Предавања из Алгебре 2 за школску 2022/23 годину

Зоран Петровић

Комутативни прстени са јединицом

У овој лекцији почињемо са изучавањем алгебарских структура са две бинарне операције, које обично зовемо сабирање и множење. Пређимо на дефиницију основног објекта, који ћемо овде проучавати.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Наведимо неке примере комутативних прстена са јединицом:

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

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

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

Подсетимо се да је $\Phi(n)$ заправо скуп свих природних бројева између 1 и н 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 $x \cdot y \equiv 1 (\mathrm{mod}\ n)$, односно да је $x \cdot_n y = 1$. Дакле,

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

Приметимо да су операције у прстену $\mathbb{Z}_6$ сабирање и множење по модулу 6, те како је $2 \cdot_6 3 = 0$ и сл. добијамо наведени резултат. Феномен, који се овде појавио састоји се у томе да производ два ненулта елемента ипак може бити једнак 0.

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

Став 3 У пољу нема правих делитеља нуле.

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

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

што противречи претпоставци $b \neq 0$. □

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

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

Став 5 Сваки коначан домен је поље.

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

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

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

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

Упутство: Погледајте доказ става **5**. □

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

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

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

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

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

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

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

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

Важнији од појма потпрстена је појам ИДЕАЛА.

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

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

Приметимо да $0 \in I$ за сваки идеал I. Наиме, како је I непразан, то постоји $x \in I$. Но, тада је и $0 = 0 \cdot x \in I$. Ознака $I \triangleleft A$ 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. $I \cdot J := \{x_1 y_1 + \cdots + x_n y_n : x_i \in I \text{ за све } i = \overline{1,n}, y_j \in J \text{ за све } j = \overline{1,n}, \text{ и све } n \geq 1\}$.

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

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

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

Наведимо неке примере.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Пример 14 Нека је K поље и $I \lhd K$. 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 $f\colon A \to B$ је хомоморфизам прстена уколико је $f(1_A) = 1_B$ и уколико за све $x, y \in A$ важи:

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

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

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

Дефиниција 18 Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Језгро хомоморфизма f, у ознаци $\mathrm{Ker}(f)$ дефинише се са:

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

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

а) $\mathrm{Ker}(f) \lhd A$;

б) ако је $J \lhd B$ онда је $f^{-1}[J] \lhd A$;

в) ако је $I \lhd A$ и f „на", онда је $f[I] \lhd B$.

Доказ.

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

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

па $x + y \in \mathrm{Ker}(f)$.

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

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

те $a \cdot x \in \mathrm{Ker}(f)$.

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

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

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

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

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

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

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

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

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

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

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

Приметимо да једнакост $J = \rho_n[\rho_n^{-1}[J]]$ следи из чињенице да је ρ_n „на", док је јасно да је $f[\langle a \rangle] = \langle f(a) \rangle$ за сваки епиморфизам (хомоморфизам који је „на") f и сваки елемент a (покажите да је ово тачно!). ♣

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

Пример 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 $\mathbb{Z}_2$ (поновите појам директног производа алгебри). Скуп $\{(0,0),(1,1)\}$ је подгрупа адитивне групе тог прстена, али није идеал пошто елемент $(1,0)\cdot(1,1) = (1,0)$ не припада том скупу, а $(1,1)$ му припада. ♣

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

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

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

Дефиниција 23 Нека је $I \triangleleft A$. На A дефинишемо релацију конгруенције по модулу I са:

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

Проверимо да је ова релација заиста конгруенција.

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

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

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

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

те је $a \equiv c (\mathrm{mod}\ I)$.

Слагање са $+$. Нека је $a \equiv a' (\mathrm{mod}\ I)$ и $b \equiv b' (\mathrm{mod}\ I)$. 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 $a \equiv a' (\mathrm{mod}\ I)$ и $b \equiv b' (\mathrm{mod}\ I)$. 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 24 *(*Теорема о изоморфизмима за прстене*)* Нека је $f \colon A \to B$ хомоморфизам комутативних прстена са јединицом. Тада је $\tilde{f} \colon A/_{\mathrm{Ker}(f)} \to \mathrm{Im}(f)$ задато са:

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

изоморфизам комутативних прстена са јединицом.

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

Проверимо да је $\tilde{f}$ хомоморфизам.

$$\tilde{f}((a + \mathrm{Ker}(f)) + (b + \mathrm{Ker}(f))) = \tilde{f}((a + b) + \mathrm{Ker}(f)) = f(a + b) =$$

$$= f(a) + f(b) = \tilde{f}(a + \mathrm{Ker}(f)) + \tilde{f}(b + \mathrm{Ker}(f)).$$

$$\tilde{f}((a + \mathrm{Ker}(f)) \cdot (b + \mathrm{Ker}(f))) = \tilde{f}((a \cdot b) + \mathrm{Ker}(f)) = f(a \cdot b) =$$

$$= f(a) \cdot f(b) = \tilde{f}(a + \mathrm{Ker}(f)) \cdot \tilde{f}(b + \mathrm{Ker}(f)).$$

Јасно је да је $\tilde{f}$ „на". Остаје да се провери да је $\tilde{f}$ „1–1".

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

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

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

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

Пример 25 Нека је $I \triangleleft A$. Тада је $p\colon A\to A/_I$ један епиморфизам. ♣

Пример 26 За све $n\geq 1$ важи: $\mathbb{Z}/_{n\mathbb{Z}}\cong\mathbb{Z}_n$.

Хомоморфизам $\rho_n\colon\mathbb{Z}\to\mathbb{Z}_n$, дат раније, је „на", а осим тога $\mathrm{Ker}(\rho_n)=n\mathbb{Z}$, те резултат следи. ♣

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

Дефиниција 27 Нека су $(A_1,+^1,\cdot^1),\dots(A_n,+^n,\cdot^n)$ комутативни прстени са јединицом. На Декартовом производу

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

задајемо структуру комутативног прстена са јединицом са:

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

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

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

Став 28 Нека су $m_1,\dots,m_n$ позитивни цели бројеви за које је: $\mathrm{NZD}(m_i,m_j)=1$ за све $i\neq j$. Тада је

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

Доказ. Дефинишимо хомоморфизам

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

са:

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

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

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

Добијамо да је

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

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

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

Закључујемо да f мора бити „на". Тиме смо добили тражени изоморфизам. □

Последица 29 (Кинеска теорема о остацима) Нека су $m_1, \ldots, m_n$ позитивни цели бројеви који су пар по пар узајамно прости и $x_1, \ldots, x_n$ произвољни цели бројеви. Тада постоји цео број x такав да је

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

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

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

Доказ. Посматрајмо елемент

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

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

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

но, то управо значи да је

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

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

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

као што је и тврђено. □

Став 30 Ако су прстени A и B изоморфни, онда је $(U(A),\cdot) \cong (U(B),\cdot)$

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

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

Став 31 Важи једнакост: $U(A_1 \times \cdots \times A_n) = U(A_1) \times \cdots \times U(A_n)$.

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

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

□

Теорема 32 Ако су $m_1, \ldots, m_n$ пар по пар узајамно прости позитивни цели бројеви, онда је

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

и

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

где је φ Ојлерова функција.

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

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

Дефиниција 33 Идеали I и J комутативног прстена са јединицом A су КОПРОСТИ (или узајамно прости) уколико је $I + J = A$.

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

Став 34 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 $| \cap J$. 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 $I \cap J$. □

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

Лема 35 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 постој $x_1 \in I$ и $y \in J$ такви да је $x + y = 1$. 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.

$$x_1 x_2 + x_1 z + y x_2 + yz = 1.$$

Но, како $x_i \in I$, то $x_1 x_2$, $x_1 z$, $y z_2 \in I$, те и $x_1 x_2 + x_1 z + y x_2 \in I$, док из $y \in J$, $z \in K$, следи да $yz \in J \cdot K$. Дакле,

$$1 = \underbrace{x_1 x_2 + x_1 z + y x_2}_{\in I} + \underbrace{yz}_{\in K} \in I + J \cdot K.$$

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

Теорема 36 (Кинеска теорема о остацима) Нека су идеали $I_1, \ldots, I_n$ комутативног прстена са јединицом A пар по пар узајамно прости. Тада важи изоморфизам:

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

Доказ. Доказ је нешто тежи него у случају прстема целих бројева. Посматрамо хомоморфизам $f \colon A \to A/I_1 \times \cdots \times A/I_n$ дефинисан са:

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

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

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

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

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

Из леме **35** 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 $(x_1 + I_1, \ldots, x_n + I_n)$ произвољни елемент из $A/I_1 \times \cdots \times A/I_n$. Уочимо елемент $x = b_1 x_1 + \cdots + b_n x_n$, где су b_i претходно изабрани елементи. Тада је, за све i:

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

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

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

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 $I_1, \ldots, I_n$: $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$. Дакле, у том случају имамо да је $A/I_1 \cdots I_n \cong A/I_1 \times \cdots \times I_n$.

Прости и максимални идеали

Започнимо ову тему следећим ставом.

Став 37 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 $b = 0$.

$1 \Longrightarrow 2$. 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 $b \in P$.

$2 \Longrightarrow 3$. 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 $y = 0$.

$3 \Longrightarrow 1$. 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. □

Дефиниција 38 Идеал $P \triangleleft A$ је прост уколико испуњава неко од претходна три еквивалентна својства.

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

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 39 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 40 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. □

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

Пример 41 У прстену $\mathbb{Z}\left[\sqrt{-5}\right]$ елемент 3 је нерастављив, али није прост.

Пре свега,

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

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

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

Уверимо се најпре да је 3 нерастављив. Претпоставимо да је $3 = uv$. Уведимо ознаку $N(z) := z\overline{z}$, за $z \in \mathbb{Z}\left[\sqrt{-5}\right]$ (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 $1 = N(u) = u\overline{u} = (a+b\sqrt{-5})(a-b\sqrt{-5}) = a^2+5b^2$. 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 $U\left(\mathbb{Z}\left[\sqrt{-5}\right]\right) = \{-1, 1\}$ 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 слуцај 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 $\mathbb{Z}\left[\sqrt{-5}\right]$:

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

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 $u \in \mathbb{Z}\left[\sqrt{-5}\right]$:

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

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 42 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. $\diamondsuit$

Следећи став је помало и очекиван.

Став 43 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 $p \mid b$. $\square$

Пређимо сада на појам максималног идеала.

Дефиниција 44 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 45 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 $m \in M$ за које је $ab + m = 1$. Дакле, $ab - 1 = m \in M$, 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. $1 \in ab - m$. 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 46 Видимо да из овог става следи да је сваки максималан идеал уједно и прост идеал, пошто у пољу нема правих делитеља нуле. $\diamondsuit$

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

Став 47 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. □

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

Теорема 48 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 49 У комутативном прстену са јединицом A постоји тачно један максималан идеал ако и само ако је $A \setminus U(A)$ идеал.

Доказ. Претпоставимо да је прстену постоји тачно један максималан идеал M. Доказаћемо да је заправо $M = A \setminus U(A)$. Пре свега, ниједан елемент у M не може бити инвертибилан пошто је M прави идеал (идеал генерисан инвертибилним елементом једнак је целом прстену). Дакле, $M \subseteq A \setminus U(A)$. Обратно, нека је $a \in A \setminus U(A)$. Како a није инвертибилан, то је идеал $\langle a \rangle$ прави идеал, па је по претходној теореми садржан у неком максималном идеалу. Но, како је M једини максималан идеал, то $a \in M$. Добили смо да је $A \setminus U(A) = M$, па је $A \setminus U(A)$ заиста идеал.

Обратно, нека у прстену A сви неинвертибилни елементи чине идеал M. Јасно је да тај идеал мора бити максималан. Наиме, ако је M прави подскуп идеала I у I постоји неки елемент који није у M. Тај елемент је нужно инвертибилан (пошто су у M сви неинвертибилни), те генерише цео прстен и следи да је и $I = A$. Дакле, M је максималан идеал. Претпоставимо да је M' неки други максималан идеал и нека је $M \neq M'$. Како је M' максималан то $M' \not\subseteq M$, па постоји елемент $x \in M' \setminus M$. Но, то значи да је x инвертибилан, па је $M' = A$ и M' није прави идеал, а то противречи претпоставци да је он максималан. Закључујемо да је M једини максималан идеал у A. □

Дефиниција 50 Комутативан прстен са јединицом у коме постоји тачно један максимални идеал назива се ЛОКАЛНИ ПРСТЕН.

Пример 51 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 $\frac{a}{b} \in U(\mathbb{Z}_{(p)})$ **акко** $p \nmid a$. Дакле, $\frac{a}{b} \notin U(\mathbb{Z}_{(p)})$ **акко** $p \mid a$. Но, то управо значи да је скуп свих неинвертибилних елемената у овом прстену скуп свих умножака броја p, тј. идеал генерисан са p. ♣

Пример 52 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 $\left[\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right] \in A$ 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 $\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$. ♣

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 53 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 54 Домен A је домен за јединственом факторизацијом уколико за сваки елемент из $a \in A \setminus (U(A) \cup \{0\})$ постоје нерастављиви елементи $p_1, \ldots, p_r$ такви да је $a = p_1 p_2 \cdots p_r$. Осим тога ако је за нерастављиве елемента 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 јединственом факторизацијом, сваки елемент може се на јединствен начин, до на придруженост и редослед фактора, приказати у облику производа нерастављивих елемената.

Став 55 Домен A је домен са јединственом 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 су p_i, q_j нерастављиви. Према доказаном, p_1 је прост, па постоји $j_1 \in \{1, \ldots, s\}$ 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 поделити са p_1 и добијамо

$$p_2 \cdots p_r = q_2' q_3 \cdots q_s,$$

где је $q_2' = q_2 u_1$ и он је такође нерастављив. Индуктивна хипотеза завршава доказ.

Обратно, претпоставимо да је A домен за јединственом 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 $z_1, \ldots, z_l$. 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 $\{p_1, \ldots, p_r, q_1, \ldots, q_s\}$. 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. □

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

Став 56 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 $a = d_1 a_1$ и $b = d_1 b_1$. С обзиром да $d \in \langle a, b\rangle$, постоје p, q такви да је $d = ap + bq$. Добијамо да је $d = d_1 a_1 p + d_1 b_1 q = d_1(a_1 p + b_1 q)$, те следи да $d_1 \mid d$. □

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 $\mathrm{NZD}(a, b)$ придружен јединици, онда $a \mid c$ (наравно, уместо да пишемо да је $\mathrm{NZD}(a, b)$ придружен јединици, писаћемо да је $\mathrm{NZD}(a, b) = 1$, имајући на уму шта то значи). Нека читаоци ово сами докажу.

Теорема 57 Сваки главноидеалски домен је и домен са јединственом 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 $\mathrm{NZD}(q,a) = 1$. Наиме, ако је $d = \mathrm{NZD}(q,a)$, 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. $\mathrm{NZD}(q,a) = 1$ (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 јединственом 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 **55**).

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

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

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. □

Дакле, домен са јединственом 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

$$a = up_1^{\alpha_1} \cdots p_k^{\alpha_k}, \tag{1}$$

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 58 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 јединственом 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 $-36 = (-1)2^2 3^2$, 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. $\diamondsuit$

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. Почнимо следећом дефиницијом.

Дефиниција 59 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 60 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!). ♣

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

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

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 61 Нека је A домен и S неки мултипликативан подскуп од A.

а) Са $i(a) = \frac{a}{1}$ задат је један мономорфизам $i \colon A \to S^{-1}A$,

б) Ако је B ма који комутативан прстен и $f \colon A \to B$ хомоморфизам такав да за све $s \in S$ важи: $f(s) \in U(B)$, онда постоји тачно један хомоморфизам $\widetilde{f} \colon S^{-1}A \to B$ за који је $\widetilde{f} \circ i = f$.

