако и само ако има корен у пољу $\mathbb{Z}_3(t)$. Како је $a(X)$ моничан из $\mathbb{Z}_3[t][X]$, на основу става **88** добијамо да он има корен у $\mathbb{Z}_3[t]$, тј. да постоји полином $p(t) \in \mathbb{Z}_3[t]$ такав да је $p(t)^3 - t = 0$. Свакако $p(t)$ није константан полином, те је $\deg(p(t)^3) = 3 \deg p(t) \neq 1 = \deg t$, па је $p(t)^3 - t \neq 0$. Дакле, $a(X)$ је нерастављив полином. Но, приметимо да је $a'(X) = 3X^2 = 0$, па има вишеструку нулу у неком раширењу поља F . Он свакако има раширење у коме има неку нулу α (то раширење можемо добити као $F[X]/\langle a(X) \rangle$). То значи да је $\alpha^3 - t = 0$ у $E[X]$. Но, тада је заправо

$$a(X) = X^3 - t = X^3 - \alpha^3 = (X - \alpha)^3,$$

у $E[X]$ пошто је $\text{char } E = \text{char } \mathbb{Z}_3(t) = \text{char } \mathbb{Z}_3 = 0$, те је α трострука нула полинома $a(X)$ у раширењу E . \clubsuit

Коначна поља

Докажимо најпре следећу једноставну чињеницу.

Став 110 Свако коначно поље има p^n елемената, за неки прост број p и природан број $n \geq 1$.

Доказ. Нека је F неко коначно поље. Знамо да оно мора да има коначну карактеристику p за неки прост број p те стога садржи, као своје потпоље, поље изоморфно пољу \mathbb{Z}_p . Дакле, F је једно раширење поља \mathbb{Z}_p . Како је F коначно, оно је и коначно раширење поља \mathbb{Z}_p . Ако је $[F : \mathbb{Z}_p] = n$, онда је, као векторски простор над пољем \mathbb{Z}_p , изоморфно са $(\mathbb{Z}_p)^n$, те има p^n елемената. \square

Наш задатак ће бити да покажемо да за сваки прост број p и свако $n \geq 1$ постоји, до на изоморфизам, тачно једно поље које има p^n елемената. У даљем ћемо поље \mathbb{Z}_p означавати са \mathbb{F}_p .

Анализирајмо мало поље са p^n елемената. Знамо свакако да нека таква постоје.

Став 111 Нека је F поље са $q = p^n$ елемената, где је p прост број и $n \geq 1$. Тада се у пољу F полином $a(X) = X^q - X$ факторише на различите линеарне факторе.

Доказ. Посматрајмо групу $(F \setminus \{0\}, \cdot)$. Подсетимо се следеће чињенице из Алгебре 1: ако је $x \in G$, где је G коначна група, онда је $x^{|G|} = e$ (поновите овај део из Алгебре 1). Дакле, ако је $\alpha \in F \setminus \{0\}$, онда је $\alpha^{q-1} = 1$, те је и $\alpha^q = \alpha$. С обзиром да ова једнакост важи и када је $\alpha = 0$, добијамо да је $a(\alpha) = 0$ за све $\alpha \in F$. Како је овај полином степена q , он не може имати више од q нула, а већ су сви елементи из F , којих има q , нуле овог полинома. То значи да су то и све нуле овог полинома, тј. $X^q - X = \prod_{\alpha \in F} (X - \alpha)$, чиме је доказ завршен. \square

Претходни став нам помаже да покажемо да поља са p^n елемената постоје.

Теорема 112 За сваки прост број p и природан број $n \geq 1$ постоји поље са p^n елемената.

Доказ. Нека је $q = p^n$ и $a(X) = X^q - X \in \mathbb{F}_p[X]$. Знамо да постоји поље F које је раширење поља \mathbb{F}_p (подсетимо се да је \mathbb{F}_p заправо \mathbb{Z}_p) у којем полином $a(X)$ има факторизацију на линеарне факторе (то је тачно за сваки полином, па стога и за овај). С обзиром да је $a'(X) = -1$, полином $a(X)$ нема вишеструких нула нигде, те он у F има факторизацију у производ различитих линеарних фактора.

Нека је $L = \{\alpha \in F : \alpha^q = \alpha\}$ (другим речима, L чине све нуле полинома $a(X)$, а оне се налазе у пољу F). Доказаћемо да је L тражено поље са $q = p^n$ елемената. Како се $X^q - X$ факторише на производ различитих линеарних фактора у F , он у F има q нула, те је $|L| = q$. Докажимо да је L потпоље од F .

