Предавања из Алгебре 2 за школску 2025/26. годину

Зоран Петровић

Прстен полинома – појам и конструкција

У курсу Алгебре 1 бавили смо се и прстеном полинома са једном неодређеном над комутативним прстеном са јединицом A, тј. прстеном $A[X]$. Тада је било наведено да је то скуп свих формалних израза облика $a_0 + a_1X + \cdots + a_nX^n$, 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.

Наведимо најпре дефиницију прстена полинома.

Дефиниција 1. 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 неко $n \geq 0$ и неке $a'_i \in A'$.

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

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

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

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

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

док је множење нешто сложеније:

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

где је за све $k\geq 0$:

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

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:

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

Најсложенија је провера асоцијативности множења:

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

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 $K[X_1, \ldots, X_n]$ за ма које $n \geq 1$.

Еуклидско дељење

Уколико је $0 \neq a(X) = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$ и $a_n \neq 0$, тада кажемо да је полином $a(X)$ степена n и то пишемо овако $\deg(a(X)) = n$. Како је производ ненула елемената у пољу такође ненула елемент, ако су полиноми $a(X)$ и $b(X)$ различити од 0, онда је $\deg(a(X) \cdot b(X)) = \deg(a(X)) + \deg(b(X))$. Но, погодно је имати ову једнакост чак и ако је један од полинома једнак 0. Стога уводимо да је $\deg(0) \colon = -\infty$, 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 2. Нека је K поље, $a(X) \in K[X]$, $b(X) \in K[X] \setminus \{0\}$. Тада постоје и јединствено су одређени полиноми $q(X), r(X) \in K[X]$ за које важи

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

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

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

Претпоставимо да $n = \deg(a(X)) \geq \deg(b(X))$ и да је тврђење тачно за све полиноме степена мањег од n. Тада је $a(X) = a_n X^n + \cdots + a_1 X + a_0$,

а $b(X) = b_m X^m + \cdots + b_1 X + b_0$, при чему је $n \geq m$. Знамо како се дељење изводи: пореде се $a_n X^n$ и $b_m X^m$ и први члан у количнику је заправо $\frac{a_n}{b_m} X^{n-m}$. Хајде да уведемо ознаке које ће нам користити и касније. Водећи моном у полиному $a(X)$ је $a_n X^n$ и то записујемо овако: $LM(a(X)) = a_n X^n$, или још краће: $LM(a) = a_n X^n$. Водећи коефицијент је a_n и то записујемо овако: $LC(a) = a_n$. Слично је $LM(b) = b_m X^m$ 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 3. Нека је K поље и $a(X) \in K[X] \setminus \{0\}$. Тада у K полином $a(X)$ има највише $\deg(a(X))$ нула.

Доказ. Најједноставније је ово доказати индукцијом по степену полинома. За базу индукције је довољно констатовати да ненула полином степена 0, дакле константа различита од нуле, нема 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 4. Нека је $a(X) = X^2 + 5X + 6 \in \mathbb{Z}_{10}[X]$. Овај полином, који је степена 2 има бар три нуле: $a(2) = 4 + 10 + 6 = 0$, $a(3) = 9 + 15 + 6 = 0$, $a(7) = 49 + 35 + 6 = 0$.

Напомена 5. 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 6. 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 $b(X)$. Осим тога, из дефиниције није баш јасно да највећи заједнички делилац увек постоји.

Следећа лема је једноставна и корисна.

Лема 7. Ако је $a_1(X) = q(X)a_2(X) + a_3(X)$, онда полиноми $a_1(X)$ и $a_2(X)$ имају највећи заједнички делилац ако и само ако полиноми $a_2(X)$ и $a_3(X)$ имају највећи заједнички делилац и важи једнакост $\mathrm{NZD}(a_1(X), a_2(X)) = \mathrm{NZD}(a_2(X), a_3(X))$.

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 $a_3(X)$. 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.

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

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

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

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

Теорема 8. 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 9. 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 $\langle X, Y\rangle \lhd K[X, Y]$ 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 10. 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 (**1**) 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. □

Количнички прстени (из Алгебре 1)

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

Дефиниција 11. 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 $a \equiv b \pmod{I}$. То значи да $a - b \in I$, но, множењем са (-1) добијамо да $b - a = (-1)(a - b)$ припада I, па је $b \equiv a \pmod{I}$.

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

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

те је $a \equiv c \pmod{I}$.