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, $a \in \mathrm{Ker}(i)$ ако и само ако је $\frac{a}{1} = \frac{0}{1}$, што је еквивалентно са $a = 0$, па је i мономорфизам.

б) Тражени хоморфизам $\widetilde{f}$ дефинишемо са: $\widetilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$. 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: $\widetilde{f} \circ i = f$. □

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

Теорема 62 За сваки прост идеал $P \lhd A$, прстен A_P је локални прстен.

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

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

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. □

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.

Прстен полинома

Конструкција прстена полинома

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 $a_0 + a_1X + \cdots + a_nX^n$, где је $n \geq 0$ природан број, а a_i елементи прстена A, а да су операције онакве какве знамо из средње школе. Уз додатак да је $a_0 + a_1X + \cdots + a_nX^n = b_0 + b_1X + \cdots + b_mX^m$ ако и само ако је $n = m$ и $a_i = b_i$ за све i.

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

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

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

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

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

Наведимо најпре дефиницију прстена полинома.

Дефиниција 63 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 $a_0 + a_1X + \cdots + a_nX^n$ за $n \geq 0$ и $a_i \in A'$.

Оно што се одмах можемо запитати после ове дефиниције је да ли може постојати више прстена полинома над прстеном A и неодређеном X. Наравно, одговор је потврдан, али сви они су међусобно изоморфни. Наиме, нека су B_1 и B_2 такви прстени који, редом, садрже потпрстене A_1' и A_2' изоморфне прстену A и елементе $X_i \in B_i$ који се наводе у дефиницији. Пошто су A_1' и A_2' изоморфни прстену A, они су и међусобно изоморфни, дакле постоји изоморфизам $f\colon A_1' \to A_2'$. Стога можемо задати $F\colon B_1 \to B_2$ са

$$F(a_0 + a_1X_1 + \cdots + a_nX_1^n) \colon = f(a_0) + f(a_1)X_2 + \cdots + f(a_n)X_2^n$$

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

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

Приметимо да се у сваком неформално задатом полиному $a_0 + a_1X + \cdots + a_nX^n$ појављује коначан низ $(a_0, a_1, \ldots, a_n)$ 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 $(a_0, a_1, \ldots)$ елемената из A. Но, нас не занимају сви такви низови, но само низови који су једнаки 0 почев од неког члана. Стога посматрамо скуп

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

Потребно је задати и операције на скупу A^{ω}. Сабирање се лако задаје:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) \colon = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$

док је множење нешто сложеније:

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

где је за све $k \geq 0$:

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

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 $\overline{a}$ за $a \in A$, означавамо низ коме је нулти члан једнак a, а сви остали једнаки $0 (= 0_A)$:

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

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 $\overline{a}$ низ $(a, 0, 0, \dots)$. Тада је

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

Дакле, $\overline{a} \cdot X^n = (0, \dots, 0, a, 0, \dots)$, 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

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

Наравно, уместо $\overline{a_i} \cdot X^i$ писали смо краће $\overline{a_i} X^i$. Уколико је

$$\overline{a_0} + \overline{a_1} X + \cdots + \overline{a_n} X^n = \overline{b_0} + \overline{b_1} X + \cdots + \overline{b_m} X^m,$$

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:

$$\overline{a} + \overline{b} = \overline{a + b} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}.$$

Из ових једнакости можемо закључити да је са $f(a) \colon = \overline{a}$ задат један хомоморфизам прстена $f \colon A \to A^\omega$, који је '1–1' и стога успоставља изоморфизам између A и његове слике $A' = \{\overline{a} : a \in A^\omega\}$. 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: $K[X, Y] \colon = K[X][Y]$. Јасно је да рекурзијом можемо задати прстен $K[X_1, \dots, X_n]$ за ма које $n \geq 1$.

Еуклидско дељење

Уколико је $0 \neq a(X) = a_0 + a_1X + \cdots + a_nX^n \in K[X]$ 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 64 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 $a(X) = a_nX^n + \cdots + a_1X + a_0$, а $b(X) = b_mX^m + \cdots + b_1X + b_0$, 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 моном 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

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

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. □

Следећа последица је добро позната.

Последица 65 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 $a(X)$ акко 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. □

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 66 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 67 Наравно да овде имамо сабирање у прстену $\mathbb{Z}_{10}$ и да је, на пример $35 = \underbrace{1 + \cdots + 1}_{35}$. ♢

Еуклидов алгоритам у прстену $K[X]$

Дефиниција 68 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 $\mathrm{NZD}(a(X), b(X))$ за моничан полином који је највећи заједнички делилац полинома $a(X)$ и $b(X)$.

Следећа лема је једноставна и корисна.

Лема 69 Ако је $a_1(X) = q(X)a_2(X) + a_3(X)$, онда је $\mathrm{NZD}(a_1(X), a_2(X)) = \mathrm{NZD}(a_2(X), a_3(X))$.

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. $b(X) \mid a_1(X)$. □

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

$$
\begin{aligned}
&(0)\ \ a(X) = q(X)b(X) + r(X), && -\infty < \deg(r(X)) < \deg(b(X))\\
&(1)\ \ b(X) = q_1(X)r(X) + r_1(X), && -\infty < \deg(r_1(X)) < \deg(r(X))\\
&(2)\ \ r(X) = q_2(X)r_1(X) + r_2(X), && -\infty < \deg(r_2(X)) < \deg(r_(X))\\
&\qquad\qquad\vdots\\
&(n-1)\ \ r_{n-3}(X) = q_{n-1}(X)r_{n-2}(X)+r_{n-1}(X), && -\infty < \deg(r_{n-1}(X)) < \deg(r_{n-2}(X))\\
&(n)\ \ r_{n-2}(X) = q_n(X)r_{n-1}(X)+r_n(X), && -\infty < \deg(r_n(X)) < \deg(r_{n-1}(X))\\
&(n+1)\ \ r_{n-1}(X) = q_{n+1}(X)r_n(X).
\end{aligned}
$$

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

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

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

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

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

$$\mathrm{NZD}(a(X), b(X)) = u(X)a(X) + v(X)b(X). \tag{2}$$

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

Теорема 70 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 $I = \langle \mu(X) \rangle$. □

Пример 71 У прстену $\mathbb{Z}[X]$ постоји идеал који није главни.

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

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

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

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

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

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

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

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 $X \in a(X, Y)$, 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 $K[X_1,\ldots,X_n]$, где је K поље, коначно генерисан, тј. за сваки идеал $I \lhd K[X_1,\ldots,X_n]$, постоје $f_1,\ldots,f_k \in I$ тако да је $I = \langle f_1,\ldots,f_k\rangle$. Ово ћемо доказати нешто касније, сада ћемо се позабавити питањем како се одређује генератор за $\langle f_1(X),\ldots,f_k(X)\rangle \neq \{0\}$ 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 72 Нека је K поље и $f_1(X),\ldots,f_k(X) \in K[X]\setminus\{0\}$. Тада је

$$\langle f_1(X),\ldots,f_k(X)\rangle = \langle \mathrm{NZD}(f_1(X),\ldots,f_k(X)\rangle.$$

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

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

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

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

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

Једнозначна факторизација у прстену полинома

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

Теорема 73 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 74 Ако је p прост елемент у A, онда је $\langle p \rangle \lhd A[X]$ 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 $\varphi\colon A[X] \to (A/_{pA})[X]$ са:

$$\varphi(a_0 + a_1X + \cdots + a_nX^n) := \overline{a_0} + \overline{a_1}X + \cdots + \overline{a_n}X^n,$$

где са $\overline{a}$ означен елемент $a + pA$ прстена $A/_{pA}$. С обзиром да је пресликавање $a \mapsto \overline{a}$ епиморфизам (хомоморфизам који је „на" прстена A на прстен A/pA), лако се проверава да је φ такође један епиморфизам. Но, $a_0 + a_1X + \cdots + a_nX^n \in \mathrm{Ker}(\varphi)$ **акко** је $a_i = 0_{A/pA}$ за све i, тј. **акко** $p \mid a_i$ 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 $\mathrm{Ker}(\varphi) = pA[X]$, 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. □

Дефиниција 75 За полином $a(X) = a_0 + a_1X + \cdots + a_nX^n \in A[X]$ кажемо да је ПРИМИТИВАН уколико је $\mathrm{NZD}(a_0, a_1, \ldots, a_n) = 1$.

Лема 76 (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

$$\varphi(f \cdot g) = 0 \in (A/_{pA})[X], \tag{3}$$

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. □

Лема 77 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 $d = b_0 b_1 \cdots b_n$, онда је јасно да $df \in A[X]$. Како $d\frac{a_i}{b_i} \in A$, може се дефинисати

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

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 $f = c_1 f_1 = c_2 f_2$, 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 $q_1 q_2$ добијамо

$$q_2 p_1 f_1 = q_1 p_2 f_2.$$

Како су f_1 и f_2 примитивни полиноми, то је $q_2 p_1$ највећи заједнички делилац коефицијената полинома $q_2 p_1 f_1$, а $q_1 p_2$ највећи заједнички делилац коефицијената полинома $q_1 p_2 f_2$. С обзиром да су ово једнаки полиноми, закључујемо да су $q_2 p_1$ и $q_1 p_2$ придружени елементи прстена A, тј. постоји $u \in U(A)$ тако да је $q_2 p_1 = u q_1 p_2$, те је $\frac{p_1}{q_1} = u\frac{p_2}{q_2}$, тј. $c_1 = u c_2$, 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 $f \cdot g = c(f)c(g)f_0 g_0$, где је $f_0 g_0$ примитиван по Гаусовој леми. Дакле,

$$c(f)c(g)f_0 g_0 = c(h)h_0.$$

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

Лема 78 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 $f = a_0 + a_1 X + \cdots + a_n X^n =$

$p(b_0 + b_1X + \cdots + b_nX^n)$ 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 **74** 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 јединственом 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 **77** 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 $A[X]$. □

Сада најзад можемо доказати теорему **73**.

Доказ теореме 73. 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 јединственом факторизацијом, могуће је наћи $d_1, \ldots, d_r$ 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 $A[X]$. □

Као последицу ове теореме имамо чињеницу да су прстени $\mathbb{Z}[X]$, $\mathbb{Z}[X, Y]$, $\mathbb{Z}[X, Y, Z]$ прстени са јединственом 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 79 Нека је A прстен са јединственом факторизацијом, K његово поље разломака и $f, g \in A[X]$. Тада је $\mathrm{NZD}(f,g) = \mathrm{NZD}(c(f), c(g)) \cdot d$, 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 јединственом 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 $\mathrm{NZD}(c(f), c(g)) \cdot d \mid f$ у $K[X]$ то је $f = \mathrm{NZD}(c(f), c(g)) \cdot d \cdot q$ за неки полином $q \in K[X]$. Добијамо да је $c(f) = \mathrm{NZD}(c(f), c(g)) c(q) u$, за неки $u \in U(A)$, пошто је $c(d) = 1$, јер је d примитивни полином. Но, $\mathrm{NZD}(c(f), c(g)) \mid c(f)$, 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 $c(D) \mid \mathrm{NZD}(c(f), c(g))$ 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 $D \mid \mathrm{NZD}(c(f), c(g))d$ у $K[X]$ и $\mathrm{NZD}(c(f), c(g))d = DQ$ у $K[X]$. Тада је $\mathrm{NZD}(c(f), c(g))c(d) = c(D)c(Q) \cdot w$, за неки $w \in U(A)$. Како $c(D) \mid \mathrm{NZD}(c(f), c(g))$ у A, то је $\mathrm{NZD}(c(f), c(g)) = c(D)a$, за неки $a \imath A$ 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 јединственом 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

$$\frac{a(X)}{b(X)} = \frac{a_1(X)}{b_1(X)} \textbf{ акко је } a(X)b_1(X) = a_1(X)b(X).$$

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.

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

Став 80 (Ајзенштајнов критеријум) Ако је $f = a_0+a_1X+\cdots+a_nX^n \in [X]$ такав да постоји прост број p за који важи:

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

онда је f нерастављив у $\mathbb{Q}[X]$

Доказ. Претпоставимо да је $f = g \cdot h$ у $\mathbb{Q}[X]$, при чему је $\deg g, \deg h < \deg f$. Тада је $c(f) = c(g)c(h)u$, за неки $u \in U(\mathbb{Z}) = \{\pm 1\}$. Како је $f \in \mathbb{Z}[X]$, то је $c(g)c(h) \in \mathbb{Z}$ и добијамо да је $f = c(g)g_0c(h)h_0 = g_1h_0$, при чему је $g_1 = c(g)c(h)g_0 \in \mathbb{Z}[X]$. Дакле, имамо факторизацију $f = g_1h_1$ и у $\mathbb{Z}[X]$.

Искористимо сада хомоморфизам φ из доказа леме **74**. Ако са $\overline{a}$ означимо слику елемента a у $\mathbb{Z}/p\mathbb{Z}[X]$, онда имамо да је $\overline{f} = \overline{a_n}X^n$, а како је $f = g_1h_1$, онда је $\overline{a_n}X^n = \overline{g_1}\overline{h_1}$, из чега следи да је $\overline{g_1} = \overline{c}X^k$, а $\overline{h_1} = \overline{d}X^{n-k}$. Но, то значи да је сваки коефицијент полинома g_1 и f_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 $\mathbb{Q}[X]$. □

Пример 81 Нека је p прост број. Доказати да је полином $a(X) = X^{p-1} + X^{p-2} + \cdots X + 1 \in \mathbb{Z}[X]$ 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

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

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 82 Нека је $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in A[X]$, где је A прстен са једнозначном факторизацијом. Уколико су $b, c \in A$ такви да је $c \neq 0$, $\mathrm{NZD}(b,c) = 1$ 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

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

Множењем са c^n добијамо

$$a_n b^n + a_{n-1} b^{n-1} c + \cdots + a_1 b c^{n-1} + a_0 c^n = 0.$$

Одавде добијамо да $b \mid a_0 c^n$, а $c \mid a_n b^n$. Из чињенице да је $\mathrm{NZD}(b,c) = 1$ следи да је и $\mathrm{NZD}(b, c^n) = 1$, 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 $b/c \in A$. □

Количнички прстени прстена полинома

Започнимо ову лекцију једним примером.

Пример 83 Проверити да је са:

$$f(p(X)) = p(i),$$

где је i имагинарна јединица, дефинисан један хомоморфизам $f\colon \mathbb{R}[X] \to \mathbb{C}$ и применити на тај хомоморфизам теорему о изоморфизмима прстена.

Није тешко проверити да је f заиста хомоморфизам прстена. Нека су $a(X), b(X) \in \mathbb{R}[X]$ и нека је $c(X) = a(X) \cdot b(X)$. Тада је

$$f(a(X)) = a(i) = a_0 + a_1 i + a_2 i^2 + \cdots + a_m i^m,$$

$$f(b(X)) = b(i) = b_0 + b_1 i + b_2 i^2 + \cdots + b_n i^n$$

и

$$f(c(X)) = c(i) = c_0 + c_1 i + c_2 i^2 + \cdots + c_{m+n} i^{m+n},$$

при чему смо претпоставили да је степен полинома $a(X)$ једнак m, а степен полинома $b(X)$ једнак n. Но, знамо како се множе полиноми, па је за $k = \overline{0, m+n}$:

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0,$$

при чему је наравно $a_i = 0$ за $i > m$, односно $b_j = 0$, за $j > n$. Но, тада је јасно да је заиста

$$c(i) = a(i) \cdot b(i),$$

те је

$$f(a(X) \cdot b(X)) = f(a(X)) \cdot f(b(X)).$$

Још лакше се проверава да је $f(a(X)+b(X)) = f(a(X))+f(b(X))$, а јасно је и да је $f(1) = 1$ (константан полином има константну вредност).