- Нека $\alpha, \beta \in L$. Тада је $(\alpha \cdot \beta)^q = \alpha^q \cdot \beta^q = \alpha \cdot \beta$, па закључујемо да $\alpha \cdot \beta \in L$.
- Нека је $\alpha \in L \setminus \{0\}$. Тада, дељењем једнакости $\alpha^q = \alpha$ са α^{q+1} добијамо да је $\alpha^{-1} = \alpha^{-q} = (\alpha^{-1})^q$, те $\alpha^{-1} \in L$.
- Нека $\alpha, \beta \in L$. Како F садржи као своје потпоље поље \mathbb{F}_p , то је карактеристика поља F једнака p , те је $p\gamma = 0$ за све $\gamma \in F$. Подсетимо се још и чињенице да је $p \mid \binom{p}{k}$ за све $1 \leq k \leq p-1$ те је $\binom{p}{k} = q_k p$ за неко $q_k \in \mathbb{N}$. Стога, у пољу F важи да је

$$(\alpha - \beta)^p = \alpha^p + \sum_{k=1}^{p-1} \binom{p}{k} (-1)^k \alpha^{p-k} \beta^k + \beta^p = \alpha^p - \beta^p,$$

јер је, за све $1 \leq k \leq p-1$: $\binom{p}{k} \alpha^{p-k} \beta^k = q_k (p \alpha^{p-k} \beta^k) = 0$, као што је примећено горе. Сада није тешко показати индукцијом да је

$$(\alpha - \beta)^{p^r} = \alpha^{p^r} - \beta^{p^r},$$

за све $r \geq 1$, те је и $(\alpha - \beta)^q = \alpha^q - \beta^q = \alpha - \beta$. Закључујемо да и $\alpha - \beta \in L$, што и завршава доказ чињенице да је L потпоље од F , те је L тражено поље са q елемената. \square

Покажимо сада јединственост.

Теорема 113 Нека су K и K' поља са p^n елемената где је p прост број и $n \geq 1$. Тада је $K \cong K'$.

Доказ. Поље K је коначно раширење поља \mathbb{F}_p . Нека је α примитивни елемент тог раширења, тј. нека је $K = \mathbb{F}_p(\alpha)$.

Нека је $\mu_\alpha(X)$ минимални полином за α над \mathbb{F}_p . Тада је $\mathbb{F}_p[X]/\langle \mu_\alpha(X) \rangle \cong \mathbb{F}_p(\alpha) (= K)$. Дакле, $\mu_\alpha(\alpha) = 0$, а такође је и $a(\alpha) = 0$, где је $a(X) = X^q - X$. Како је $\mu_\alpha(X)$ минимални полином, можемо да закључимо да $\mu_\alpha(X) \mid a(X)$.

„Пређимо” сада у поље K' . У њему су такође све нуле полинома $a(X)$, те из чињенице да $\mu_\alpha(X) \mid a(X)$ следи да $\mu_\alpha(X)$ има нулу у K' . Нека је α' једна нула полинома $\mu_\alpha(X)$ у K' . Тада је $\mathbb{F}_p(\alpha') \cong \mathbb{F}_p[X]/\langle \mu_\alpha(X) \rangle \cong K$, те је K изоморфно потпољу $\mathbb{F}_p(\alpha')$ поља K' . Но, како су поља K и K' коначна поља са истим бројем елемената закључујемо да је заправо $\mathbb{F}_p(\alpha') = K'$ и $K \cong K'$. \square

Показали смо да за сваки прост број p и природан $n \geq 1$ постоји поље са p^n елемената и да су свака два таква поља изоморфна. Стога је оправдано увести ознаку \mathbb{F}_q за поље са q елемената. За крај овог дела испитајмо када је неко коначно поље потпоље другог коначног поља.

Став 114 Поље са p^m елемената је потпоље поља са p^n елемената ако и само ако $m \mid n$.

Доказ. \Leftarrow . Нека је $q = p^n$ и $r = p^m$, где $m \mid n$. То коначно поље са q елемената означимо са \mathbb{F}_q . Посматрајмо, као у доказу теореме **112**, подскуп L :

$$L = \{\alpha \in \mathbb{F}_q : \alpha^r = \alpha\}.$$

И овде се лако провери да је L потпоље поља \mathbb{F}_q . Поставља се питање колико има елемената у L . Рекло би се, ако се не промисли, да је јасно да има $r = p^m$ елемената. Али, ми нигде нисмо користили да $m \mid n$. У доказу теореме **112** било нам је важно да у пољу F (овде је то поље \mathbb{F}_q) полином $X^q - X$ има факторизацију у производ различитих линеарних фактора, Овде нам, дакле, треба да полином $X^r - X$ има исто својство. Наиме, ми не знамо да су све нуле полинома $X^r - X$ садржане у \mathbb{F}_q . У ту сврху ће нам користити претпоставка да $m \mid n$. Наиме, покажимо да

$$(X^{p^m} - X) \mid (X^{p^n} - X),$$

ако $m \mid n$. Лако се види да је ово еквивалентно са:

$$(X^{p^m-1} - 1) \mid (X^{p^n-1} - 1).$$

Следећи резултат је лак за доказивање, а веома користан: ако $k \mid l$ онда $(X^k - 1) \mid (X^l - 1)$ у прстену $\mathbb{Z}[X]$. Ово следи из још једноставније чињенице: за сваки $s \geq 1$: $(Y - 1) \mid (Y^s - 1)$ у $\mathbb{Z}[Y]$:

$$Y^s - 1 = (Y - 1)(Y^{s-1} + \dots + Y + 1).$$

Сада, како је $l = ks$ за неко s , постављајући $Y = X^k$ имамо:

$$\begin{aligned} X^l - 1 &= X^{ks} - 1 = (X^k)^s - 1^s = Y^s - 1 = (Y - 1)(Y^{s-1} + \dots + Y + 1) \\ &= (X^k - 1)((X^k)^{s-1} + (X^k)^{s-2} + \dots + X^k + 1). \end{aligned}$$

Из овог резултата, рачунајући у тачки $p \in \mathbb{Z}$, ако $m \mid n$ добијамо да $(p^m - 1) \mid (p^n - 1)$. А потом, још једном применом овог резултата, добијамо да $(X^{p^m-1} - 1) \mid (X^{p^n-1} - 1)$.