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

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

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

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

Приметимо да је класа еквиваленције елемента a заправо скуп

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

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

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

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

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

Теорема 12. (Основна теорема о изоморфизму 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 13. Нека је $I \triangleleft A$. Тада је $p\colon A \to A/_I$ један епиморфизам. ♣

Пример 14. 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. ♣

Директан производ прстена; Кинеска теорема о остацима

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

Дефиниција 15. Нека су $(A_1, +^1, \cdot^1), \ldots, (A_n, +^n, \cdot^n)$ комутативни прстени са јединицом. На Декартовом производу

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

задајемо структуру комутативног прстена са јединицом са:

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

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

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

Искористимо конструкцију директног производа за добијање неких нових занимљивих примера.

Пример 16. Посматрајмо полином $f(X) = X^2 + (5,5)X + (6,6) \in (\mathbb{Z}\times\mathbb{Z})[X]$. Он има следеће четири нуле: $(-2,-2), (-2,-3), (-3,-2), (-3,-3)$ што се може лако проверити. На пример:

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

Пример 17. Додатном модификацијом претходног примера можемо добити полином степена 2 који има бесконачно много нула. Посматрајмо полином: $g(X) = (1,0)X^2 + (5,0)X + (6,0) \in (\mathbb{Z}\times\mathbb{Z})[X]$. Лако је проверити да је сваки елемент облика $(-2,m) \in \mathbb{Z}\times\mathbb{Z}$ нула овог полинома:

$$(1,0)(-2,m)^2 + (5,0)(-2,m) + (6,0)$$
$$= (1,0)(4,m^2) + (-10,0) + (6,0) = (4,0) + (-10,0) + (6,0) = (0,0). \quad ♣$$

Овај став и његову последицу смо имали у Алгебри 1.

Став 18. Нека су $m_1, \ldots, m_n$ позитивни цели бројеви за које је: $\mathrm{NZD}(m_i, m_j) = 1$ за све $i \neq j$. Тада је

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

Последица 19. (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

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

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

Дефиниција 20. 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 21. За копросте идеале I и J важи следећа једнакост: $I \cdot J = I \cap J$.

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

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

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

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

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

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

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

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

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

Теорема 23. (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 прстена 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 **22** 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 $x=b_1x_1+\cdots+b_nx_n$, где су b_i претходно изабрани елементи. Тада је, за све i:

$$x=b_1x_1+\cdots+b_ix_i+\cdots+b_nx_n\equiv 0\cdot x_1+\cdots+1\cdot x_i+\cdots+0\cdot x_n \pmod{I_i}.$$

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". □

Како 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 24. Нека је A комутативан прстен са јединицом и $P\lhd A$ $(P\neq A)$. Следећи услови су еквивалентни.

1. За $I,J\lhd A$ 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. $x=0_{A/_P}$, или $y=0_{A/_P}$.

$3\Longrightarrow 1$. 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 25. Идеал $P \triangleleft A$ је прост уколико испуњава неко од претходна три еквивалентна својства.

Пример 26. Идеал $\langle 2, 1-\sqrt{-5}\rangle \triangleleft \mathbb{Z}[\sqrt{-5}]$ је прост идеал.

Покажимо да је $\mathbb{Z}[\sqrt{-5}]/\langle 2, 1-\sqrt{-5}\rangle \cong \mathbb{Z}_2$. 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

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

Дефинишимо пресликавање $f\colon \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}_2$ са:

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

Покажимо да је ово пресликавање хомоморфизам прстена.

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

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

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

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

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

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

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

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

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

Приметимо да, уколико је P прост идеал, а $a_1, \ldots, a_n \in A$, 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).

Пређимо сада на појам максималног идеала.

Дефиниција 27. 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 28. 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. $1 = ab - m$. 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. □

Напомена 29. Видимо да из овог става следи да је сваки максималан идеал уједно и прост идеал, пошто у пољу не постоје прави делитељи нуле. ♢

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 30. 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 31. 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 32. У прстену $\mathbb{Z}\left[\sqrt{-5}\right]$ елемент 3 је нерастављив, али није прост.

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 случај 2) и не појављује.

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

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

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

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

Следећи став је помало и очекиван.

Став 34. 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 $p \mid b$. □

Напомена 35. Као што смо доказали да 3 није прост, можемо доказати да ни 2 није прост. Стога идеал $\langle 2\rangle$ није прост. Но, важи једнакост

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

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

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

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

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

Став 36. 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 37. 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 38. У комутативном прстену са јединицом A постоји тачно један максималан идеал ако и само ако је $A \setminus U(A)$ идеал.