Теорема о изоморфизмима за прстене даје следећи изоморфизам:

$$\mathbb{R}[X]/_{\mathrm{Ker}(f)} \cong \mathrm{Im}(f).$$

Идентификујмо слику и језгро хомоморфизма f.

Уколико је $a+bi$ произвољни елемент из $\mathbb{C}$, јасно је да је $f(a+bX) = a + bi$, па је f „на". Претпоставимо да $a(X) \in \mathrm{Ker}(f)$. То значи да је $a(i) = 0$. Дакле, $a(X)$ је полином са реалним коефицијентима чија је једна нула комплексан број i. Из средње школе нам је познато да је тада и $-i$ обавезно нула тог полинома. Но, α је нула полинома $a(X)$ ако и само ако $X - \alpha$ дели $a(X)$ (ово смо већ имали прилике да користимо). Добијамо да и $X - i$ дели $a(X)$, али да и $X + i = X - (-i))$ такође дели $a(X)$. Полиноми $X - i$ и $X + i$ су узајамно прости, па закључујемо да полином $X^2+1 = (X-i)(X+i)$ дели $a(X)$. Према томе, ако $a(X) \in \mathrm{Ker}(f)$, онда $(X^2 + 1) \mid a(X)$. То се може записати и овако:

$$a(X) \in \mathrm{Ker}(f) \Longrightarrow a(X) \in \langle X^2 + 1 \rangle,$$

где наравно $\langle X^2+1 \rangle$ означава главни идеал генерисан полиномом X^2+1. Јасно је да важи и обратно. Наиме, ако $a(X) \in \langle X^2 + 1 \rangle$, то значи да је $a(X) = q(X)(X^2 + 1)$ за неки полином $q(X)$, но тада је

$$f(a(X)) = f(q(X)(X^2 + 1)) = f(q(X))f(X^2 + 1) = q(i)(i^2 + 1) = 0,$$

па $a(X) \in \mathrm{Ker}(f)$. Закључујемо да је $\mathrm{Ker}(f) = \langle X^2+1 \rangle$, те важи изоморфизам $\mathbb{R}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C}$. ♣

Урадимо још један пример.

Пример 84 Доказати да је $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ једно потпоље поља $\mathbb{C}$. Применити теорему о изоморфизмима за прстене на хомоморфизам $f\colon \mathbb{Q}[X] \to Q(\sqrt{2})$ дефинисан са $f(a(X)) = a(\sqrt{2})$.

Јасно је да је разлика два елемента из $Q(\sqrt{2})$ такође у $Q(\sqrt{2})$. Проверимо то за производ.

$$(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(ad+bc)\sqrt{2},$$

а како су $ac+2bd$ и $ad+bc$ рационални бројеви ако су то a,b,c,d, закључујемо да $(a+b\sqrt{2})(c+d\sqrt{2}) \in \mathbb{Q}(\sqrt{2})$. Да бисмо показали да је $\mathbb{Q}(\sqrt{2})$ потпоље поља комплексних бројева, треба још само да проверимо да је инверз сваког не-нула елемента из $\mathbb{Q}(\sqrt{2})$ такође у $\mathbb{Q}(\sqrt{2})$. Приметимо да је $a+b\sqrt{2}=0$ ако и само ако је $a=b=0$. Наиме, уколико претпоставимо да је $b\neq 0$, а $a+b\sqrt{2}=0$, добијамо да је $\sqrt{2}=-\frac{a}{b}$, па би $\sqrt{2}$ био рационалан број, а знамо још из средње школе да то није случај. Дакле, уколико је $a+b\sqrt{2}\neq 0$, то је (наравно да је и $a-b\sqrt{2}\neq 0$ за $a,b\in\mathbb{Q}$):

$$\frac{1}{a+b\sqrt{2}} = \frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2} = \frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}\in\mathbb{Q}(\sqrt{2}).$$

На исти начин као и у претходном примеру, проверава се да је f хоморфизам. Осим тога, како је $f(a+bX)=a+b\sqrt{2}$, видимо да је f „на". Покажимо да је $\mathrm{Ker}(f)=\langle X^2-2\rangle$.

Уколико $a(X)\in\langle X^2-2\rangle$, то је $a(X)=q(X)(X^2-2)$ за неки полином $q(X)\in\mathbb{Q}[X]$, па је

$$f(a(X)) = f(q(X)(X^2-2)) = f(q(X))f(X^2-2) = q(\sqrt{2})((\sqrt{2})^2-2)=0.$$

Дакле, $\langle X^2-2\rangle\subseteq\mathrm{Ker}(f)$. Покажимо да важи обратна импликација. Нека $a(X)\in\mathrm{Ker}(f)$. То значи да је $a(\sqrt{2})=0$, па $(X-\sqrt{2})\mid a(X)$. Да бисмо показали да $(X^2-2)\mid a(X)$, потребно нам је, а и довољно, да покажемо да и $(X+\sqrt{2})\mid a(X)$, тј. да је $a(-\sqrt{2})=0$. Нека је

$$a(X)=a_0+a_1X+a_2X^2+\cdots+a_nX^n.$$

Како је $a(\sqrt{2})=0$, то је

$$a_0+a_1\sqrt{2}+a_2\cdot 2+a_3\cdot 2\sqrt{2}+\cdots+a_n(\sqrt{2})^n=0.$$

Природно је дакле раздвојити парне степене од X и непарне степене од X. Претпоставимо, због једноставности ознака, да је $n=2k$ (ако је n непаран број, то додајемо још један коефицијент који је једнак нули — то не мења ништа у полиному, само у запису). Дакле,

$$a(X)=\sum_{i=0}^{k}a_{2i}X^{2i}+\sum_{i=0}^{k-1}a_{2i+1}X^{2i+1}.$$

Добијамо да је

$$0=a(\sqrt{2})=\sum_{i=0}^{k}a_{2i}2^i+\left(\sum_{i=0}^{k-1}a_{2i+1}2^i\right)\sqrt{2}.$$

Како су $a_s \in \mathbb{Q}$, то мора бити

$$\sum_{i=0}^{k} a_{2i} 2^i = 0 \quad \text{и} \quad \sum_{i=0}^{k-1} a_{2i+1} 2^i = 0.$$

Но, одавде добијамо да је и

$$\sum_{i=0}^{k} a_{2i} 2^i - \left(\sum_{i=0}^{k-1} a_{2i+1} 2^i \right) \sqrt{2} = 0,$$

а то управо значи да је $a(-\sqrt{2}) = 0$ ($(-\sqrt{2})^{2i} = 2^i$, а $(-\sqrt{2})^{2i+1} = -2^i\sqrt{2}$). Овим је завршен доказ да је $\mathrm{Ker}(f) = \langle X^2 - 2 \rangle$, те добијамо изоморфизам $\mathbb{Q}[X]/\langle X^2 - 2 \rangle \cong \mathbb{Q}(\sqrt{2})$. ♣

Напомена 85 Могли смо и краће доказати да је $\mathrm{Ker}(f) \subseteq \langle X^2 - 2 \rangle$. Наиме, ако је $a(X) \in \mathrm{Ker}(f)$, поделимо $a(X)$ са $X^2 - 2$. Добијамо да је $a(X) = q(X)(X^2 - 2) + r + sX$, за неки полином $q(X) \in \mathbb{Q}[X]$ и рационалне бројеве r, s. Како је $a(\sqrt{2}) = 0$, добијамо да је $r + s\sqrt{2} = 0$, а како су $r, s \in \mathbb{Q}$, то је $r = s = 0$, тј. $a(X) \in \langle X^2 - 2 \rangle$. Но, није лоше видети и онај дужи доказ, па је зато и презентиран. ♢

Раширења поља

Изанализирајмо мало шта смо добили у претходним примерима. Посматрајмо, да се тако изразимо, „леву" страну у добијеним изоморфизмима. Видимо да се у оба случаја ради о количничким прстену прстена полинома по идеалу који је генерисан једним нерастављивим (над пољем $\mathbb{Q}$) полиномом другог степена. Оставимо за сада по страни чињеницу да је полином другог степена и концентришимо се на то да је он нерастављив. Количнички прстен је у оба случаја заправо поље. То, наравно не може бити случајно. Доказаћемо следећу важну теорему. Пре даљег читања, препорука је да читаоци понове градиво из Линеарне алгебре – појам векторског простора, линеарне независности вектора, базе и димензије векторског простора.

Теорема 86 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 $f\colon F \to E$ 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 $\mathrm{Ker}(f) = \{0\}$ (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 $\widetilde{X}$. Уколико је $a(X) = a_0 + a_1X + \cdots + a_nX^n$, добијамо да је

$$a(\widetilde{X}) = a_0+a_1\widetilde{X}+a_2\widetilde{X}^2+\cdots+a_n\widetilde{X}^n = a_0+a_1(X+I)+a_2(X+I)^2+\cdots+a_n(X+I)^n,$$

$$= (a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) + I = a(X) + I = I,$$

те добијамо да $\widetilde{X}$ 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

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

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

$\{1 + I, X + I, \ldots, X^{n-1} + I\}$ 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 $1 + I, \ldots, X^{n-1} + I$ 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 $1 + I, \ldots, X^{n-1} + I$ заиста линеарно независни. □

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 87 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 F_4 је дато са

$$F_4 = \mathbb{Z}_2[X]/\langle X^2 + X + 1 \rangle.$$

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

$$F_4 = \{0, 1, \eta, 1 + \eta\}.$$

Како у пољу F_4 важи: $\eta^2 = 1 + \eta$ (зашто?), можемо написати и таблице сабирања и множења у том пољу.

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

$\cdot$	0	1	η	$1+\eta$
0	0	0	0	0
1	0	1	η	$1+\eta$
η	0	η	$1+\eta$	1
$1+\eta$	0	$1+\eta$	1	η

♣

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 88 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. □

У даљем ћемо разматрати такозвана бројевна поља, тј. нека потпоља од $\mathbb{C}$. Приметимо да свако такво поље обавезно садржи као своје потпоље поље $\mathbb{Q}$. Најмање раширење поља F у коме се дати полином из $F[X]$ факторише на линеарне факторе назива се коренско поље тог полинома.

У претходном је коришћена ознака $\mathbb{Q}[\sqrt{2}]$. Овде је $\mathbb{Q}$ наравно поље, док је $\sqrt{2}$ елемент који није у том пољу. Његовим „додавањем" добијамо структуру, која је поље. Позабавимо се мало општијим разматрањем.

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 $a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n$ 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 $\mathbb{C}$ и $\alpha \in \mathbb{C} \backslash F$, 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 $a(X) = a_0 + a_1 X + \cdots + a_n X^n$, то добијамо да је

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

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

Дефиниција 89 Нека је F потпоље од $\mathbb{C}$ и $\alpha \in \mathbb{C}$. 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 90 Нека је F потпоље од $\mathbb{C}$ и $\alpha \in \mathbb{C}$. 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 $I \lhd F[X]$ 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, као и у ранијим примерима, посматрамо хомоморфизам

$$f \colon F[X] \to F[\alpha]$$

дефинисан са $f(p(X)) = p(\alpha)$. Хомоморфизам f је очигледно „на", а $\mathrm{Ker}(f) = I$. 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. □

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 $1, \alpha, \ldots, \alpha^{n-1}$ уколико је $n = \deg \mu_\alpha(X)$.

Пример 91 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 растаља 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

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

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)

$$\begin{aligned} a + c &= 0 && (4)\\ b + ac + d &= -10 && (5)\\ ad + bc &= 0 && (6)\\ bd &= 1 && (7) \end{aligned}$$

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

$$\begin{aligned} b + d &= -10 && (8)\\ bd &= 1 && (9) \end{aligned}$$

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:

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

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

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

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

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

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

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

Препуштамо читаоцима да реше овај систем једначина. ♣

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

Дефиниција 92 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 93 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 од $n+1$ вектора $\{1, \alpha, \ldots, \alpha^n\}$ сигурно линеарно зависан скуп вектора, тј. постоје $a_0, \ldots, a_n \in E$ такви да је

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

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

Теорема о примитивном елементу и примери

Дефиниција 94 Нека је A комутативни прстен са јединицом. Прстен A има карактеристику $n > 0$ уколико је n најмањи позитиван број за који је

$$n1_A = \underbrace{1_A + \cdots + 1_A}_{n} = 0_A.$$

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 95 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. □

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 96 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 $f(\frac{m}{n}) := (m1_K)(n1_K)^{-1}$ добро задата функција $f\colon \mathbb{Q} \to K$ 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 $g\colon \mathbb{Z} \to K$ са $g(m) = m1_K$ (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 $\mathbb{Z}_p$. □

Већ смо се упознали са проширењима облика $F(\alpha)$. Но, ако $\beta \notin F(\alpha)$, може се формирати и проширење $F(\alpha)(\beta)$, које се краће означава са $F(\alpha, \beta)$. Општије, имамо и проширења $F(\alpha_1, \ldots, \alpha_n)$. Но, веома је занимљив следећи резултат који нам каже да у случају алгебарских проширења поља $\mathbb{Q}$ ситуација није толико компликована колико изгледа.

Теорема 97 (Теорема о примитивном елементу) Свако коначно раширење E поља F које је карактеристике 0 је облика $\mathbb{F}(\alpha)$, за неко $\alpha \in E$.

Елемент α је тај примитивни елемент раширења E. Ову теорему нећемо доказивати.

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

Још два примера за крај овог дела.

Пример 98 Наћи примитивни елемент коренског поља полинома $X^4 - X^2 - 2 \in \mathbb{Q}[X]$.

Другим речима, треба наћи коренско поље K датог полинома и елемент $\alpha \in K$ за који је $K = \mathbb{Q}(\alpha)$. Факторишимо наш полином над $\mathbb{Q}$ методом комплетирања квадрата:

$$X^4 - X^2 - 2 = \left(X^2 - \frac{1}{2}\right)^2 - \frac{1}{4} - 2 = \left(X^2 - \frac{1}{2}\right)^2 - \left(\frac{3}{2}\right)^2 =$$

$$= \left(X^2 - \frac{1}{2} - \frac{3}{2}\right)\left(X^2 - \frac{1}{2} + \frac{3}{2}\right) = \left(X^2 - 2\right)\left(X^2 + 1\right) =$$

$$= (X - \sqrt{2})(X + \sqrt{2})(X - i)(X + i),$$

где је i наравно имагинарна јединица. Дакле, коренско поље K је поље $K = \mathbb{Q}(\sqrt{2}, i)$. Ми треба да нађемо α за које је $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\alpha)$. Покушајмо да докажемо да се за α може узети елемент $\alpha = \sqrt{2} + i$. Јасно је да је $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Обратна инклузија је нетривијална. Наравно, довољно је да докажемо да нпр. $\sqrt{2} \in \mathbb{Q}(\alpha)$, пошто из тога непосредно следи да и $i \in \mathbb{Q}(\alpha)$, а тиме и тражено. Једнакост

$$\alpha = \sqrt{2} + i,$$

„подигнимо" на трећи степен. Добијамо

$$\alpha^3 = 2\sqrt{2} + 6i - 3\sqrt{2} - i = -\sqrt{2} + 5i = 5(\sqrt{2} + i) - 6\sqrt{2}.$$

Дакле,

$$\alpha^3 - 5\alpha = 6\sqrt{2},$$

па је

$$\sqrt{2} = \frac{1}{6}(\alpha^3 - 5\alpha) \in \mathbb{Q}(\alpha).$$

♣

Пример 99 Нека је K коренско поље полинома $X^4 - 24X^2 + 4 \in \mathbb{Q}[X]$.
а) Показати да је $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.
б) Одредити $\alpha \in \mathbb{C}$ тако да је $K = \mathbb{Q}(\alpha)$.