Сада из чињенице да полином $X^{p^m} - X$ дели $X^{p^n} - X$ и да полином $X^{p^n} - X$ има линеарну факторизацију у производ различитих фактора у $\mathbb{F}_q[X]$, добијамо да и $X^{p^m} - X$ има такву факторизацију у $\mathbb{F}_q[X]$. То нам је довољно да закључимо да је L поље са p^m елемената.

\implies . Дакле, нека је F поље са p^m елемената, E поље са p^n елемената, F потпоље од E . Но, тада је и група $U(F)(= F \setminus \{0\})$ подгрупа групе $U(E)$, па $|U(F)|$ дели $|U(E)|$. Дакле, $(p^m - 1) \mid (p^n - 1)$. Сада ћемо ипак морати да докажемо јачи резултат од претходног. Наиме, важи следеће: ако је остатак при дељењу n са m једнак r , онда је остатак при дељењу $X^n - 1$ са $X^m - 1$ једнак $X^r - 1$. Дакле, нека је $n = mq + r$, где је $0 \leq r < m$. Тада је

$$X^n - 1 = X^{mq+r} - 1 = X^{mq}X^r - 1 = (X^{mq} - 1 + 1)X^r - 1 = (X^{mq} - 1)X^r + X^r - 1,$$

а како знамо да $(X^m - 1) \mid (X^{mq} - 1)$ добијамо тражено. Ако ово срачунамо у p , добијамо:

$$p^n - 1 = (p^{mq} - 1)p^r + p^r - 1,$$

те из $(p^m - 1) \mid (p^n - 1)$, узимајући у обзир да $(p^m - 1) \mid (p^{mq} - 1)$, добијамо да $(p^m - 1) \mid (p^r - 1)$. Како је $0 \leq r < m$, ово је могуће само ако је $r = 0$, тј. ако $m \mid n$ што се и тражило. \square

На пример, поље \mathbb{F}_4 није потпоље од \mathbb{F}_8 , јер $2 \nmid 3$, али јесте потпоље од \mathbb{F}_{16} , јер $2 \mid 4$. Заправо се може узети да је $\mathbb{F}_4 = \{\alpha \in \mathbb{F}_{16} : \alpha^4 = \alpha\}$.

Овде се завршава материјал за други колоквијум.

Факторизација на нерастављиве у $\mathbb{F}_q[X]$; Берлекампов алгоритам

У овом одељку бавимо се факторизацијом полинома из $\mathbb{F}_q[X]$ на нерастављиве факторе. Приказаћемо Берлекампов алгоритам, који се примењује у ову сврху и то на бесквадратне полиноме, тј. оне који немају поновљене нерастављиве факторе. Код факторизације полинома f најпре проверавамо да ли је $f' = 0$. Уколико је то тако, онда је полином f p -ти степен неког полинома g и прелазимо на испитивање факторизације g . Уколико је $f' \neq 0$, посматрамо $d = \text{NZD}(f, f')$. Уколико је $d = 1$, онда знамо да полином f нема вишеструких нула у ма ком раширењу, а тиме знамо и да нема поновљене нерастављиве факторе и можемо да наставимо по алгоритму, који ћемо приказати. Уколико је $d \neq 1$, онда се проблем факторизације дели на проблем факторизације полинома d , за који се понавља претходни поступак, и и полинома f/d који нема поновљене факторе. Докажимо да је то заиста тако.

Став 115 Нека је $q = p^n$, за неки прост број p и $n \geq 1$, $f \in \mathbb{F}_q[X]$. Ако је $d = \text{NZD}(f, f')$, онда је полином f/d бесквадратни.

Доказ. Претпоставимо да постоји неконстантан полином b , такав да b^2 дели f/d . Тада је $f = db^2c$ за неки полином c . Тада је $f' = d'b^2c + 2dbb'c + db^2c'$. Видимо да $b \mid f'$. Како $b \mid f$, то $b \mid d$ те је $d = bd_1$ за неки полином d_1 . Дакле, $f = d_1b^3c$. Из $f' = d_1'b^3c + 3d_1b^2b'c + d_1b^3c'$ и следи да $b^2 \mid f'$. Како $b^2 \mid f$, добијамо да $b^2 \mid d$ и поступак се понавља неограничено. Ова контрадикција завршава доказ. \square

Докажимо један једноставан став, који ће нам бити од централног значаја за касније.