Доказ. Приметимо да важи следеће. Идеал $I \lhd A$ је прави акко I не садржи ниједан инвертибилан елемент. Наиме, ако је $u \in I$ инвертибилан елемент, и $a \in A$ произвољан елемент, онда се у I налази и $au^{-1} \cdot u = a$, па је тада $I = A$.

Претпоставимо да у прстену постоји тачно један максималан идеал M. Према претходном је $U(A) \subseteq A \setminus M$. Но, ако постоји $a \in A \setminus M$ који није инвертибилан, онда је идеал $\langle a\rangle$ прави, па је према теореми **37** $\langle a\rangle$ садржан у неком максималном, а како је M једини такав, то је $\langle a\rangle \subseteq M$, што није могуће, јер $a \notin M$.

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

Дефиниција 39. Комутативан прстен са јединицом у коме постоји тачно један максимални идеал назива се ЛОКАЛНИ ПРСТЕН.

Пример 40. 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 41. 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 $\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$. ♣

Нетерини прстени

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

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

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

Став 42. 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 $n \geqslant m$.

(3) Сваки непразан скуп идеала у A има максималан елемент.

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) $\implies$ (3). Нека је $\mathcal{I}$ непразан скуп идеала прстена A. Претпоставимо да он нема максималан елемент. Нека је $I_0 \in \mathcal{I}$ ма који идеал из $\mathcal{I}$. Како у $\mathcal{I}$ не постоји максималан елемент, то у $\mathcal{I}$ постоји I_1 за који је $I_0 \subset I_1$ ($\subset$ означава прави подскуп). Како ни I_1 није максималан, то постоји $I_2 \in \mathcal{I}$ за који је $I_1 \subset I_2$, па имамо да је $I_0 \subset I_1 \subset I_2$. Ни, I_2 није максималан, па постоји $I_3 \in \mathcal{I}$ за који је $I_2 \subset I_3$. Настављајући поступак добијамо бесконачан строго растући низ идеала $I_0 \subset I_1 \subset I_2 \subset \cdots$, а по (2) то није могуће. Ова контрадикција нам показује да у $\mathcal{I}$ мора постојати максималан елемент.

(3) $\implies$ (1): Претпоставимо да постоји идеал $I \triangleleft A$, који није коначно генерисан. Нека је $\mathcal{I} = \{J \triangleleft A : J \subseteq I, J \text{ јесте коначно генерисан}\}$. На основу (3), у $\mathcal{I}$ постоји максималан елемент $J_{\max}$. Имамо да је $J_{\max} \neq I$, јер I није коначно генерисан, а $J_{\max}$. Стога постоји $x \in I \setminus J_{\max}$. Тада је $J_{\max} \subset J_{\max} + \langle x \rangle \subseteq I$ и $J_{\max} + \langle x \rangle$ јесте коначно генерисан. Стога је он садржан у $\mathcal{I}$, али је истовремено и прави надскуп максималног елемента $J_{\max}$ у $\mathcal{I}$, а то, наравно, није могуће. Стога је сваки идеал у A коначно генерисан. □

Дефиниција 43. За комутативан прстен A кажемо да је Нетерин ако испуњава било који од ова три еквивалентна услова.

Пример 44. 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. ♣

Пример 45. Нека је $A = \mathbb{Z} + X\mathbb{Q}[X]$ потпрстен прстена $\mathbb{Q}[X]$, који се састоји од полинома са рационалним коефицијентима, код којих је слободан члан цео број. Овај прстен није Нетерин, јер имамо бесконачан строго растући низ идеала: $\langle X/2\rangle \subset \langle X/4\rangle \subset \langle X/8\rangle \subset \cdots$. Наиме, ако бисмо имали да $\frac{X}{2^{n+1}} \in \langle \frac{X}{2^n}\rangle$ добили бисмо да је $\frac{X}{2^{n+1}} = p(X) \cdot \frac{X}{2^n}$ за неки $p(X) \in A$, но то би значило да је $\frac{1}{2} = p(X) \in A$, што није тачно. ♣

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 46. (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:

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

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 47. 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 48. 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. □

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.

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

Дефиниција 49. 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 50. 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 $P \lhd A$.

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 и $t \neq 0$, 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 51. 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 $S = A \setminus P$ за неки прост идеал P, онда се уместо $(A \setminus P)^{-1}A$ краће пише: A_P. Важи следећа теорема.