Поступимо као у претходном примеру.

$$\begin{aligned} X^4-24X^2+4 &= (X^2-12)^2-144+4\\ &= (X^2-12)^2-140\\ &= (X^2-12)^2-(2\sqrt{35})^2\\ &= (X^2-12-2\sqrt{35})(X^2-12+2\sqrt{35})\\ &= (X^2-(12+2\sqrt{35})(X^2-(12-2\sqrt{35}), \end{aligned}$$

те добијамо $X^4-24X^2+4=(X-\sqrt{12+2\sqrt{35}})(X+\sqrt{12+2\sqrt{35}})(X-\sqrt{12-2\sqrt{35}})(X+\sqrt{12-2\sqrt{35}})$. Према томе, добијамо да је

$$K=\mathbb{Q}\left(\sqrt{12+2\sqrt{35}},\sqrt{12-2\sqrt{35}}\right).$$

Један савет: увек када добијете овакав резултат, није лоше помножити ова два корена и видети шта се добија. Применимо тај савет у овом случају.

$$\sqrt{12+2\sqrt{35}}\cdot\sqrt{12-2\sqrt{35}}=\sqrt{144-140}=\sqrt{4}=2.$$

Дакле, можемо да закључимо да, ако је $\alpha=\sqrt{12+2\sqrt{35}}$, а $\beta=\sqrt{12-2\sqrt{35}}$, онда је $\alpha\cdot\beta=2$, па је $\beta=\frac{2}{\alpha}\in\mathbb{Q}(\alpha)$. Закључујемо да је $K=\mathbb{Q}(\alpha)$. Тако смо нашли примитивни елемент и урадили оно што је тражено под б)!

Други савет: када имате корен попут овога: $\sqrt{12+2\sqrt{35}}$, проверите да можда не можете да га „препознате". Шта то значи? У овом случају, појављује се корен из броја облика $p+q\sqrt{s}$ где су p,q,s цели бројеви. Да ли је можда тај корен збир (или разлика) два корена из неких целих бројева? Како је $35=5\cdot 7$, намеће се да израчунамо колико је $(\sqrt{5}+\sqrt{7})^2$. Добијамо

$$(\sqrt{5}+\sqrt{7})^2=5+2\sqrt{35}+7=12+2\sqrt{35},$$

тј. баш оно што имамо. Дакле, $\alpha=\sqrt{5}+\sqrt{7}$ (приметимо да је $\beta=\sqrt{7}-\sqrt{5}$), те је $K=\mathbb{Q}\left(\sqrt{5}+\sqrt{7}\right)$. Ми треба да покажемо да је $K=\mathbb{Q}\left(\sqrt{5},\sqrt{7}\right)$. То није тешко, поступићемо као у претходном примеру.

$$\begin{aligned} \alpha &= \sqrt{5}+\sqrt{7}\\ \alpha^3 &= 5\sqrt{5}+15\sqrt{7}+21\sqrt{5}+7\sqrt{7}\\ \alpha^3 &= 26\sqrt{5}+22\sqrt{7}\\ 22\alpha &= 22\sqrt{5}+22\sqrt{7}\\ \alpha^3-22\alpha &= 4\sqrt{5}\\ \sqrt{5} &= \frac{\alpha^3-22\alpha}{4}\in\mathbb{Q}(\alpha)\\ \sqrt{7} &= \alpha-\sqrt{5}\\ \sqrt{7} &= \frac{26\alpha-\alpha^3}{4}\in\mathbb{Q}(\alpha). \end{aligned}$$

Наравно, могли смо то да урадимо и другачије. Пошто смо већ препознали да је $\beta = \sqrt{7} - \sqrt{5}$, онда само треба показати да је

$$\mathbb{Q}\left(\sqrt{5} + \sqrt{7}, \sqrt{7} - \sqrt{5}\right) = \mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right),$$

а то је наравно врло једноставно. ♣

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 100 Полином $f \in E[X]$ има двоструку нулу $\alpha \in E$ 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 101 Нека је $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in F[X]$. Тада се извод полинома дефинише са:

$$f'(X) \colon = a_1 + 2a_2 X + \cdots + n a_n X^{n-1}.$$

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 102 Полином $f \in F[X]$ има двоструку нулу $\alpha \in F$ акко $f(\alpha) = f'(\alpha) = 0$.

Доказ. $\Longrightarrow$: 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 $f'(\alpha) = 0$.

$\Longleftarrow$: Претпоставимо да је $f(\alpha) = f'(\alpha) = 0$. Поделимо 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

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

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. □

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

Став 103 Нека је $f(X) \in F[X]$. Тада f има вишеструку нулу у неком проширењу E поља F ако и само је $\mathrm{NZD}(f(X), f'(X)) \neq 1$.

Доказ. $\Longrightarrow$: Претпоставимо да постоји проширење E поља F и елемент $\alpha \in E$ такав да је $f(\alpha) = f'(\alpha) = 0$ (видети претходни став). Уколико би важило да је $\mathrm{NZD}(f(X), f'(X)) = 1$, 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, $\mathrm{NZD}(f(X), f'(X)) \neq 1$.

$\Longleftarrow$: Нека је $d(X) = \mathrm{NZD}(f(X), f'(X)) \neq 1$. Како је $\deg d(X) > 0$, на основу ранијих резултата постоји проширење 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 проширењу поља F има вишеструку нулу. □

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

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

Пример 105 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 **82** 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 (то раширење можемо добити као $F[X]/\langle a(X)\rangle$) α. 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 $\operatorname{char} E = \operatorname{char} \mathbb{Z}_3(t) = \operatorname{char} \mathbb{Z}_3 = 0$, те је α трострука нула полинома $a(X)$ у раширењу E. ♣

Коначна поља

Докажимо најпре следећу једноставну чињеницу.

Став 106 Свако коначно поље има p^n елемената, за неки прост број p и природан број $n \geqslant 1$.

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. □.

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 107 Нека је F поље са $q = p^n$ елемената, где је p прост број и $n \geqslant 1$. 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. □

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

Теорема 108 За сваки прост број p и природан број $n \geqslant 1$ 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 линеарних различитих 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 $1 \leqslant k \leqslant p-1$ 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 $1 \leqslant k \leqslant p-1$: $\binom{p}{k}\alpha^{p-k}\beta^k = q_k(p\alpha^{p-k}\beta^k) = 0$, као што је примећено горе. Сада није тешко показати индукцијом да је

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

  за све $r \geqslant 1$, 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. □

Покажимо сада јединственост.

Теорема 109 Нека су K и K' поља са p^n елемената где је p прост број и $n \geqslant 1$. Тада је $K \cong K'$.

Доказ. Из Алгебре 1 нам је познато (поновити ту чињеницу) да је свака коначна подгрупа мултипликативне групе поља циклична. Стога је група $(K \setminus \{0\}, \cdot)$ циклична. Дакле постоји елемент $\alpha \in K \setminus \{0\}$ такав да је $K \setminus \{0\} = \{1, \alpha, \ldots, \alpha^{q-2}\}$. Наравно, $\alpha^{q-1} = 1$ (овде је $q = p^n$). Стога је $K = \mathbb{F}_p(\alpha)$. Нека је $f(X)$ минимални полином за α над $\mathbb{F}_p$. Тада је $\mathbb{F}_p[X]/\langle f(X)\rangle \cong \mathbb{F}_p(\alpha)(= K)$. Дакле, $f(\alpha) = 0$, а такође је и $a(\alpha) = 0$, где је $a(X) = X^q - X$. Како је $f(X)$ минимални полином, можемо да закључимо да $f(X) \mid a(X)$.

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

Напомена 110 Приметимо да смо у оквиру овог доказа показали да увек имамо примитивни елемент за раширење $\mathbb{F}_p \subset K$, ако је K коначно поље. На сличан начин се може показати да примитиван елемент постоји и за раширење $F \subset E$, где су E и F коначна поља. ♢

Показали смо да за сваки прост број p и природан $n \geqslant 1$ 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 покажимо и везу између неизоморфних коначних поља исте карактеристике.

Став 111 Поље са p^m елемената је потпоље поља са p^n елемената ако и само ако $m \mid n$.

Доказ. $\Longleftarrow$. Нека је $q = p^n$ и $r = p^m$, где $m \mid n$. Посматрајмо, као у доказу теореме **108**, 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 **108** 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 $\mathbb{Z}[Y]$:

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

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

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

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.

$\Longrightarrow$. 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. □

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 $\mathbb{F}_4 = \{\alpha \in \mathbb{F}_{16} : \alpha^4 = \alpha\}$.

Неки алгоритми за факторизацију полинома са једном неодређеном

Практичан проблем факторизације полинома појављује се у многим областима симболичног рачунања. Значајан је као помоћ у разрешавању проблема поједностављивања израза, симболичке интеграције и решавању алгебарских једначина. Такође се користи у алгебарској теорији кодирања и криптографији.

У оквиру курса ћемо кратко приказати два алгоритма. Први се односи на налажење такозване бесквадратне факторизације која проблем факторизације своди на проблем факторизације полинома који немају поновљених фактора и који се односи на било који домен са једнозначном факторизацијом, а други је Берлекампов алгоритам који се користи за факторизацију оних полинома који немају поновљених фактора и односи се на факторизацију над коначним пољима.

Бесквадратна факторизација

У овом пододељку подразумевамо да су сви прстени са којима радимо домени са једнозначном факторизацијом. Уведимо најпре појам бесквадратног полинома.

Дефиниција 112 За примитивни полином $a(X) \in A[X]$ кажемо да је бесквадратни уколико нема нетривијалних поновљених фактора, тј. не постоји полином $b(X) \in A[X]$ такав да је $\deg b(X) \geq 1$ и $b(X)^2 \mid a(X)$.

Бесквадратна факторизација примитивног полинома $a(X)$ је факторизација у облику

$$a(X) = a_1(X)a_2(X)^2 \cdots a_k(X)^k,$$

при чему су сви полиноми $a_i(X)$ бесквадратни и пар-по-пар су узајамно прости, тј. $\mathrm{NZD}(a_i(X), a_j(X)) = 1$ за $i \neq j$.

Напомена 113 Сами полиноми $a_i(X)$ не морају бити нерастављиви, они само немају поновљене факторе. ♢

Напомена 114 Није искључена могућност да се у горњој факторизацији не појављује неки од чланова наведеног облика. На пример факторизација

$$a(X) = (X^2 - 1)^2(X^2 + X + 1)^5 \in \mathbb{Q}[X],$$

је бесквадратна факторизација. Поента је да се налажењем ове факторизације проблем факторизације полинома своди на проблем факторизације бесквадратних полинома. Уколико је почетни полином $a(X)$ сам бесквадратни, онда имамо тривијалну бесквадратну факторизацију, тј. $k = 1$, а $a_1(X) = a(X)$. ♢

Упоредити следећи став са ставом **103**.

Став 115 Нека је $a \in A[X]$ примитивни полином, где је A домен са једнозначном факторизацијом карактеристике 0. Тада је a бесквадратни **акко** је $\mathrm{NZD}(a, a') = 1$.

Доказ. $\Longleftarrow$: Претпоставимо да је $a = b^2 c$ за неки полином b, такав да је $\deg b \geq 1$. Тада је $a' = 2bb'c + b^2 c'$, те b дели и a и a'. Стога је $\mathrm{NZD}(a, a') \neq 1$.

$\Longrightarrow$: Како је a бесквадратни, то се у његовој факторизацији на нерастављиве полиноме: $a = p_1 p_2 \cdots p_k$ нерастављиви фактори не понављају. Тада је

$$a' = p_1' p_2 \cdots p_k + p_1 p_2' \cdots p_k + \cdots + p_1 p_2 \cdots p_k'. \tag{12}$$

Како су p_i једини нерастављиви фактори од a, уколико имамо да је $\mathrm{NZD}(a, a') \neq 1$, неки од тих фактора мора делити a'. Нека је то p_{i_0}. Из (**12**) следи да тада

$$p_{i_0} \mid p_1 \cdots p_{i_0 - 1} p_{i_0}' p_{i_0 + 1} \cdots p_k.$$

Како је p_{i_0} нерастављив и $p_{i_0} \nmid p_i$ за $i \neq i_0$, добијамо да $p_{i_0} \mid p_{i_0}'$, но ово није могуће, јер је $\deg p_{i_0}' < \deg p_{i_0}$, а $p_{i_0}' \neq 0$, јер је карактеристика прстена A једнака 0. Ова контрадикција нам завршава доказ. □

Размотримо сада како да дођемо до тражене бесквадратне факторизације. Анализирајмо ситуацију, тј. претпоставимо да је $a = a_1 a_2^2 \cdots a_k^k$ тражена факторизација. Тада је

$$\begin{aligned} a' &= a_1' a_2^2 \cdots a_k^k + a_1 \cdot 2 a_2 a_2' \cdots a_k^k + a_1 a_2^2 \cdot 3 a_3^2 a_3' \cdots a_k^k + \cdots + a_1 a_2^2 \cdots k a_k^{k-1} a_k' \\ &= a_2 a_3^2 \cdots a_k^{k-1} (a_1' a_2 \cdots a_k + 2 a_1 a_2' a_3 \cdots a_k + 3 a_1 a_2 a_3' \cdots a_k + \cdots + k a_1 a_2 a_3 \cdots a_k'). \end{aligned} \tag{13}$$

Ако је p било који нерастављив полином, који дели a, онда он дели и a_i за неко i, а не дели остале a_j, јер су они узајамно прости са a_i. Ако би тај p делио и елемент који се налази у загради у (**13**), онда би он морао да дели и a_i' пошто сви остали сабирци садрже a_i. Но, то би значило да је $\mathrm{NZD}(a_i, a_i') \neq 0$, па a_i не би био бесквадратни што противречи нашој претпоставци. Из овога следи да је

$$d = \mathrm{NZD}(a, a') = a_2 a_3^2 \cdots a_k^{k-1}. \tag{14}$$

Сада нам је јасно како да нађемо a_1. Наиме, $a/d = a_1 a_2 \cdots a_k$,

$$\mathrm{NZD}(d, a/d) = \mathrm{NZD}(a_2 a_3^2 \cdots a_k^{k-1}, a_1 a_2 \cdots a_k) = a_2 \cdots a_k, \tag{15}$$

те је

$$a_1 = (a/d)/\mathrm{NZD}(d, a/d) = \frac{a}{d \cdot \mathrm{NZD}(d, a/d)}. \tag{16}$$

Наравно, налажење a_2 се добија на исти начин полазећи од d, узимајући у обзир (**14**). Но, овде можемо да приметимо да НЕ морамо да рачунамо d', нама заправо треба $d_1 = \mathrm{NZD}(d, d')$ а то знамо да одредимо. Наиме, видимо да мора бити — погледајте (**14**) и (**15**):

$$d_1 = a_3 a_4^2 \cdots a_k^{k-2} = d/\mathrm{NZD}(d, a/d). \tag{17}$$

Поступак се завршава када добијемо јединицу коју би требало да факторишемо.