Став 116 Нека $f \mid g_1g_2 \cdots g_s$, при чему су $f, g_1, \dots, g_s \in \mathbb{F}_q[X]$ и $\text{NZD}(g_i, g_j) = 1$ за $i \neq j$. Тада је

$$f = \text{NZD}(f, g_1)\text{NZD}(f, g_2) \cdots \text{NZD}(f, g_s).$$

Доказ. Дакле, претпоставимо да $f \mid g_1g_2 \cdots g_s$. Нека је $f = p_1^{r_1} \cdots p_k^{r_k}$ факторизација f на нерастављиве полиноме. Како су g_i пар-по-пар узајамно прости, они немају заједничких делилаца. За $1 \leq i \leq s$, нека је:

$$I_i = \{j \in \{1, \dots, k\} : p_j \mid g_i\}.$$

Наравно, из $p_j \in I_i$, следи да $p_j^{r_j} \mid g_i$. Стога је

$$\text{NZD}(f, g_i) = \prod_{j \in I_i} p_j^{r_j}.$$

Како је $\{1, \dots, k\} = I_1 \sqcup I_2 \sqcup \dots \sqcup I_s$, добијамо да је

$$f = \text{NZD}(f, g_1) \text{NZD}(f, g_2) \cdots \text{NZD}(f, g_s). \quad \square$$

Дакле, идеја је да нађемо погодне g_i , који ће нам генерисати тражену факторизацију f на нерастављиве факторе. У нашем случају нема поновљених фактора у f , али горње тврђење важи и за општију ситуацију, па смо га зато за општи случај и формулисали.

Посматрајмо полином $h \in F_q[X]$ такав да $f \mid (h^q - h)$. Видећемо како ћемо наћи такав полином, за сада само претпоставимо да га имамо. Знамо да у $F_q[X]$ имамо факторизацију:

$$X^q - X = \prod_{c \in \mathbb{F}_q} (X - c),$$

Из ње добијамо факторизацију

$$h^q - h = \prod_{c \in \mathbb{F}_q} (h - c).$$

Приметимо да су полиноми $h - c$ и $h - c'$ за $c \neq c'$ узајамно прости. Наиме, ако је $d = \text{NZD}(h - c, h - c')$ онда и $d \mid ((h - c') - (h - c))$ те $d \mid (c - c')$, те следи да је $d = 1$. Дакле, из чињенице да $f \mid (h^q - h)$ добијамо да је

$$f = \prod_{c \in \mathbb{F}_q} \text{NZD}(f, h - c).$$

Треба приметити да ово јесте факторизација f на узајамно просте факторе, но то не морају нужно бити нерастављиви фактори, а свакако су многи чланови у овом производу једнаки 1. Стога нам није довољно наћи само један такав полином h . Треба нам више таквих, те се комбинацијом више факторизација добија тражено.

Како $f \mid (h^q - h)$, то је природно посматрати количнички прстен $\mathbb{F}_q[X]/\langle f \rangle$. Ако са \bar{h} означимо класу полинома h у овом прстену, имамо да је у њему $\bar{h}^q = \bar{h}$. Нека је $f = f_1 f_2 \cdots f_k$ факторизација f на производ нерастављивих. Знамо да су они сви различити, не знамо који су то полиноми. А не знамо ни колико их има. Но, посматрајмо идеале $P_i = \langle f_i \rangle$. Како су полиноми f_i нерастављиви, идеали P_i су максимални и $\mathbb{F}_q[X]/P_i$ су коначна поља која су раширења поља \mathbb{F}_q . Из максималности идеала P_i следи да је $P_i + P_j = \mathbb{F}_q[X]$ за $i \neq j$ (зашто је то тако?). Кинеска теорема о остацима, тј. теорема **48**, нам даје:

$$\mathbb{F}_q[X]/P_1 \cap P_2 \cap \cdots \cap P_k \cong \mathbb{F}_q[X]/P_1 \times \mathbb{F}_q[X]/P_2 \times \cdots \times \mathbb{F}_q[X]/P_k.$$

Но, знамо да је за копросте идеале P_i, P_j , на основу става **46**: $P_i \cap P_j = P_i \cdot P_j$. Уз тај став и лему **47** (видети и коментар после доказа теореме **48**) имамо да је $P_1 \cap P_2 \cap \cdots \cap P_k = P_1 \cdot P_2 \cdots P_k$. Како је

$$P_1 \cdot P_2 \cdots P_k = \langle f_1 \rangle \cdot \langle f_2 \rangle \cdots \langle f_k \rangle = \langle f_1 f_2 \cdots f_k \rangle = \langle f \rangle,$$

добијамо да је

$$\mathbb{F}_q[X]/\langle f \rangle \cong \mathbb{F}_q[X]/P_1 \times \mathbb{F}_q[X]/P_2 \times \cdots \times \mathbb{F}_q[X]/P_k.$$

Ако је $\bar{h} \in \mathbb{F}_q[X]/\langle f \rangle$ такав елемент да је $\bar{h}^q = \bar{h}$, онда он при овом изоморфизму одговара k -торци елемената

$$(\bar{h}_1, \bar{h}_2, \dots, \bar{h}_k) \in \mathbb{F}_q[X]/P_1 \times \mathbb{F}_q[X]/P_2 \times \cdots \times \mathbb{F}_q[X]/P_k$$

таквој да је

$$(\bar{h}_1, \bar{h}_2, \dots, \bar{h}_k)^q = (\bar{h}_1, \bar{h}_2, \dots, \bar{h}_k),$$

те је $\bar{h}_i^q = \bar{h}_i$ за све $i = \overline{1, k}$. С обзиром да су, а приори, полиноми f_i различитог степена и поља $F_i = \mathbb{F}_q[X]/P_i$ могу бити неизоморфна за различите индексе i , али знамо да елементи x у тим пољима, за које важи $x^q = x$ нужно припадају потпољу \mathbb{F}_q . Другим речима, сви елементи \bar{h}_i су елементи из \mathbb{F}_q . Дакле, $(\bar{h}_1, \bar{h}_2, \dots, \bar{h}_k) \in \mathbb{F}_q^k$. Стога је и

$$W = \left\{ \bar{h} \in \mathbb{F}_q[X]/\langle f \rangle : \bar{h}^q = \bar{h} \right\}$$