Теорема 52. За сваки прост идеал $P \triangleleft A$, прстен A_P је локални прстен.

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

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

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.

Претходни део је за први колоквијум.

Раширења поља

Уколико је поље F садржано у пољу E, онда кажемо да је поље E РАШИРЕЊЕ поља F. Следећа важна теорема, која је доказана у оквиру предмета Алгебра 1, описује Кронекерову конструкцију којим се дато поље проширује до новог поља додавањем нула нерастављивог полинома. Пре даљег читања, препорука је да читаоци понове градиво из Линеарне алгебре – појам векторског простора, линеарне независности вектора, базе и димензије векторског простора, као и одговарајући доказ из Алгебре 1.

Теорема 53. 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 $a(X)$.

Напомена 54. Приметимо да је, као векторски простор над пољем F, поље E из претходне теореме изоморфно са F^n: $E \cong F^n$. Но, директан производ поља никада није поље, јер ту увек имамо делитеље нуле: $(1,0)\cdot(0,1) = (0,0)$. Ради се о томе што овде на F^n операцију сабирања заиста дефинишемо по координатама, али је операција множења задата на другачији начин – ту користимо полином $a(X)$. Наиме, да бисмо нашли производ n-торки $(\alpha_0,\alpha_1,\ldots,\alpha_{n-1})\cdot(\beta_0,\beta_1,\ldots,\beta_{n-1})$ из F^n, ми налазимо остатак при дељењу полинома $(\alpha_0+\alpha_1X+\cdots+\alpha_{n-1}X^{n-1})\cdot(\beta_0+\beta_1X+\cdots\beta_{n-1}X^{n-1})$ полиноном $a(X)$ и ако је тај остатак полином $\gamma_0+\gamma_1X+\cdots+\cdots\gamma_{n-1}X^{n-1}$, тада је

$$(\alpha_0,\alpha_1,\ldots,\alpha_{n-1})\cdot(\beta_0,\beta_1,\ldots,\beta_{n-1}) = (\gamma_0,\gamma_1,\ldots,\gamma_{n-1}). \qquad \diamondsuit$$

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 55. Конструисати поље, које има тачно 4 елемента.

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

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

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

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

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

$+$	0	1	η	$1+\eta$
0	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

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

$$(\alpha_0, \alpha_1) + (\beta_0, \beta_1) = (\alpha_0 + \beta_0, \alpha_1 + \beta_1)$$
$$(\alpha_0, \alpha_1) \cdot (\beta_0, \beta_1) = (\alpha_0\beta_0 + \alpha_1\beta_1, \alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_1\beta_1),$$

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

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

Последица 56. 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. □

Минимално поље K_f у коме се дати полином f из $F[X]$ факторише на линеарне факторе назива се КОРЕНСКО ПОЉЕ полинома f.

Веома је занимљив следећи резултат.

Теорема 57. (Теорема о примитивном елементу) Свако коначно раширење E поља F, где је $F = \mathbb{Q}$ или је F коначно поље, је облика $F(\alpha)$, за неко $\alpha \in E$.

Елемент α је тај примитивни елемент раширења E.

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

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

Вишеструке нуле полинома

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

Дефиниција 58. Полином $f \in F[X]$ има двоструку нулу $\alpha \in F$ уколико $(X - \alpha)^2 \mid f(X)$. На аналогни начин се дефинише и појам n-тоструке нуле за ма које $n \geq 2$.

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

Дефиниција 59. 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 60. 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 61. Нека је $f(X) \in F[X]$. Тада f има вишеструку нулу у неком проширењу E поља F ако и само ако 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 62. Нека је $f(X) \in F[X]$ нерастављив полином. Тада он има вишеструку нулу у неком раширењу E поља F ако и само ако је $f'(X) = 0$.