Пример 116 Наћи бесквадратну факторизацију полинома

$$a(X) = X^8 - 2X^6 + 2X^2 - 1 \in \mathbb{Z}[X].$$

Имамо да је $a' = 8X^7 - 12X^5 + 4X$. Добијамо редом (читаоци треба да провере ове рачунице сами):

$$\begin{aligned} d = \mathrm{NZD}(a, a') &= X^4 - 2X^2 + 1, \\ a/d &= X^4 - 1, \\ \mathrm{NZD}(d, a/d) &= X^2 - 1, \\ a_1 = (a/d)/\mathrm{NZD}(d, a/d) = (X^4 - 1)/(X^2 - 1) &= X^2 + 1. \end{aligned}$$

Настављамо са d.

$$\begin{aligned} d_1 = d/\mathrm{NZD}(d, a/d) &= X^2 - 1, \\ d/d_1 &= X^2 - 1, \\ \mathrm{NZD}(d_1, d/d_1) &= X^2 - 1, \\ a_2 = (d/d_1)/\mathrm{NZD}(d_1, d/d_1) = (X^2 - 1)/(X^2 - 1) &= 1. \end{aligned}$$

За налажење a_3 користимо d_1.

$$d_2 = d_1/\mathrm{NZD}(d_1, d/d_1) = \mathrm{NZD}(X^2 - 1, X^2 - 1) = 1.$$

Дакле, ово је крај, $a_3 = (d_1/d_2)/\mathrm{NZD}(d_2, d_1/d_2) = d_1$, те је бесквадратна факторизација:

$$a = a_1 \cdot a_2^2 \cdot a_3^3 = (X^2+1) \cdot 1 \cdot (X^2-1)^3 = (X^2+1)(X^2-1)^3. \qquad \spadesuit$$

Наравно да смо, пошто је пример једноставан, могли да се 'довијамо' и да ово брже нађемо, али овде показујемо алгоритам постепеним налажењем свих фактора.

Позабавимо се сада бесквадратном факторизацијом у случају да карактеристика није једнака 0. То нећемо радити у општем случају домена са једнозначном факторизацијом, него у специјалном, али довољно важном случају коначних поља.

Дакле, нека је сада F неко коначно поље карактеристике p. Гледајући претходни поступак, видимо да је разлика у томе што се може десити да је неки полином различит од нуле, а да му је извод једнак нули. Но, следећи став нам у томе помаже.

Став 117 Ако је $0 \neq a \in F[X]$, где је $\operatorname{char} F = p$ и ако је $a' = 0$, онда постоји полином $b \in F[X]$ такав да је $a = b^p$.

Доказ. Нека је $a = a_n X^n + \cdots a_1 X + a_0$. Тада је $a' = n a_n X^{n-1} + \cdots + 2a_2 X + a_1$. Како је $a' = 0$, имамо да је за све $k = \overline{0,n}$: $k a_k = 0$. То значи да је за све $k = \overline{0,n}$: $k 1_F = 0_F$ или је $a_k = 0_F$. С обзиром да је $\operatorname{char} F = p$, ово се своди на то да, ако $p \nmid k$, онда је $a_k = 0_F$ (пошто је $k1_F = 0_F$, ако $p \mid k$). Дакле, полином a је облика

$$a = a_{pm} X^{pm} + a_{p(m-1)} X^{p(m-1)} + \cdots + a_p X^p + a_0.$$

Подсетимо се сада резултата који смо доказали за коначна поља: ако је $|F| = q = p^n$ за неко n, онда је $x^{p^n} = x^q = x$ за све $x \in F$. Посебно, добијамо да је $(x^{p^{n-1}})^p = x$. Дакле,

$$\begin{aligned}
a &= a_{pm} X^{pm} + a_{p(m-1)} X^{p(m-1)} + \cdots + a_p X^p + a_0 \\
&= a_{pm}^{p^n} X^{pm} + a_{p(m-1)}^{p^n} X^{p(m-1)} + \cdots + a_p^{p^n} X^p + a_0^{p^n} \\
&= (a_{pm}^{p^{n-1}})^p (X^m)^p + (a_{p(m-1)}^{p^{n-1}})^p (X^{(m-1)})^p + \cdots + (a_p^{p^{n-1}})^p X^p + (a_0^{p^{n-1}})^p \\
&= (a_{pm}^{p^{n-1}} X^m + a_{p(m-1)}^{p^{n-1}} X^{(m-1)} + \cdots + a_p^{p^{n-1}} X + a_0^{p^{n-1}})^p \\
&= b^p. \qquad \square
\end{aligned}$$

Дакле, поступак за налажење бесквадратне факторизације у случају коначних поља има једноставно додатно гранање. Уколико се испостави да је извод полинома са којим се ради једнак 0, онда је он сам p-ти степен неког полинома (ако је карактеристика поља p) и, када одредимо тај полином, даље радимо са њим. Иначе поступамо као и у случају поља карактеристике 0.

Илуструјмо ово једним примером.

Пример 118 Нека је $a = X^{11} + 2X^9 + 2X^8 + X^6 + X^5 + 2x^3 + 2X^2 + 1 \in \mathbb{F}_3[X]$. Наћи бесквадратну факторизацију полинома a.

Имамо да је

$$a' = 11X^{10} + 18X^8 + 16X^7 + 6X^5 + 5X^4 + 6X^2 + 4X = 2X^{10} + X^7 + 2X^4 + X.$$

Како је $a' \neq 0$ настављамо као и у случају карактеристике 0.

$$\begin{aligned}
d = \mathrm{NZD}(a, a') &= X^9 + 2X^6 + X^3 + 2, \\
a/d &= X^2 + 2, \\
\mathrm{NZD}(d, a/d) &= X + 2, \\
a_1 = (a/d)/\mathrm{NZD}(d, a/d) &= (X^2 + 2)/(X + 2) = X + 1.
\end{aligned}$$

Сада радимо са d. Добијамо да је $d' = 0$. Сада смо у новој ситуацији. До сада смо добили a_1, а знамо и да је

$$a = a_1 \cdot \mathrm{NZD}(d, a/d) \cdot d = (X + 1)(X + 2)d.$$

Како је $d' = 0$ постоји d_1 такав да је $d = d_1^3$. У овом случају је d_1 врло лако наћи пошто је у питању поље $\mathbb{F}_3$ и у њему је сваки елемент једнак свом трећем степену, те нема никакве додатне рачунице (у случају да смо, на пример радили у пољу $\mathbb{F}_9$, било би потребно наћи треће степене коефицијената да би се одредили коефицијенти полинома d_1). Дакле, имамо да је $d_1 = X^3 + 2X^2 + X + 2$ и $d_1' = X + 1 \neq 0$. Но,

$$\mathrm{NZD}(d_1, d_1') = \mathrm{NZD}(X^3 + 2X^2 + X + 2, X + 1) = 1,$$

те је d_1 бесквадратни. Дакле, до сада смо добили да је

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

Но, $(X + 2) \mid d$ и знамо да сигурно не „улази" у a_1 па стога мора бити и $(X+2) \mid d_1$. Заправо је $X^3+2X^2+X+2 = (X+2)(X^2+1)$, па добијамо да је

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

што је заправо тражена бесквадратна факторизација. Дакле, овде је $k = 4, a_1 = X + 1, a_2 = 1, a_3 = X^2 + 1, a_4 = X + 2$. ♣

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

У овом пододељку 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 $d = \mathrm{NZD}(f, f')$. 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 119 Нека је $q = p^n$, за неки прост број p и $n \geq 1$, $f \in \mathbb{F}_q[X]$. Ако је $d = \mathrm{NZD}(f, f')$, 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, која ће нам бити од централног значаја за доказ.

Став 120 Нека $f \mid g_1 g_2 \cdots g_s$, при чему су $f, g_1, \ldots, g_s \in \mathbb{F}_q[X]$ и $\mathrm{NZD}(g_i, g_j) = 1$ за $i \neq j$. Тада је

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

Доказ. Дакле, претпоставимо да $f \mid g_1 g_2 \cdots g_s$. 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:

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

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

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

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

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

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 $h \in F_q[X]$ такве 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 $d = \mathrm{NZD}(h - c, h - c')$ 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

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

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 $\overline{h}$ означимо слику класу полинома h у овом прстену, имамо да је у њему $\overline{h}^q = \overline{h}$. 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 **36**, нам даје:

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

Но, знамо да је за копросте идеале P_i, P_j, на основу става **34**: $P_i \cap P_j = P_i \cdot P_j$. Уз тај став и лему **35** (видети и коментар после доказа теореме **36**) 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

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

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

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

таквој да је

$$(\overline{h}_1, \overline{h}_2, \ldots, \overline{h}_k)^q = (\overline{h}_1, \overline{h}_2, \ldots, \overline{h}_k),$$

те је $\overline{h}_i^q = \overline{h}_i$ за све $i = \overline{1,k}$. С обзиром да су, а приори, полиноми f_i различитог степена и поља $F_i = F_q[X]/_{P_i}$ 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 $\overline{h}_i$ су елементи из $\mathbb{F}_q$. Дакле, $(\overline{h}_1, \overline{h}_2, \ldots, \overline{h}_k) \in \mathbb{F}_q^k$. Стога је и

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

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 $e = [\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1}]$. 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 $\beta\colon V \to V$ дефинисано са $\beta(u) = u^q$ једно линеарни оператор простора V, то је $W = \mathrm{Ker}(\beta - I_V)$, где смо са I_V означили идентични оператор на простору V. Дакле, ако одредимо $\mathrm{Ker}(\beta - I_V)$ знаћемо колико има фактора у факторизацији за f. А затим ћемо, користећи став **120** покушати да одредимо и саму факторизацију.

За налажење $\mathrm{Ker}(\beta - I_V)$ 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 121 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 бесквадратни. Имамо да је $f' = X^6 + 2X^4 + 2X^3 + X$. Добија се да је $d = \mathrm{NZD}(f, f') = X + 1$. 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 $e = [\overline{1}, \overline{X}, \overline{X}^2, \overline{X}^3, \overline{X}^4, \overline{X}^5]$ и то је простор димензије 6, пошто је степен полинома g једнак 6. У нашем случају је $q = 3$ и потребно је елементе $\left(\overline{X}^i\right)^3$ за $i = \overline{0,5}$ изразити у бази e.

$$\overline{1}^3 = \overline{1},$$
$$\overline{X}^3 = \overline{X}^3,$$
$$\left(\overline{X}^2\right)^3 = \overline{X}^6 = -\overline{X}^5 - 2\overline{X}^3 - \overline{X}^2 - \overline{X} - \overline{2} = 2\overline{X}^5 + \overline{X}^3 + 2\overline{X}^2 + 2\overline{X} + \overline{1}.$$

Застанимо овде. Заправо, ако желимо да елемент $a(\overline{X})$, 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 $\overline{X}^3$ и сређивати. Нећемо писати сав рачун пошто би било мало непрегледно, него само почетак и крај.

$$\left(\overline{X}^3\right)^3 = 2\overline{X}^8 + \overline{X}^6 + 2\overline{X}^5 + 2\overline{X}^4 + \overline{X}^3 = \overline{X}^5 + \overline{X}^4 + \overline{X}^3 + \overline{X}^2 + \overline{X},$$
$$\left(\overline{X}^4\right)^3 = \overline{X}^8 + \overline{X}^7 + \overline{X}^6 + \overline{X}^5 + \overline{X}^4 = \overline{X}^5 + 2\overline{X} + \overline{1},$$
$$\left(\overline{X}^5\right)^3 = \overline{X}^8 + 2\overline{X}^4 + \overline{X}^3 = 2\overline{X}^3 + \overline{X}^2 + \overline{X} + \overline{1}.$$

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 $(B - I_6)X = O$.

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

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:

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

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

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

те је

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

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.

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

Дакле, „кренуло је", добили смо да је

$$g(X) = (X^4 + X^3 + 2X^2 + X + 2)(X^2 + 1). \tag{18}$$

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

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

Добијамо нову факторизацију:

$$g(X) = (X^5 + 2X^2 + 2X + 2)(X + 1). \tag{19}$$

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 (**18**). 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 $d = \mathrm{NZD}(f, f') = X + 1$ и да имамо факторизацију $g = f/d$, коначно добијамо тражену факторизацију:

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

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:

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

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 122 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:

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

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

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

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

Докажимо да је I идеал у A. Најпре, ако је $x \in I$ и $a \in A$, онда $x \in I_j$ за неко $j \geqslant 0$. 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 $j_1, j_2 \geqslant 0$. 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

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

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

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

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

(2) $\Longrightarrow$ (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

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

тј. добијамо бесконачни строго растући низ идеала

$$I_0 \subset I_1 \subset I_2 \subset \cdots$$

што противречи претпоставци (2). □

Дефиниција 123 За комутативан прстен A кажемо да је Нетерин ако испуњава било који од ова два еквивалентна услова.

Пример 124 Нека је A прстен свих непрекидних функција $f\colon [0,1] \to \mathbb{R}$, при чему су операције међу функцијама дефинисане тачка по тачка:

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

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 $g : [0,1] \to \mathbb{R}$ дефинисана са

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

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 125 (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:

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$$

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

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

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 $0 \leqslant k \leqslant m$, $1 \leqslant j_k \leqslant s_k$ генеришу идеал

I. Означимо са $\widetilde{I}$ идеал у $A[X]$ генерисан овим полиномима. Очигледно је $\widetilde{I} \subseteq I$. Докажимо другу инклузију.

Нека је $f \in I \setminus \{0\}$. Доказ изводимо индукцијом по степену 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 $f_{01}, \ldots, f_{0s_0}$ константни полиноми који генеришу овај идеал, видимо да $f \in \widetilde{I}$.

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

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

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

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

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

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

$\mathbf{t > m}$. Дакле, f је полином степена t, те $LC(f) \in I_t = I_m$. Како $a_{m1}, \ldots, a_{ms_m}$ генеришу идеал I_m, то постоје $b_{m1}, \ldots, b_{ms_m} \in A$ такви да је

$$LC(f) = b_{m1}a_{m1} + \cdots + b_{ms_m}a_{ms_m}.$$

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

$$\deg(f - X^{t-m}b_{m1}f_{m1} - \cdots - X^{t-m}b_{ms_m}f_{ms_m}) < t,$$

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

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

Напомена 126 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. ♢

Последица 127 Сваки идеал у прстену $K[X_1, \ldots, X_n]$ је коначно генерисан.

Доказ. Заправо је све већ урађено. Индукцијом по n се показује да је $K[X_1, \ldots, X_n]$ Нетерин прстен, а то управо значи да је сваки идеал у њему коначно генерисан. □

Диксонова лема

У овом кратком одељку доказаћемо једно чисто комбинаторно тврђење које ће нам користити у даљем.

Став 128 (Диксонова лема) Нека је $n \geqslant 1$. На скупу $\mathbb{N}^n$ дефинишемо уређење $\ll$ са:

$$(x_1, x_2, \ldots, x_n) \ll (y_1, \ldots, y_n) \stackrel{\text{def}}{\Longleftrightarrow} (x_1 \leqslant y_1 \text{ и } x_2 \leqslant y_2 \text{ и } \ldots \text{ и } x_n \leqslant y_n).$$

Нека је T произвољан непразан подскуп од $\mathbb{N}^n$. Тада је скуп минималних елемената у T у односу на ово уређење коначан.

Доказ. Доказаћемо заправо да у парцијално уређеном скупу $(\mathbb{N}^n, \ll)$ не постоји бесконачан антиланац (бесконачан скуп у коме су свака два елемента међусобно неупоредива). Ово нам доказује да и ма који подскуп од $\mathbb{N}^n$ не може имати бесконачан скуп минималних елемената, јер и минимални елементи чине један антиланац. Представићемо два доказа.

Први доказ. Тврђење доказујемо индукцијом по n. У случају $n = 1$ тврђење је тривијално пошто сваки непразан подскуп од $\mathbb{N}$ има **најмањи** елемент.