један векторски простор над \mathbb{F}_q димензије k . Прстен $V = \mathbb{F}_q[X]/\langle f \rangle$ није поље (сем ако је сам f нерастављив), али је свакако векторски простор над \mathbb{F}_q . Ако је $\deg f = n$, погодна база за овај простор је $e = [\overline{1}, \overline{X}, \dots, \overline{X}^{n-1}]$. Ово се може видети као и у случају када је f нерастављив. А, како је карактеристика овог прстена једнака p ($q = p^n$), то за све $u, v \in V$ важи: $(u + v)^q = u^q + v^q$. Наш задатак је да нађемо потпростор $W \leq V$ који чине елементи $u \in V$ такви да је $u^q = u$. Како смо видели да је пресликавање $\beta: V \rightarrow V$ дефинисано са $\beta(u) = u^q$ једно линеарни оператор простора V , то је $W = \text{Ker}(\beta - I_V)$, где смо са I_V означили идентични оператор на простору V . Дакле, ако одредимо $\text{Ker}(\beta - I_V)$ знаћемо колико има фактора у факторизацији за f . А затим ћемо, користећи став **116** покушати да одредимо и саму факторизацију.

За налажење $\text{Ker}(\beta - I_V)$ је, као што добро знамо из линеарне алгебре, најкорисније наћи матрицу тог оператора. Означимо са B матрицу линеарног оператора β , тј. нека је $B = [\beta]_e$. Тада је $[\beta - I_V]_e = B - I_n$, где смо са I_n означили јединичну матрицу реда n . Матрицу за β налазимо тако што нађемо слике базних елемената: $\beta(\overline{X}^i)$, изразимо их у бази e и од тих координата формирамо колоне матрице B . Потом се тражено језгро добија решавањем хомогеног система једначина $(B - I_n)X = O$.

Овим је теоријски део завршен. Време је за пример!

Пример 117 Нека је $f = X^7 + 2X^6 + X^5 + 2X^4 + 2X^2 + 2 \in \mathbb{F}_3[X]$. Наћи факторизацију f на нерастављиве полиноме у $\mathbb{F}_3[X]$.

Најпре морамо проверити да ли је полином бесквadratни. Имамо да је $f' = X^6 + 2X^4 + 2X^3 + X$. Добија се да је $d = \text{NZD}(f, f') = X + 1$. Као што смо рекли, факторизација се своди на факторизацију f/d и d . Но, за d је то већ урађено. Пређимо на f/d . Означимо га са g . Имамо да је $g = f/d = X^6 + X^5 + 2X^3 + X^2 + X + 2$.

База простора V је $e = [\bar{1}, \bar{X}, \bar{X}^2, \bar{X}^3, \bar{X}^4, \bar{X}^5]$ и то је простор димензије 6, пошто је степен полинома g једнак 6. У нашем случају је $q = 3$ и потребно је елементе $(\bar{X}^i)^3$ за $i = \bar{0}, \bar{5}$ изразити у бази e .

$$\begin{aligned}\bar{1}^3 &= \bar{1}, \\ \bar{X}^3 &= \bar{X}^3, \\ (\bar{X}^2)^3 &= \bar{X}^6 = -\bar{X}^5 - 2\bar{X}^3 - \bar{X}^2 - \bar{X} - \bar{2} = 2\bar{X}^5 + \bar{X}^3 + 2\bar{X}^2 + 2\bar{X} + \bar{1}.\end{aligned}$$

Застанимо овде. Заправо, ако желимо да елемент $a(\bar{X})$, где је $a(X)$ ма који полином из $\mathbb{F}_3[X]$ изразимо у нашој бази, ми заправо треба да нађемо остатак при дељењу полинома $a(X)$ полиномом $g(X)$, односно да нађемо чему је он конгруентан по модулу $g(X)$ (како је коме погодно да ово посматра). За прва два случаја нисмо ништа имали да радимо, јер су то били полиноми степена мањег од 6. У последњем је било лако. У наредним случајевима је погодно користити већ добијено, само множити претходни са \bar{X}^3 и сређивати. Нећемо писати сав рачун пошто би било мало непрегледно, него само почетак и крај.

$$\begin{aligned}(\bar{X}^3)^3 &= 2\bar{X}^8 + \bar{X}^6 + 2\bar{X}^5 + 2\bar{X}^4 + \bar{X}^3 = \bar{X}^5 + \bar{X}^4 + \bar{X}^3 + \bar{X}^2 + \bar{X}, \\ (\bar{X}^4)^3 &= \bar{X}^8 + \bar{X}^7 + \bar{X}^6 + \bar{X}^5 + \bar{X}^4 = \bar{X}^5 + 2\bar{X} + \bar{1}, \\ (\bar{X}^5)^3 &= \bar{X}^8 + 2\bar{X}^4 + \bar{X}^3 = 2\bar{X}^3 + \bar{X}^2 + \bar{X} + \bar{1}.\end{aligned}$$

Сада можемо исписати матрице B и $B - I_6$. Обратите пажњу на редослед елемената у бази, степени расту.