Доказ. На основу претходног става $f(X)$ има вишеструку нулу у неком раширењу ако и само ако је $\mathrm{NZD}(f(X), f'(X)) \neq 1$. 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 63. 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 $\mathbb{Z}_3(t)$. Претпоставимо да је $\frac{f(t)}{g(t)} \in \mathbb{Z}_3(t)$ (при чему претпостављамо да је $\mathrm{NZD}(f(t), g(t)) = 1$) нула полинома $a(X)$. Добијамо да је $f(t)^3 = tg(t)^3$ у $\mathbb{Z}_3[t]$. Тада је $f(0)^3 = 0$, па је наравно и $f(0) = 0$, те је $f(t) = tf_1(t)$ за неки полином $f_1(t) \in \mathbb{Z}_3[t]$. Стога је $t^3 f_1(t)^3 = tg(t)^3$, те је $t^2 f_1(t)^3 = g(t)^3$, па је $g(0)^3 = 0$, те је и $g(0) = 0$ и добијамо да је $g(t) = tg_1(t)$ за неки полином $g_1(t) \in \mathbb{Z}_3[t]$. Но, то значи да t дели и $f(t)$ и $g(t)$ за које смо претпоставили да су узајамно прости. Ова контрадикција нам показује нерастављивост полинома $a(X)$.

Дакле, $a(X)$ је нерастављив полином. Но, приметимо да је $a'(X) = 3X^2 = 0$, па има вишеструку нулу у неком раширењу поља F. Он свакако има раширење у коме има неку нулу α (то раширење можемо добити као $F[X]/\langle a(X)\rangle$). То значи да је $\alpha^3 - t = 0$ у $E[X]$. Но, тада је заправо

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

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

Коначна поља

Докажимо најпре следећу једноставну чињеницу.

Став 64. 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 $n \geqslant 1$ 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 поље са p^n елемената. Знамо свакако да нека таква постоје.

Став 65. 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 66. 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 на то да је $a'(X) = -1$, полином $a(X)$ нема вишеструких нула нигде, те он у F има факторизацију у производ различитих линеарних фактора.

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

- Нека $\alpha, \beta \in L$. Тада је $(\alpha \cdot \beta)^q = \alpha^q \cdot \beta^q = \alpha \cdot \beta$, па закључујемо да $\alpha \cdot \beta \in L$.
- Нека је $\alpha \in L \setminus \{0\}$. Тада, дељењем једнакости $\alpha^q = \alpha$ са α^{q+1} добијамо да је $\alpha^{-1} = \alpha^{-q} = (\alpha^{-1})^q$, те $\alpha^{-1} \in L$.
- Нека $\alpha, \beta \in L$. Како F садржи као своје потпоље поље $\mathbb{F}_p$, то је карактеристика поља F једнака p, те је $p\gamma = 0$ за све $\gamma \in F$.

Подсетимо се још и чињенице да је $p \mid \binom{p}{k}$ за све $1 \leqslant k \leqslant p-1$ 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 67. 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. Поље K је коначно раширење поља $\mathbb{F}_p$. Нека је α примитивни елемент тог раширења, тј. нека је $K = \mathbb{F}_p(\alpha)$.

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

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

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 испитајмо када је неко коначно поље потпоље другог коначног поља.

Став 68. 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 $m \mid n$. То коначно поље са q елемената означимо са $\mathbb{F}_q$. Посматрајмо, као у доказу теореме **66**, 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 **66** 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 $0 \leqslant r < m$, ово је могуће само ако је $r = 0$, тј. ако $m \mid n$ што се и тражило. $\square$

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

Прстен полинома са више неодређених

Сада почињемо део курса у коме ћемо се више позабавити полиномима са више неодређених са коефицијентима у пољу. 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.

Диксонова лема

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

Став 69. (Диксонова лема) Нека је $n \geqslant 1$. На скупу $\mathbb{N}^n$ дефинишемо уређење $\ll$ са:

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

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, $(a_1, \ldots, a_n) \in S \setminus S_0$ 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 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 $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$ и $h_1(X) = b_mX^m + b_{m-1}X^{m-1} + \cdots + b_1X + b_0$. Уколико је $n < m$ ништа не можемо да урадимо, зато посматрајмо случај $n \geqslant m$. Шта радимо? Посматрамо *искључиво* мономе a_nX^n и b_mX^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 $f_1(X) = f(X) - \frac{a_nX^n}{b_mX^m}h_1(X)$. 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, најпре, 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 $\boldsymbol{X^\alpha}$ (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 $\boldsymbol{X^\alpha} \mid \boldsymbol{X^\beta}$ следи $\boldsymbol{X^\alpha} \preccurlyeq \boldsymbol{X^\beta}$. Такође желимо да тако добијемо ДОБРО УРЕЂЕН скуп свих производа, јер не желимо бесконачан опадајући низ: $\boldsymbol{X^{\alpha_1}} \succ \boldsymbol{X^{\alpha_2}} \succ \ldots$. Посебно, то значи да имамо једно ЛИНЕАРНО УРЕЂЕЊЕ, тј. свака два производа морају бити упоредива. Приметимо да је и $1 \preccurlyeq \boldsymbol{X^\alpha}$ за свако $\boldsymbol{\alpha}$ ($1 = \boldsymbol{X^0}$, $\boldsymbol{0} = (0,0,\ldots,0)$). 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 70. ЛИНЕАРНО УРЕЂЕЊЕ на скупу свих производа је мономни поредак уколико испуњава следећа два услова.