Претпоставимо да је $n > 1$ и да је тврђење тачно за све бројеве мање од n. Претпоставимо да је S бесконачан антиланац у $\mathbb{N}^n$. Нека је $(a_1, \ldots, a_n)$ произвољан елемент у S. Тада скуп S можемо да 'разбијемо' на два дисјунктна скупа: $S = S_+ \sqcup S_-$, где је

$$S_+ = \{(x_1, \ldots, x_n) \in S : x_n > a_n\},$$

$$S_- = \{(x_1, \ldots, x_n) \in S : x_n \leqslant a_n\}.$$

Бар један од ова два скупа је бесконачан. Уколико је то скуп S_-, онда постоји природан број $k \in \{0, \ldots, a_n\}$ такав да је скуп

$$\widetilde{S} = \{(x_1, \ldots, x_{n-1}) \in \mathbb{N}^{n-1} : (x_1, \ldots, x_{n-1}, k) \in S\}$$

бесконачан. Но, тада је $\widetilde{S}$ бесконачан антиланац у $\mathbb{N}^{n-1}$ што противречи индуктивној хипотези. Закључујемо да је скуп S_+ бесконачан. Тада је $S_+ = S_{++} \sqcup S_{+-}$, где је

$$S_{++} = \{(x_1, \ldots, x_n) \in S_+ : x_{n-1} > a_{n-1}\},$$

$$S_{+-} = \{(x_1, \ldots, x_n) \in S_+ : x_{n-1} \leqslant a_{n-1}\}.$$

Бар један од ова два скупа је бесконачан и као и пре, то мора бити скуп S_{++}. Дакле, за сваки елемент $(x_1, \ldots, x_n)$ скупа S_{++} важи: $x_n > a_n$, $x_{n-1} > a_{n-1}$. Поступак настављамо док не добијемо бесконачан скуп

$S_{\underbrace{+\ldots+}_{n}} \subset S$ у коме је за све i: $x_i > a_i$, што противречи претпоставци да су у S неупоредиви елементи (подсетимо се да је $(a_1, \ldots, a_n) \in S$).

Други доказ. Нека је, као и у претходном доказу $(a_1, \ldots, a_n) \in S$, где је S неки бесконачан антиланац. За $1 \leqslant i \leqslant n$ уочимо скупове

$$S_i = \{(x_1, \ldots, x_n) \in S : x_i \leqslant a_i\}$$

и скуп

$$S_0 = \{(x_1, \ldots, x_n) \in S : (\forall i) x_i > a_i\}.$$

Тада је

$$S = S_0 \sqcup (S_1 \cup S_2 \cup \cdots \cup S_n),$$

те је бар један од ових скупова бесконачан. Ако би то био неки од скупова S_i за $1 \leqslant i \leqslant n$, добили бисмо контрадикцију на исти начин на који смо је добили из претпоставке да је скуп S_- бесконачан. Дакле, скуп S_0 мора бити бесконачан. Но, $(a_1, \ldots, a_n) \notin S_0$ и за сваки елемент $(x_1, \ldots, x_n)$ у скупу S_0 важи

$$(a_1, \ldots, a_n) \ll (x_1, \ldots, x_n).$$

Ово противречи претпоставци да је S антиланац (довољно је било да нађемо у S један елемент упоредив са $(a_1, \ldots, a_n)$, а различит од њега, а ми нађосмо бесконачно много њих!). □

Мономни поредак и редукције полинома

Ми сада знамо да је сваки идеал у прстену полинома $K[X_1, \ldots, X_n]$, где је K поље, коначно генерисан. За дати идеал $I = \langle h_1, \ldots, h_k \rangle$ природно се појављује питање *припадности идеалу*. Како установити да ли је дати полином f у идеалу I?

Погледајмо најпре најједноставнији случај: $n = 1, k = 1$ (овде ћемо мало поновити нешто из ранијих лекција, али корисно је то у овом тренутку). Дакле, питамо се да ли полином $f(X) \in K[X]$ припада идеалу генерисаном полиномом $h_1(X) \in K[X]$. Јасно је како то радимо. Једноставно поделимо полином $f(X)$ полиномом $h_1(X)$ и проверимо да ли је остатак једнак 0. Ако јесте, онда је $f(X) = q(X)h_1(X)$ за неки полином $q(X)$ и $f(X)$ јесте у том идеалу. У случају да постоји ненула остатак, полином није у идеалу. Дакле, ништа простије. Подсетимо се како се врши дељење. Нека је $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ и $h_1(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$. Уколико је $n < m$ ништа не можемо да урадимо, зато посматрајмо случај $n \geqslant m$. Шта радимо? Посматрамо *искључиво* мономе $a_n X^n$ и $b_m X^m$ и први моном поделимо другим. Добијамо да је резултат $\frac{a_n}{b_m} X^{n-m}$. То ће нам бити

први моном у количнику. Потом помножимо тим мономом полином $h_1(X)$ и одузмемо резултат од полинома f. Добијамо нови полином $f_1(X) = f(X) - \frac{a_n X^n}{b_m X^m} h_1(X)$. Ово можемо записати и овако:

$$f \xrightarrow{h_1} f_1,$$

и то можемо читати: полином f је сведен (редукован) на полином f_1 помоћу полинома h_1. Да бисмо поједноставили запис, полиноме смо писали без експлицитног навођења неодређене. То ћемо често радити и даље.

Поступак даље примењујемо на полином f_1. Ово се наставља све док не дођемо или до нуле или до полинома степена мањег од степена полинома h_1. Тај добијени полином, који можемо (не превише маштовито) да означимо са r, заправо је остатак при дељењу полинома f полиномом h_1. То се у претходној симболици записује и овако:

$$f \xrightarrow{h_1} f_1 \xrightarrow{h_1} f_2 \xrightarrow{h_1} \cdots \xrightarrow{h_1} f_s = r.$$

Дакле, дељење једног полинома другим заправо се састоји из више корака које називамо редукције. Ово дељење нам једноставно омогућава да разрешимо питање припадности идеалу у случају полинома са једном неодређеном и идеала генерисаног једним елементом.

Шта се дешава у случају $n = 1, k = 2$? Тада имамо идеал $I = \langle h_1(X), h_2(X) \rangle$. Како установити да ли дати полином f припада овом идеалу? Рекло би се, ништа посебно. Рецимо, поделимо полином f полиномом h_1. Ако је остатак 0, онда јесте у идеалу, ако није, онда тај остатак поделимо полиномом h_2. Сад, ту постоји извесна произвољност – зашто прво h_1, па после h_2, али добро. Но, да ли ово 'ради'?

Размотримо следећи пример: $f = X^3 + X$, $h_1 = X^2 - X$, $h_2 = X^2$. Вршимо редукције полиномом h_1:

$$X^3 + X \xrightarrow{h_1} X^2 + X \xrightarrow{h_1} 2X.$$

У првој редукцији смо од полинома f одузели полином h_1 помножен мономом $X = \frac{X^3}{X^2}$, а потом смо од добијеног полинома одузели полином h_1 помножен мономом $1 = \frac{X^2}{X^2}$. Све по правилима којима вршимо редукције. Добили смо полином $2X$ и њега не можемо више да редукујемо полиномом h_1. Добро, пређимо на полином h_2... Али, не можемо да га редукујемо ни полиномом h_2! Чини се да он није у идеалу. А шта би се десило да смо прво редуковали полиномом h_2?

$$X^3 + X \xrightarrow{h_2} X.$$

Опет не можемо да наставимо даље. Приметимо да нисмо добили исти резултат. Но, ми смо дељење раставили на појединачне кораке – редукције. Можда можемо да мало редукујемо помоћу h_1, а мало помоћу h_2?

$$X^3 + X \xrightarrow{h_1} X^2 + X \xrightarrow{h_2} X.$$

Како год да радимо, не добијамо да полином припада идеалу. Али, јасно се види да полином јесте у идеалу: $X = h_2 - h_1$, па $X \in I$, а $f = (X^2 + 1) \cdot X$, па $f \in I$.

Дакле, овај наш поступак не ради баш добро. Требало би мало да размислимо. Очигледно је било погрешно користити само полиноме h_1 и h_2. Треба гледати и друге полиноме који су у идеалу. Наравно, лако ћемо се досетити како ово поправити. Не само за овај посебан случај, него уопште. Ми врло добро знамо да је прстен полинома $K[X]$ главноидеалски, тј. у њему је сваки идеал генерисан једним полиномом. Знамо и који је то полином. То је полином који је заправо највећи заједнички делилац тог коначног броја полинома који генеришу идеал. У случају два полинома, највећи заједнички делилац се добија Еуклидовим алгоритмом, а за више полинома се поступак итерира. У нашем случају се лако добија да је $\mathrm{NZD}(X^2 - X, X^2) = X$ и онда је све јасно (и лако).

Према томе, проблем припадности идеалу $I = \langle h_1, \ldots, h_k \rangle$ решили смо преласком на „бољи" генераторни скуп. У случају идеала генераторни скуп назива се, као што рекосмо, и база. Дакле, од базе $\{h_1, \ldots, h_k\}$ прелазимо на једночлану базу $\{\mathrm{NZD}(h_1, \ldots, h_k)\}$ и тада се проблем припадности идеалу једноставно решава.

Позабавимо се сада случајем полинома са више неодређених. Морамо пре свега, да разјаснимо дељење у прстену полинома са више неодређених. Као што смо видели, дељење је заправо низ редукција, те ћемо стога разјаснити појам редукције.

Када вршимо редукцију полинома са једном неодређеном, ми се концентришемо на два монома, који су заправо мономи највећег степена у два полинома које разматрамо. Другим речима, они су **водећи мономи**. Како то изгледа у случају полинома са више неодређених? На пример, који је то водећи моном у полиному $X^3Y + 4X^2Y^2 + 3X^2Y + Y^3 - X^2 + 2Y - 1$? Ако гледамо по тоталним степенима, онда су и X^3Y и $4X^2Y^2$ степена 4. Наравно, можемо да се концентришемо на највиши степен од X. Али, шта рећи за овај полином: $X^2Y^2Z + X^2YZ^2 - Y^2 + 3Z - 5$? Овде можемо да гледамо већи степен од Y. Треба то пажљивије осмислити.

Ево мало пригодне терминологије. Ако је $cX_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}$ **моном**, онда је ту c **коефицијент**, а $X_1^{\alpha_1}X_2^{\alpha_2}\cdots X_n^{\alpha_n}$ је **производ степена неодређених**, кратко **производ**. Овај производ ћемо кратко означавати

са $\boldsymbol{X}^{\boldsymbol{\alpha}}$ (овде су $\boldsymbol{X}$ и $\boldsymbol{\alpha}$ одговарајуће n-торке). (Овде није лоше напоменути да је при писању згодно, уместо овако затамњених слова, та слова подвући, тј. $\underline{X}$ уместо $\boldsymbol{X}$ и $\underline{\alpha}$ уместо $\boldsymbol{\alpha}$.)

Желимо да уведемо неки поредак на скупу свих производа $\mathbb{P}_n$. Пре свега желимо да тај поредак проширује поредак у смислу дељивости, тј. да из $\boldsymbol{X}^{\boldsymbol{\alpha}} \mid \boldsymbol{X}^{\boldsymbol{\beta}}$ следи $\boldsymbol{X}^{\boldsymbol{\alpha}} \preceq \boldsymbol{X}^{\boldsymbol{\beta}}$. Такође желимо да тако добијемо ДОБРО УРЕЂЕНИ скуп свих производа, јер не желимо бесконачан опадајући низ: $\boldsymbol{X}^{\boldsymbol{\alpha}_1} \succ \boldsymbol{X}^{\boldsymbol{\alpha}_2} \succ \ldots$. Посебно, то значи да имамо једно ЛИНЕАРНО УРЕЂЕЊЕ, тј. свака два производа морају бити упоредива. Приметимо да је и $1 \preceq \boldsymbol{X}^{\boldsymbol{\alpha}}$ за свако $\boldsymbol{\alpha}$ ($1 = \boldsymbol{X}^{\boldsymbol{0}}$, $\boldsymbol{0} = (0, 0, \ldots, 0)$). Сваки такав поредак назива се МОНОМНИ ПОРЕДАК (мада је заправо дефинисан на производима, а не мономима, али не постоји усаглашеност термина, те се нећемо даље бринути о томе).

Заправо, ево прецизне дефиниције која нам даје све тражене услове.

Дефиниција 129 ЛИНЕАРНО УРЕЂЕЊЕ на скупу свих производа је мономни поредак уколико испуњава следећа два услова.

1. *За све* $\boldsymbol{\alpha} \neq \boldsymbol{0}$ *је* $1 \prec \boldsymbol{X}^{\boldsymbol{\alpha}}$
2. *За све* $\boldsymbol{\alpha}, \boldsymbol{\beta}, \boldsymbol{\gamma}$ *из* $\boldsymbol{X}^{\boldsymbol{\alpha}} \prec \boldsymbol{X}^{\boldsymbol{\beta}}$ *следи* $\boldsymbol{X}^{\boldsymbol{\alpha}}\boldsymbol{X}^{\boldsymbol{\gamma}} \prec \boldsymbol{X}^{\boldsymbol{\beta}}\boldsymbol{X}^{\boldsymbol{\gamma}}$.

Сада показујемо да смо овако заиста добили једно добро уређење на скупу свих производа.

Став 130 Мономни поредак је ДОБРО УРЕЂЕЊЕ на скупу свих производа.

Доказ. Нека је $\preceq$ неки мономни поредак на скупу $\mathbb{P}_n$ и нека је T непразан подскуп од $\mathbb{P}_n$. Желимо да покажемо да T има најмањи елемент. Приметимо пре свега да придруживање $\Phi\colon \mathbb{N}^n \to \mathbb{P}_n$ задато са

$$\Phi(\alpha_1, \ldots, \alpha_n) = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$$

успоставља једну бијекцију између $\mathbb{N}^n$ и $\mathbb{P}_n$ за коју важи

$$(\alpha_1, \ldots, \alpha_n) \ll (\beta_1, \ldots, \beta_n) \iff X_1^{\alpha_1} \cdots X_n^{\alpha_n} \mid X_1^{\beta_1} \cdots X_n^{\beta_n}.$$

Другим речима, парцијално уређени скупови $(\mathbb{N}^n, \ll)$ и $(\mathbb{P}_n, |)$ су изоморфни. Диксонова лема каже да скуп $\Phi^{-1}[T] \subseteq \mathbb{N}^n$ има само коначно много минималних елемената у односу на поредак $\ll$ па стога и $T \subseteq \mathbb{P}_n$ има само коначно много минималних елемената $\mathbf{X}_1, \ldots, \mathbf{X}_k$ у односу на поредак $|$. Но, мономни поредак проширује поредак задат дељивошћу, а уз то је и линеарно уређење. Код сваког линеарног уређења, сваки коначан скуп има и најмањи и највећи елемент. Највећи елемент нас не занима, али најмањи елемент, нека је то $\mathbf{X}_i$, у скупу тих минималних елемената је најмањи елемент у скупу T у односу на мономни поредак $\preceq$. Наиме, ако би у T постојао производ $\mathbf{X}$ такав да је $\mathbf{X} \prec \mathbf{X}_i$

он свакако не би делио ниједан од наведених минималних елемената. Такође, за $1 \leq j \leq k$: $\mathbf{X}_j \nmid \mathbf{X}$, јер би онда било и $\mathbf{X}_j \preceq \mathbf{X}$, што је супротно чињеници да је $\mathbf{X} \prec \mathbf{X}_i \preceq \mathbf{X}_j$ (поредак $\preceq$ проширује $|$). Како постоји само коначно много производа који деле било који производ, постоји коначно много њих из T који деле $\mathbf{X}$. Узмимо минималан такав $\mathbf{X}'$ (то може бити и сам $\mathbf{X}$, нема значаја). Но, он би онда био и минималан у T у односу на $|$, различит од $\mathbf{X}_1, \ldots, \mathbf{X}_k$, а то су сви минимални у T. Ова контрадикција завршава доказ. □

Мономних поредака има уистину много. Наведимо два најједноставнија. Први је *лексикографски* поредак, ознака lex. У том случају је

$$X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n} \prec_{\text{lex}} X_1^{\beta_1} X_2^{\beta_2} \cdots X_n^{\beta_n}$$
$$\stackrel{\text{def}}{\iff} (\exists i \in \{1, \ldots, n\})((\forall j < i)(\alpha_j = \beta_j) \text{ и } \alpha_i < \beta_i).$$

Кратко речено, производи се пореде као у речнику. Замислите да сте исписали производ као реч у речнику (при чему су неодређене слова и то тако да је X_1 прво слово итд.). Онда је „већа" она која се прва појави. Рецимо $X_1^2 X_2 X_3^7 \prec_{\text{lex}} X_1^2 X_2^2 X_3$: $\alpha_1 = 2 = \beta_1$, а $\alpha_2 = 1 < 2 = \beta_2$. Заправо, прва одговара речи (речник је на ћирилици): аабвввввввв, а друга ааббв. Сигурно се ни у једном речнику српског језика ове две речи не појављују, али знамо која би се прва појавила. Посебно, овде је $X_1 \succ_{\text{lex}} X_2 \succ_{\text{lex}} \cdots \succ_{\text{lex}} X_n$. Наиме, $X_2 = X_1^0 X_2^1 \cdots X_n^0$, а $X_1 = X_1^1 X_2^0 \cdots X_n^0$, па је $X_2 \prec_{\text{lex}} X_1$, што се види поређењем степена неодређене X_1. Уосталом, слово а се појављује пре слова б, зар не? Наравно, поређење са речником је натегнуто: наше неодређене комутирају, а слова у речима сигурно не, али ово објашњава терминологију.