$$B = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 2 & 1 & 2 & 1 \\ 0 & 0 & 2 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 2 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 1 & 1 & 0 \end{bmatrix}, \quad B - I_6 = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 2 & 2 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 2 \\ 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 2 & 1 & 1 & 2 \end{bmatrix}.$$

Решимо систем једначина $(B - I_6)X = O$.

$$\begin{array}{rcccccc} & & x_2 & & + & x_4 & + & x_5 & = & 0 \\ 2x_1 & + & 2x_2 & + & x_3 & + & 2x_4 & + & x_5 & = & 0 \\ & & x_2 & + & x_3 & & & + & x_5 & = & 0 \\ x_1 & + & x_2 & & & & & + & 2x_5 & = & 0 \\ & & & & x_3 & + & 2x_4 & & & = & 0 \\ & & 2x_2 & + & x_3 & + & x_4 & + & 2x_5 & = & 0 \end{array}$$

Опште решење је

$$(x_0, x_1, x_2, x_3, x_4, x_5) = (\gamma, \alpha + 2\beta, 2\alpha + 2\beta, \alpha, \alpha, \beta), \quad \alpha, \beta, \gamma \in \mathbb{F}_3.$$

Другим речима:

$$W = \left\{ \gamma \cdot \bar{1} + (\alpha + 2\beta)\bar{X} + (2\alpha + 2\beta)\bar{X}^2 + \alpha\bar{X}^3 + \alpha\bar{X}^4 + \beta\bar{X}^5 : \alpha, \beta, \gamma \in \mathbb{F}_3 \right\}.$$

Дакле, $\dim W = 3$, те полином g има три нерастављива фактора. Ако је $h(\bar{X})$ произвољни елемент W , имамо да

$$g(X) \mid (h(X)^3 - h(X)) (= h(X)(h(X) - 1)(h(X) - 2)),$$

те је

$$g(X) = \text{NZD}(g(X), h(X))\text{NZD}(g(X), h(X) - 1)\text{NZD}(g(X), h(X) - 2).$$

Но, превише би било да проверавамо све полиноме који одговарају елементима W . Фокусираћемо се на једну базу тог простора коју чине полиноми $h_0(X) = 1$, $h_1(X) = X^4 + X^3 + 2X^2 + X$ и $h_2(X) = X^5 + 2X^2 + 2X$ (које смо добили наравно узимајући редом да је један од параметара једнак јединици, а да су остали нуле). Полином $h_0(X) = 1$ није од користи јер је константан полином (он се наравно појављује увек у овом поступку пошто је $1^q = 1$). Дакле, остала су нам два полинома и покушаћемо да нађемо факторизацију користећи њих.

$$\begin{aligned} \text{NZD}(g(X), h_1(X)) &= 1, \\ \text{NZD}(g(X), h_1(X) - 1) &= X^4 + X^3 + 2X^2 + X + 2, \\ \text{NZD}(g(X), h_1(X) - 2) &= X^2 + 1. \end{aligned}$$

Дакле, „крнуло је”, добили смо да је

$$g(X) = (X^4 + X^3 + 2X^2 + X + 2)(X^2 + 1). \quad (12)$$

Како $g(X)$ има три нерастављива фактора, ово сигурно није факторизација на нерастављиве. Но, нешто смо добили. Пређимо на h_2 .

$$\begin{aligned}\text{NZD}(g(X), h_2(X)) &= 1, \\ \text{NZD}(g(X), h_1(X) - 1) &= X^5 + 2X^2 + 2X + 2, \\ \text{NZD}(g(X), h_1(X) - 2) &= X + 1.\end{aligned}$$

Добијамо нову факторизацију:

$$g(X) = (X^5 + 2X^2 + 2X + 2)(X + 1). \quad (13)$$

Опет смо добили два фактора, али нова два фактора. Сада није тешко завршити ово. Наиме, $X + 1$ је очигледно нерастављив. Треба проверити да ли он дели неки од фактора у (12). Но, то се своди на проверу да ли је $-1 (= 2)$ корен неког од тих фактора. Како је $(-1)^4 + (-1)^3 + 2(-1)^2 + (-1) + 2 = 1 - 1 + 2 - 1 + 2 = 0$ у \mathbb{F}_3 , добијамо да $(X + 1) \mid (X^4 + X^3 + 2X^2 + X + 2)$. Заправо је

$$X^4 + X^3 + 2X^2 + X + 2 = (X + 1)(X^3 + 2X + 2)$$

и добили смо факторизацију $g(X)$ на нерастављиве:

$$g(X) = (X + 1)(X^2 + 1)(X^3 + 2X + 2).$$

Не смемо заборавити који нам је био основни задатак, а то је да нађемо факторизацију полинома $f(X) = X^7 + 2X^6 + X^5 + 2X^4 + 2X^2 + 2$. Узимајући у обзир да је $d = \text{NZD}(f, f') = X + 1$ и да имамо факторизацију $g = f/d$, коначно добијамо тражену факторизацију:

$$f(X) = (X + 1)^2(X^2 + 1)(X^3 + 2X + 2). \quad \spadesuit$$

Прстен полинома са више неодређених

Сада почињемо завршни део курса у коме ћемо се више позабавити полиномима са више неодређених. Нешто од тога смо већ имали, али овде нам је главни фокус на увођење појма ГРЕБНЕРОВИХ БАЗА које имају велики теоријски, али још више практичан значај при раду са идеалима у прстену са више неодређених над произвољним пољем. Најпре морамо доказати неке основне ствари.