Други једноставан поредак, који ћемо користити у даљем је такозвани *степенасти лексикографски* поредак, у ознаци grlex. У овом поретку, ако гледамо аналогију са речником, прво поредите дужину речи (дуже речи су веће од краћих), а речи исте дужине поредите лексикографски: $X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n} \prec_{\text{grlex}} X_1^{\beta_1} X_2^{\beta_2} \cdots X_n^{\beta_n}$ ако и само ако је

$$\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i$$

или је

$$\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i, \text{ а } X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n} \prec_{\text{lex}} X_1^{\beta_1} X_2^{\beta_2} \cdots X_n^{\beta_n}.$$

Јасно је да је и овде $X_i \succ_{\text{grlex}} X_j$ за $i < j$.

Заправо, ми смо и дефинисали оба ова поретка тако да неодређене овако буду уређене. Може се наравно, аналогно, задати лексикографски и степенасти лексикографски поредак да неодређене буду уређене на неки други начин.

Изаберимо неки мономни поредак $\preceq$. Сваки полином $f \neq 0$ из $K[X_1, X_2, \ldots, X_n]$ можемо записати на следећи начин:

$$f = a_1 \boldsymbol{X}^{\boldsymbol{\alpha}_1} + a_2 \boldsymbol{X}^{\boldsymbol{\alpha}_2} + \cdots + a_r \boldsymbol{X}^{\boldsymbol{\alpha}_r},$$

при чему је $\boldsymbol{X}^{\boldsymbol{\alpha}_1} \succ \boldsymbol{X}^{\boldsymbol{\alpha}_2} \succ \cdots \succ \boldsymbol{X}^{\boldsymbol{\alpha}_r}$. Природно је увести следећу терминогију (и ознаке). *Водећи производ* полинома f, у ознаци $LP(f)$, је $\boldsymbol{X}^{\boldsymbol{\alpha}_1}$, *водећи коефицијент* тог полинома, у ознаци $LC(f)$ је a_1, док је $a_1 \boldsymbol{X}^{\boldsymbol{\alpha}_1}$ *водећи моном*: $LM(f) = \alpha_1 \boldsymbol{X}^{\boldsymbol{\alpha}_1}$.

Нека је задат идеал $I = \langle h_1, h_2, \ldots, h_k \rangle$. Занима нас питање припадности полинома $f \neq 0$ овом идеалу. На аналоган начин са полиномима са једном неодређеном можемо увести појам редукције. Уочимо $LP(f)$ и $LP(h_i)$. Ако $LP(h_i) \mid LP(f)$, онда вршимо редукцију:

$$f \xrightarrow{h_i} f_1,$$

где је

$$f_1 = f - \frac{LM(f)}{LM(h_i)} h_i.$$

Приметимо да је сада $LP(f_1) \prec LP(f)$, јер смо водећи моном 'скинули', а све се радило производима који су мањи од $LP(f)$ (користили смо водећи моном и у h_i). Дакле, можемо понављати ове редукције користећи све ове полиноме $h_1, \ldots, h_k$. На крају долазимо до полинома r који даље не можемо да редукујемо. У случају полинома са једном неодређеном, то се дешава када степен добијеног полинома буде мањи од степена полинома h_i, а у случају полинома са више неодређених, то се дешава када ниједан од водећих производа $LP(h_i)$ не дели $LP(r)$. Ако је $r = 0$, онда знамо да је f у идеалу, а ако није, онда...

Гребнерове базе – појам и егзистенција

Настављамо са питањем редукције. Уместо да радимо са датом базом $h_1, \ldots, h_k$, ми желимо да добијемо бољу базу, у којој ће редукција решити проблем припадности идеалу (а и у којој 'остатак' не зависи од редоследа редукција).

Дефиниција 131 Нека је $\{0\} \neq I \lhd K[X_1, \ldots, X_n]$. Полиноми $g_1, \ldots, g_s \in I$ чине ГРЕБНЕРОВУ БАЗУ за идеал I уколико

$$\text{за сваки } g \in I \setminus \{0\} \text{ постоји } i \in \{1, \ldots, s\} \text{ тако да } LP(g_i) \mid LP(g). \qquad (20)$$

Став 132 Гребнерова база постоји за сваки идеал $I \neq 0$ и она је један генераторни скуп за тај идеал.

Доказ. Посматрајмо скуп $\mathcal{LP}(I) = \{LP(g) : g \in I \setminus \{0\}\}$. То је скуп свих водећих производа полинома из I. Према Диксоновој леми, постоји коначно много минималних елемената (у смислу дељивости) у овом скупу, тј. постоји коначно много полинома $g_1, \ldots, g_s \in I$ таквих да је скуп $\{LP(g_1), \ldots, LP(g_s)\}$ скуп свих минималних елемената скупа $\mathcal{LP}(I)$.

Заправо овако добијени елементи $g_1, \ldots, g_s$ и представљају тражену погодну базу – то је Гребнерова база идеала I. Покажимо то.

Докажимо да $g_1, \ldots, g_s$ испуњавају услов из дефиниције **131**. У супротном, нека је g ненула полином из идеала I чији водећи производ није дељив ниједним од водећих производа полинома g_i. Како су они минимални (у односу на дељивост), то, за све i: $LP(g) \nmid LP(g_i)$. Постоји само коначно много ма каквих производа који деле $LP(g)$. Самим тим постоји само коначно много производа из скупа $\mathcal{LP}(I)$ који деле $LP(g)$. Изаберимо неки минималан такав (можда је то баш $LP(g)$, нема везе). Тај производ ће онда бити и минималан у целом скупу $\mathcal{LP}(I)$, а то противречи чињеници да је $\{LP(g_1), \ldots, LP(g_s)\}$ скуп свих минималних елемената (тај производ није ни један од ових – они не деле $LP(g)$).

Дакле, сада имамо полиноме $g_1, \ldots, g_s$ из идеала I са горенаведеним својством (**20**). Покажимо да они генеришу I. Заправо ћемо показати да је $f \in I$ ако и само ако се помоћу g_i може редуковати до 0.

Наравно, један смер је лак. Ако се полином редукује до 0 коришћењем полинома g_i, онда је тај полином облика $\sum_i p_i g_i$ за неке полиноме p_i, па самим тим припада идеалу I (при редукцији од датог полинома f одузимамо неки g_i помножен неким мономом; ако дођемо на крају од нуле, онда, радећи уназад, добијамо да је f сума умножака g_i неким полиномима). Претпоставимо стога да $f \in I$. То значи да је $LP(g_i) \mid LP(f)$ за неко i, па можемо извршити редукцију:

$$f \xrightarrow{g_i} f_1,$$

при чему је $LP(f_1) \prec LP(f)$ и $f_1 \in I$. Уколико је $f_1 = 0$, добили смо тражено; у супротном настављамо поступак. Тако добијамо низ полинома: $f = f_0, f_1, \ldots$ за које је $LP(f_0) \succ LP(f_1) \succ \ldots$ На основу својстава мономног поретка, знамо да такав низ не може бити бесконачан, те се процес мора завршити и добијамо 0 после коначно много корака. □

Ми смо до сада само разматрали редукцију полинома тако што смо 'скидали' његов водећи моном. Но, редукција се може вршити и тако да се 'скида' ма који моном у датом полиному. Када се више ниједан моном не може 'скинути' добијамо прави остатак. Видели смо да се при произвољној бази могу добити различити остаци, чак и у случају

полинома са једном неодређеном. Разјаснимо сада недоумицу — да ли остатак који се добија при редукцији зависи од редоследа којом редукцију вршимо ако имамо Гребнерову базу.

Став 133 Нека је $G = \{g_1, \ldots, g_s\}$ једна Гребнерова база идеала I прстена $K[X_1, \ldots, X_n]$ и нека је $f \neq 0$ произвољан полином из $K[X_1, \ldots, X_n]$. Уколико су полиноми r_1 и r_2 добијени редукцијом полинома f помоћу базе G и не могу се даље редуковати, онда је $r_1 = r_2$.

Доказ. С обзиром на начин на који се врши редукција добијамо да постоје полиноми $p_1, \ldots, p_s$ и полиноми $q_1, \ldots, q_s$ за које је

$$f = p_1 g_1 + \cdots + p_s g_s + r_1, \quad f = q_1 g_1 + \cdots + q_s g_s + r_2.$$

Одавде добијамо да је

$$r_1 - r_2 = (q_1 - p_1)g_1 + \cdots + (q_s - p_s)g_s \in I.$$

Дакле, уколико је $r_1 - r_2 \neq 0$ онда $LP(g_i) \mid LP(r_1 - r_2)$, за неко i (G је Гребнерова база). Наравно, може се десити да су се при одузимању $r_1 - r_2$ водећи мономи у овим полиномима скратили, али, пошто по претпоставци $r_1 - r_2 \neq 0$, ипак је нешто и остало, тј. $LP(r_1 - r_2)$ је неки од производа који се појављују у полиному r_1 и/или полиному r_2. Но, то значи да $LP(g_i)$ дели неки од производа у бар једном од ова два полинома, те бар један од њих није потпуно редукован, што противречи претпоставци. Закључујемо да мора важити $r_1 = r_2$, што се и тражило. □

Видели смо да Гребнерова база увек постоји. Друго је питање како је наћи. Постоје алгоритми за налажење Гребнерове базе конкретног идеала, а они су и имплементирани у разним пакетима за симболичка израчунавања. Ми ћемо се тиме кратко бавити у наредном одељку. Овде ћемо само прокоментарисати да, наравно, Гребнерова база зависи од избора мономног поретка, али је занимљива и следећа једноставна чињеница: ако је $\{g_1, \ldots, g_s\}$ Гребнерова база за поредак $\preceq_1$ и посматрамо поредак $\preceq_2$ и скуп полинома $\{h_1, \ldots, h_s\}$ за које је $LP_{\preceq_1}(g_i) = LP_{\preceq_2}(h_i)$ за све i, онда је скуп $\{h_1, \ldots, h_s\}$ Гребнерова база за поредак $\preceq_2$. Надамо се да је читаоцу потпуно јасно зашто ово важи.

За крај овог одељка, наведимо да се појам Гребнерове базе може задати и за случај полинома над неким прстеном коефицијената. Наравно да је ту сложеније разматрање (на пример, одмах се може приметити да морамо разматрати да ли $LM(g) \mid LM(f)$, а не само да ли $LP(g) \mid LP(f)$), али за правилне прстене, попут главноидеалских домена, теорија се може фино развити.

S-полиноми и Бухбергеров алгоритам

Уведимо најпре једну ознаку. Нека је $F = \{f_1, \ldots, f_s\}$ скуп полинома из $K[X_1, \ldots, X_n]$. Тада

$$f \xrightarrow{F}_+ h$$

означава да је полином f редукован на полином h низом редукција у којима су учествовали полиноми из скупа F.

Посматрајмо идеал $I = \langle f_1, \ldots, f_s \rangle$. Сваки елемент из овог идеала је облика $h_1 f_1 + \cdots + h_s f_s$. Знамо да полиноми $f_1, \ldots, f_s$ чине неку Гребнерову базу за идеал I ако је водећи производ сваког ненула елемента идеала I дељив неким од $LP(f_i)$. На први поглед се може учинити да водећи производи од f_i увек учествују у елементу идеала, али то наравно није случај. Наиме, водећи производи $LP(h_i f_i) = LP(h_i)LP(f_i)$ могу се скратити међусобно. Најједноставнији случај у коме се то дешава је следећи.

Дефиниција 134 Нека су $f, g \in K[X_1, \ldots, X_n] \setminus \{0\}$ и нека је

$$L = \mathrm{NZS}(LP(f), LP(g)).$$

Полином $S(f, g)$ задат са:

$$S(f, g) \colon = \frac{L}{LM(f)} f - \frac{L}{LM(g)} G.$$

назива се S-полином од f и g.

Наравно, $\mathrm{NZS}(P_1, P_2)$ означава најмањи заједнички садржалац производа P_1 и P_2. На пример, ако имамо grlex поредак у коме је $X > Y$ и ако је $f = 3X^3Y + 4Y^2$, а $g = 2XY^2 - 7Y + 6$, онда је $L = \mathrm{NZS}(X^3Y, XY^2) = X^3Y^2$ и

$$S(f, g) = \frac{X^3Y^2}{3X^3Y}(3X^3Y + 4Y^2) - \frac{X^3Y^2}{2XY^2}(2XY^2 - 7Y + 6) = \frac{7}{2}X^2Y + \frac{4}{3}Y^3 - 3X^2.$$

Видимо да је дошло до скраћивања водећих производа и да водећи производ полинома $S(f, g)$ није дељив водећим производима полинома f и g. Како је јасно да $S(f, g) \in \langle f, g \rangle$, то скуп $\{f, g\}$ сигурно не чини Гребнерову базу. Но, занимљиво је да је за проверу да ли неки скуп полинома чини Гребнерову базу довољно посматрати S-полиноме парова полинома из тог скупа кандидата. То је суштина следеће теореме.

Теорема 135 (Бухбергерова теорема) Нека је $G = \{g_1, \ldots, g_s\}$ скуп ненула полинома из $K[X_1, \ldots, X_n]$. Тада је G Гребнерова база за идеал генерисан тим полиномима ако и само ако за све $i \neq j$ важи:

$$S(g_i, g_j) \xrightarrow{G}_+ 0.$$

Ову теорему нећемо доказивати.

Теорема 136 Нека је $F = \{f_1, \ldots, f_s\} \subseteq K[X_1, \ldots, X_n] \setminus \{0\}$. Вршимо следећи поступак са овим полиномима.