Нетерини прстени

Као што смо већ видели, прстен полинома са n неодређених може се рекурзивно задати на следећи начин:

$$K[X_1, \dots, X_n] := K[X_1, \dots, X_{n-1}][X_n].$$

Прстен полинома са више неодређених, чак и ако је над пољем, нема више онолико правилности колико има прстен полинома са једном неодређеном. Но, као што смо већ навели, мада у прстену полинома са више неодређених није сваки идеал главни, ипак је сваки идеал коначно генерисан. Да бисмо то показали, користан нам је следећи став.

Став 118 Нека је A комутативан прстен са јединицом. Тада су следећи услови еквивалентни:

- (1) Сваки идеал у A је коначно генерисан.
- (2) Сваки растући низ идеала у A :

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

је стационаран, тј. постоји $m \geq 0$ тако да је $I_n = I_m$ за све $n \geq m$.

Доказ. (1) \implies (2): Посматрајмо унију ових идеала:

$$I = \bigcup_{j \geq 0} I_j.$$

Докажимо да је I идеал у A . Најпре, ако је $x \in I$ и $a \in A$, онда $x \in I_j$ за неко $j \geq 0$. Како је I_j идеал у A , закључујемо да $a \cdot x \in I_j \subseteq I$.

Уколико $x, y \in I$, онда $x \in I_{j_1}$ и $y \in I_{j_2}$, за неке $j_1, j_2 \geq 0$. Уколико је $j = \max\{j_1, j_2\}$, онда $x, y \in I_j$, па, пошто је I_j идеал, следи да $x + y \in I_j \subseteq I$.

Како је I идеал у A , он је по претпоставци коначно генерисан, те је

$$I = \langle x_1, \dots, x_k \rangle.$$

Како је I унија растућег низа идеала, закључујемо да је $x_s \in I_{j_s}$ за неке $j_s \geq 0$. Ако је $m = \max\{j_1, \dots, j_k\}$ онда $x_s \in I_m$ за све $s \in \{1, \dots, k\}$. Но, то управо значи да је $I = I_m$. Како је, за $n \geq m$:

$$I_m \subseteq I_n \subseteq I = I_m,$$

добијамо да је $I_n = I_m$ за све $n \geq m$, као што се и тражило.

(2) \implies (1): Претпоставимо да идеал I није коначно генерисан. То значи да, ако узмемо било који елемент $x_0 \in I$ тада $I \neq \langle x_0 \rangle = I_0$. Сада, ако узмемо било који елемент $x_1 \in I \setminus I_0$, $I \neq \langle x_0, x_1 \rangle = I_1$, јер I није коначно генерисан. Тада је $I_0 \subset I_1$. На аналогни начин налазимо низ елемената $x_i \in I$ тако да је

$$I_n = \langle x_0, \dots, x_n \rangle \subset I_{n+1} = \langle x_0, \dots, x_{n+1} \rangle,$$

тј. добијамо бесконачни строго растући низ идеала

$$I_0 \subset I_1 \subset I_2 \subset \dots$$

што противречи претпоставци (2). □

Дефиниција 119 За комутативан прстен A кажемо да је Нетерин ако испуњава било који од ова два еквивалентна услова.

Пример 120 Нека је A прстен свих непрекидних функција $f: [0, 1] \rightarrow \mathbb{R}$, при чему су операције међу функцијама дефинисане тачка по тачка:

$$(f + g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x).$$

Посматрајмо низ идеала $I_n = \{f \in A : (\forall x < \frac{1}{n})f(x) = 0\}$ (уверите се да је I_n идеал у A). Јасно је да је $I_n \subset I_{n+1}$. Наиме, како је $\frac{1}{n+1} < \frac{1}{n}$, јасно је да из $f(x) = 0$ за $x < \frac{1}{n}$ следи да је $f(x) = 0$ за $x < \frac{1}{n+1}$, но функција $g: [0, 1] \rightarrow \mathbb{R}$ дефинисана са

$$g(x) = \begin{cases} 0, & x \leq \frac{1}{n+1} \\ x - \frac{1}{n+1} & \text{иначе,} \end{cases}$$

припада I_{n+1} , али не припада I_n , те имамо бесконачан строго растући низ идеала. Дакле, прстен A није Нетерин. ♣

Овај пример нећемо даље користити, наведен је само зато да се покаже да постоје прстени који нису Нетерини. Задатак следећег одељка ће се састојати у томе да докажемо да прстени полинома са више неодређених ЈЕСУ Нетерини.

Хилбертова теорема о бази

Следећа теорема је од централног значаја. Из ње се лако изводи чињеница да је сваки идеал у прстену полинома са више неодређених над пољем коначно генерисан, што је предуслов за постојање разноврсних алгоритама у том прстену. Директан доказ ове чињенице не би био лакши од доказа ове теореме, запис би био и компликованији.

Теорема 121 (Хилбертова теорема о бази) Ако је прстен A Нетерин, онда је и прстен $A[X]$ Нетерин.