Рачунамо $S(f_1, f_2)$ и редукујемо у односу на F до полинома h, који се не може даље редуковати у односу на F. Ако је $h = 0$, разматрамо полиноме f_1 и f_3. А ако је $h \neq 0$, додајемо га у скуп F и настављамо разматрање полинома f_1 и f_3, али сада уз коришћење скупа F проширеног полиномом h. Поступак завршавамо када се сви S-полиноми парова полинома из тако проширеног скупа редукују до 0. Тако проширени скуп је једна Гребнерова база за идеал генерисан скупом полинома F.

Доказ. Овде треба доказати да се овај поступак завршава после коначно много корака, као и да се заиста добија Гребнерова база за идеал генерисан полиномима $f_1, \ldots, f_s$. Корисно је, за скуп полинома F увести ознаку

$$LP(F) := \langle LP(f) : f \in F \setminus \{0\} \rangle.$$

Дакле, то је идеал генерисан водећим производима полинома из F.

Уколико се поступак не би завршио, добили бисмо растући низ скупова полинома

$$F = G_0 \subset G_1 \subset G_2 \subset \cdots$$

при чему се сваки од G_i добија од претходног додавањем неког елемента $h \in I$ који је ненула редукција у односу на G_{i-1} неког S-полинома два елемента из G_{i-1}. Како је h редукован у односу на G_{i-1}, то $LP(h) \notin LP(G_{i-1})$, па је низ идеала

$$LP(G_0) \subset LP(G_1) \subset LP(G_2) \subset \cdots$$

стриктно растући низ идеала који се не завршава, а ово није могуће јер је прстен полинома $K[X_1, \ldots, X_n]$ Нетерин. Закључујемо да се поступак мора завршити.

Дакле, поступак се завршава и добијамо нови скуп полинома, зовимо га G: $G = \{f_1, \ldots, f_s, h_1, \ldots, h_t\}$. Нека је $g_i := f_i$ за $1 \leqslant i \leqslant s$ и $g_{s+j} := h_j$ за $1 \leqslant j \leqslant t$. С обзиром да важи да је $S(g_i, g_j) \xrightarrow{G}_+ 0$ за све $i \neq j$, Бухбергерова теорема нам каже да смо заиста добили једну Гребнерову базу. □

Поступак описан у претходној теореми зове се Бухбергеров алгоритам. Као што видимо, то је један доста једноставан поступак базиран на Бухбергеровој теореми. Знамо да се сви S-полиноми за парове полинома из Гребнерове базе морају редуковати до нуле. Стога рачунамо те полиноме. Сваки пут кад не добијемо нулу, тај редуковани полином додајемо у базу. На крају заиста и добијамо једну Гребнерову базу.

Редуковане Гребнерове базе

Дакле, имамо један поступак (Бухбергеров алгоритам) који нам омогућава налажење неке Гребнерове базе почев од датог скупа генератора идеала. Јасно је да су при конструкцији базе вршени многи избори што се тиче редоследа редукције, а од њих зависи и коначан исход. Да бисмо можда дошли до неке јединствености, наведимо најпре следећу дефиницију.

Дефиниција 137 За Гребнерову базу $G = \{g_1, \ldots, g_s\}$ кажемо да је минимална уколико важи следеће:

1) $LC(g_i) = 1$, за све i.

2) За све $i \neq j$: $LP(g_i) \nmid LP(g_j)$.

Није тешко видети како се од ма које Гребнерове базе добија минимална. Пре свега, први услов је лако испунити — довољно је поделити сваки члан базе његовим водећим коефицијентом. Што се тиче другог услова, ако је G нека Гребнерова база и $g_1, g_2 \in G$, уколико $LP(g_2) \mid LP(g_1)$, онда је и $G \setminus \{g_1\}$ Гребнерова база — сваки производ дељив са $LP(g_1)$ дељив је и са $LP(g_2)$, те нам полином g_1 и није неопходан за ту базу.

Став 138 Нека су $F = \{f_1, \ldots, f_s\}$ и $G = \{g_1, \ldots, g_t\}$ две минималне Гребнерове базе неког идеала. Тада је $s = t$ и

$$\{LP(f_1), \ldots, LP(f_s)\} = \{LP(g_1), \ldots, LP(g_s)\}.$$

Доказ. Означимо са I идеал о коме је реч. Како $f_1 \in I$, а G је Гребнерова база, $LP(g_{i_1}) \mid LP(f_1)$ за неко i_1. Слично, како $g_{i_1} \in I$, а F је Гребнерова база, онда $LP(f_j) \mid LP(g_{i_1})$ за неко j. Следи да $LP(f_j) \mid LP(f_1)$. Но, како је база F минимална, мора бити $j = 1$. Дакле, $LP(f_1) \mid LP(g_{i_1})$ и $LP(g_{i_1}) \mid LP(f_1)$. С обзиром да су водећи коефицијенти једнаки 1, добијамо да је $LP(f_1) = LP(g_{i_1})$.

Посматрајмо скупове $F \setminus \{f_1\}$ и $G = \setminus\{g_{i_1}\}$. Елемент f_2 је у I, а како је G Гребнерова база, $LP(g_{i_2}) \mid LP(f_2)$ за неко i_2. С обзиром да је $LP(g_{i_1}) = LP(f_1)$, а $LP(f_1) \nmid LP(f_2)$, мора бити $i_2 \neq i_1$. Као и у претходном случају, $LP(f_j) \mid LP(g_{i_2})$ за неко j и то j мора бити баш једнако 2. И овде добијамо да је $LP(f_2) = LP(g_{i_2})$.

Поступак се наставља и добијамо да је за све $1 \leqslant k \leqslant s$: $LP(f_k) = LP(g_{i_k})$ при чему је $g_{i_k} \neq g_{i_l}$ кад год је $k \neq l$. То показује да је $s \leqslant t$. Како смо могли да кренемо симетрично, од g_1, важи и да је $t \leqslant s$. Стога је $s = t$ и $\{LP(f_1), \ldots, LP(f_s)\} = \{LP(g_1), \ldots, LP(g_s)\}$, што се и тражило. □

Дефиниција 139 За Гребнерову базу $G = \{g_1, \ldots, g_s\}$ кажемо да је редукована уколико је $LC(g_i) = 1$ за све i и уколико је, за све i, елемент g_i редукован у односу на $G \setminus \{g_i\}$, тј. ниједан моном у g_i није дељив неким од $LP(g_j)$ за неко $j \neq i$.

Теорема 140 Нека је изабран неки мономни поредак на скупу $\mathbb{P}_n$. Сваки ненула идеал $I \lhd K[X_1, \ldots, X_n]$ има јединствену редуковану Гребнерову базу у односу на изабрани мономни поредак.

Доказ. Није тешко уверити се како се од ма које Гребнерове базе налази редукована. Најпре се сви чланови базе редукују у односу на остале, а затим се они чланови базе који су остали, поделе својим водећим коефицијентима.

Остаје питање јединствености. С обзиром да је свака редукована база уједно и минимална, сваке две редуковане базе имају исти број елемената. Нека су $G = \{g_1, \ldots, g_t\}$ и $H = \{h_1, \ldots, h_t\}$ две редуковане Гребнерове базе за дати идеал. Можемо претпоставити и да је $LP(g_i) = LP(h_i)$ за све i (видети претходни став).

Уколико би било $g_k \neq h_k$ за неко k, имали бисмо ненула елемент идеала I: $g_k - h_k$, те $LP(h_j) \mid LP(g_k - h_k)$. Како је $LP(g_k - h_k) \prec LP(h_k)$, јер су се водећи мономи скратили, то је $j \neq k$. Но, то значи да $LP(h_j) = LP(g_j)$ дели неки од монома у $g_k - h_k$. Но, ма који моном у том полиному је умножак неког од монома из g_k и/или h_k. Но, то би значило да база G или база H није редукована, што противречи претпоставци. □

Елементарне примене Гребнерових база

У овом делу ћемо навести неколико једноставних примена Гребнерових база. У свим применама $I = \langle f_1, \ldots, f_s \rangle \lhd K[X_1, \ldots, X_n]$.

Прва примена. Нека је $f \in K[X_1, \ldots, X_n]$. Одредити да ли $f \in I$.

Овде је јасно шта радимо. Најпре нађемо Гребнерову базу $G = \{g_1, \ldots, g_t\}$ за идеал I и онда имамо еквиваленцију:

$$f \in I \iff f \xrightarrow{G}_+ 0. \qquad \diamondsuit$$

Друга примена. Дата су два идеала I и J у прстену полинона. Одредити да ли су једнаки.

И ово није тешко. Пошто је редукована Гребнерова база за идеал једнозначно одређена, треба одредити редуковане базе за I и J и упоредити их. $\diamondsuit$

Трећа примена. Наћи представнике за косете у $K[X_1,\ldots,X_n]/_I$.

Нека је G Гребнерова база за I. За сваки $f \in K[X_1,\ldots,X_n]$ постоји тачно један елемент $r \in K[X_1,\ldots,X_n]$, који је редукован у односу на G, такав да је $f \xrightarrow{G}_+ r$. Он се означава са $N_G(f)$ и назива НОРМАЛНА ФОРМА ОД f У ОДНОСУ НА G. Важи следећи став.

Став 141 Нека су $f, g \in K[X_1,\ldots,X_n]$, $I \lhd K[X_1,\ldots,X_n]$. Тада је $f + I = g + I$ **акко** $N_G(f) = N_G(g)$. Стога је

$$\{N_G(f) : f \in K[X_1,\ldots,X_n]\}$$

тражени скуп представника косета за $K[X_1,\ldots,X_n]/_I$. Штавише, пресликавање $N_G \colon K[X_1,\ldots,X_n] \to K[X_1,\ldots,X_n]$ је K-линеарно.

Доказ става није тежак, али га нећемо давати.

Четврта примена. Одредити базу K-векторског простора $K[X_1,\ldots,X_n]/_I$.

Ово нам разрешава следећи став.

Став 142 Нека је $G = \{g_1,\ldots,g_t\}$ Гребнерова база за идеал I. Базу за K-векторски простор $K[X_1,\ldots,X_n]/_I$ чине они производи $\mathbf{X}$ који нису дељиви водећим производима полинома из G.

Доказ. Као што смо навели, за сваки полином f је $f + I = N_G(f) + I$. Како је $N_G(f)$ редукован у односу на G, он је сума монома који се не могу даље редуковати, тј. који нису дељиви са $LP(g_i)$ за све i. Косети одговарајућих производа су линеарно независни над K, баш због јединствености нормалне форме. □

Пример 143 Претпоставимо да смо за неки идеал I прстена $\mathbb{Q}[X,Y]$ добили Гребнерову базу $G = \{XY^2 - X + Y, -X^2 + XY + Y^2, Y^3 + X - 2Y\}$ при чему имамо *grlex* поредак у коме је $X \succ_{grlex} Y$. Водећи производи су овде XY^2, X^2, Y^3. Стога базу чине косети производа који нису дељиви овим, а то су $1, X, Y, XY, Y^2$, те је $\dim \mathbb{Q}[X,Y]/_I = 5$. Да истакнемо, базу чине: $1 + I, X + I, Y + I, XY + I, Y^2 + I$. ♣

Пета примена. Одредити операције у количничком прстену.

Представници косета су $N_G(f)$. Оно што је занимљиво је множење. Представник производа косета $(f + I) \cdot (g + I)$ је $N_G(f \cdot g)$. ♢

Пример 144 Направићемо таблицу множења елемената базе векторског простора из претходног примера. Сваки производ ће бити изражен као линеарна комбинација елемената базе. На пример, производ $(XY + I) \cdot (Y^2 + I) = XY^3 + I$ добијамо редукцијом полинома XY^3 помоћу базе G.

$$\begin{aligned} XY^3 &\xrightarrow{g_3} XY^3 - Xg_3 = XY^3 - X(Y^3 + X - 2Y) = -X^2 + 2XY \\ &\xrightarrow{g_2} -X^2 + 2XY - g_2 = -X^2 + 2XY + X^2 - XY - Y^2 = XY - Y^2. \end{aligned}$$

Дакле, ако косет $f+I$ означимо са $\overline{f}$ имамо да је $\overline{XY}\cdot\overline{Y^2}=\overline{XY}-\overline{Y^2}$. Ево целе таблице.

$\cdot$	$\overline{1}$	$\overline{X}$	$\overline{Y}$	$\overline{Y^2}$	$\overline{XY}$
$\overline{1}$	$\overline{1}$	$\overline{X}$	$\overline{Y}$	$\overline{Y^2}$	$\overline{XY}$
$\overline{X}$	$\overline{X}$	$\overline{XY}+\overline{Y^2}$	$\overline{XY}$	$\overline{X}-\overline{Y}$	$\overline{Y}$
$\overline{Y}$	$\overline{Y}$	$\overline{XY}$	$\overline{Y^2}$	$-\overline{X}+2\overline{Y}$	$\overline{X}-\overline{Y}$
$\overline{Y^2}$	$\overline{Y^2}$	$\overline{X}-\overline{Y}$	$-\overline{X}+2\overline{Y}$	$-\overline{XY}+2\overline{Y^2}$	$\overline{XY}-\overline{Y^2}$
$\overline{XY}$	$\overline{XY}$	$\overline{Y}$	$\overline{X}-\overline{Y}$	$\overline{XY}-\overline{Y^2}$	$\overline{Y^2}$

Ову таблицу ћемо искористити у наредном примеру. ♣

Шеста примена. Одредити инверзе елемената у количничком прстену ако постоје.

Уколико је количнички прстен K-векторски простор коначне димензије, онда се ово решава методом неодређених елемената. Ако базу чине косети производа $\mathbf{X}_1,\dots,\mathbf{X}_n$ и тражимо инверз елемента $f+I$, онда тражимо $a_1,\dots,a_n\in K$ тако да је

$$(a_1\mathbf{X}_1+\cdots+a_n\mathbf{X}_n)\cdot f\equiv 1 \pmod I.$$

Уколико наведени елемент нема инверз, систем једначина који добијемо нема решење. ♢

Пример 145 Искористимо пример **143**. Потражимо ту инверз косета $(X+Y+1)+I$. С обзиром да знамо базу, треба одредити $a,b,c,d,e\in\mathbb{Q}$ такве да је

$$(aXY+bY^2+cX+dY+e)(X+Y+1)\equiv 1 \pmod I.$$

Рачунамо

$$\begin{aligned}(aXY+bY^2+cX+dY+e)(X+Y+1) &= aX^2Y+aXY^2+aXY+bXY^2+bY^3+bY^2\\ &+cX^2+cXY+cX+dXY+dY^2+dY+eX+eY+e \equiv_I aY+a(X-Y)+aXY+b(X-Y)\\ &+b(2Y-X)+bY^2+c(XY+Y^2)+cXY+cX+dXY+dY^2+dY+eX+eY+e\\ &= (a+2c+d)XY+(b+c+d)Y^2+(a+c+e)X+(b+d+e)Y+e.\end{aligned}$$

Овде смо код множења монома користили редукције које су наведене у таблици множења из претходног примера. Добијамо систем једначина

$$\begin{array}{rcrcrcrcl} a & & + & 2c & + & d & & = & 0\\ & b & + & c & + & d & & = & 0\\ a & & + & c & & & + \quad e & = & 0\\ & b & & & + & d & + \quad e & = & 0\\ & & & & & & e & = & 1 \end{array}$$

Решење система је $(a,b,c,d,e)=(-2,-1,1,0,1)$. Дакле, инверз косета $X+Y+I$ је косет $(-2XY-Y^2+X+1)+I$. ♣