Доказ. Нека је I идеал у прстену $A[X]$. Дефинишимо идеал I_n у прстену A са:

$$I_n := \{a_n \in A : (\exists a(X) \in A[X])(\deg a(X) = n \text{ и } LC(a(X)) = a_n)\} \cup \{0\}.$$

Кратко: у I_n се налазе водећи коефицијенти свих полинома степена n који се налазе у идеалу I , а осим њих је ту и 0 (нула нам је неопходна да бисмо имали идеал, а морамо је овако додати, јер она не може бити водећи коефицијент ниједног ненула полинома).

Докажимо најпре да је I_n идеал у A . Нека је $a_n \in I_n$ и $b \in A$. Ако је $ba_n = 0$, онда свакако $ba_n \in I_n$. Ако је $ba_n \neq 0$ и ако је $a(X) \in I$

полином степена n у I чији је водећи коефицијент a_n , онда је $ba(X)$ полином степена n у I чији је водећи коефицијент ba_n , па закључујемо да $ba_n \in I_n$.

Уколико $a_n, b_n \in I_n$, нека су $a(X), b(X)$ полиноми степена n из I , такви да је $LC(a(X)) = a_n$, а $LC(b(X)) = b_n$. Ако је $a_n + b_n = 0$, онда је јасно да $a_n + b_n$ припада I_n . У супротном, полином $a(X) + b(X)$ је полином степена n из I (јер је I идеал) чији је водећи коефицијент $a_n + b_n$, те $a_n + b_n \in I_n$.

Није тешко доказати да је $I_n \subseteq I_{n+1}$. Наиме, ако је $a_n \in I_n$, онда постоји полином $a(X)$ из I степена n такав да је $LC(a(X)) = a_n$. Тада је $Xa(X)$ полином степена $n+1$ у I чији је водећи коефицијент такође a_n , те $a_n \in I_{n+1}$.

Тако смо добили растући низ идеала у A :

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

Како је прстен A Нетерин, то је овај низ идеала стационаран, тј. постоји $m \geq 0$ тако да је $I_n = I_m$ за све $n \geq m$. Осим тога, сви идеали I_k су коначно генерисани и нека је, за $0 \leq k \leq m$:

$$I_k = \langle a_{k1}, \dots, a_{ks_k} \rangle$$

и нека су $f_{kj_k} \in I$ полиноми степена k такви да је $LC(f_{kj_k}) = a_{kj_k}$. Докажимо да полиноми f_{kj_k} за $0 \leq k \leq m$, $1 \leq j_k \leq s_k$ генеришу идеал I . Означимо са \tilde{I} идеал у $A[X]$ генерисан овим полиномима. Очигледно је $\tilde{I} \subseteq I$. Докажимо другу инклузију.

Нека је $f \in I \setminus \{0\}$. Доказ изводимо индукцијом по степењу полинома f .

Претпоставимо да је $\deg f = 0$. То значи да је заправо f константан полином и да се налази у I_0 . Како су и полиноми f_{01}, \dots, f_{0s_0} константни полиноми који генеришу овај идеал, видимо да $f \in \tilde{I}$.

Претпоставимо да је полином f степена t и да је тврђење доказано за све полиноме степена мањег од t , Имамо две могућности.

t ≤ m. Дакле, f је полином степена t , те $LC(f) \in I_t$. Како a_{t1}, \dots, a_{ts_t} генеришу идеал I_t , то постоје $b_{t1}, \dots, b_{ts_t} \in A$ такви да је

$$LC(f) = b_{t1}a_{t1} + \dots + b_{ts_t}a_{ts_t}.$$

Подсетимо се да је $a_{tj_t} = LC(f_{tj_t})$ и да је $\deg f_{tj_t} = t$. То значи да је

$$\deg(f - b_{t1}f_{t1} - \dots - b_{ts_t}f_{ts_t}) < t,$$

а овај полином свакако припада идеалу \tilde{I} . По индуктивној хипотези закључујемо да он припада \tilde{I} , па је и $f \in \tilde{I}$.

$t > m$. Дакле, f је полином степена t , те $LC(f) \in I_t = I_m$. Како $a_{m_1}, \dots, a_{m_{s_m}}$ генеришу идеал I_m , то постоје $b_{m_1}, \dots, b_{m_{s_m}} \in A$ такви да је

$$LC(f) = b_{m_1}a_{m_1} + \dots + b_{m_{s_m}}a_{m_{s_m}}.$$

Подсетимо се да је $a_{m_{j_m}} = LC(f_{m_{j_m}})$ и да је $\deg f_{m_{j_t}} = m$. То значи да је

$$\deg(f - X^{t-m}b_{m_1}f_{m_1} - \dots - X^{t-m}b_{m_{s_m}}f_{m_{s_m}}) < t,$$

а овај полином свакако припада идеалу I . По индуктивној хипотези закључујемо да он припада \tilde{I} , па је и $f \in \tilde{I}$.

Ово и завршава доказ, јер смо показали да коначно много полинома генеришу идеал I . \square

Напомена 122 У називу ове теореме спомиње се нека база. Овде напомињемо да се не ради о бази у смислу векторских простора, него о томе да се генераторни скуп неког идеала у полиномијалном прстену назива и његовом БАЗОМ. \diamond

Последица 123 Сваки идеал у прстену $K[X_1, \dots, X_n]$ је коначно генерисан.

Доказ. Заправо је све већ урађено. Индукцијом по n се показује да је $K[X_1, \dots, X_n]$ Нетерин прстен, а то управо значи да је сваки идеал у њему коначно генерисан. \square