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

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

Став 71. Мономни поредак је ДОБРО УРЕЂЕЊЕ на скупу свих производа.

Доказ. Нека је $\preccurlyeq$ 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 $\preccurlyeq$.

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. Осим тога, за $1 \leqslant j \leqslant k$: $\mathbf{X}_j \nmid \mathbf{X}$, јер би онда било и $\mathbf{X}_j \preccurlyeq \mathbf{X}$, што је супротно чињеници да је $\mathbf{X} \prec \mathbf{X}_i \preccurlyeq \mathbf{X}_j$ (поредак $\preccurlyeq$ 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

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

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, задати лексикографски и степенасти лексикографски поредак да неодређене буду уређене на неки други начин.

Изаберимо неки мономни поредак $\preccurlyeq$. 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. Најпре уводимо 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 користе ћи 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 72. 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

$$\text{за сваки } g \in I \setminus \{0\} \text{ постоји } i \in \{1, \ldots, s\} \text{ тако да } LP(g_i) \mid LP(g). \quad (2)$$

Став 73. 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 и делу доказа става **71**, 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 $\mathcal{LP}(I)$ у односу на релацију дељивости.

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 **72**. 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 $LP(g)$, не смета ништа то). 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 (**2**). Покажимо да они генеришу I. Заправо ћемо показати да је $f \in I$ ако и само ако се помоћу $g_1, \ldots, g_s$ 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. □

Напомена 74. Приметимо да из претходног става следи и последица 48. Дакле, Диксонова лема нам је помогла да директно добијемо овај важан резултат. ♢

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 75. Нека је $G = \{g_1, \ldots, g_s\}$ једна Гребнерова база идеала I прстена $K[X_1, \ldots, X_n]$ и $f \neq 0$ 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 $\preccurlyeq_1$ и посматрамо поредак $\preccurlyeq_2$ и скуп полинома $\{h_1, \ldots, h_s\}$ за које је $LP_{\preccurlyeq_1}(g_i) = LP_{\preccurlyeq_2}(h_i)$ за све i, онда је скуп $\{h_1, \ldots, h_s\}$ Гребнерова база за поредак $\preccurlyeq_2$. 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 76. 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 77. (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 78. 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 $1 \leqslant j \leqslant t$. Како важи: $S(g_i, g_j) \xrightarrow{G}_+ 0$ 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 79. 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 80. 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 $F\backslash\{f_1\}$ и $G\backslash\{g_{i_1}\}$. 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 81. 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 82. 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 $j \neq k$. То значи да имамо 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. Тако бисмо добили 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 нађимо 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 83. 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 84. Нека је $G = \{g_1, \ldots, g_t\}$ Гребнерова база за идеал I. Тада једну базу за K-векторски простор $K[X_1, \ldots, X_n]/_I$ чине косети оних производа $\mathbf{X}$, за које $LP(g_i) \nmid \mathbf{X}$ за све $i \in \{1, \ldots, t\}$.

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. $\square$

Пример 85. 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 $X \succ_{\text{grlex}} Y$. 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: $1 + I, X + I, Y + I, XY + I, Y^2 + I$. $\clubsuit$

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 $N_G(f\cdot g)$. $\diamondsuit$

Пример 86. 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. $\clubsuit$

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 коефицијената. Ако базу чине косети производа $\mathbf{X}_1,\ldots,\mathbf{X}_n$ и тражимо инверз елемента $f+I$, онда тражимо $a_1,\ldots,a_n\in K$ 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. $\diamondsuit$

Пример 87. Искористимо пример **85**. 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

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

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

Једна напреднија примена

Покажимо сада како се Гребнерове базе могу искористити за испитивање да ли се дати граф може обојити са 3 боје.

Подсетимо се најпре да граф $\Gamma = (V, E)$ уређен пар једног коначног скупа V и скупа E који чине неки двочлани подскупови од V (V=vertices, E=edges). Ако је $m \geqslant 2$, онда за граф Γ кажемо да је m-обојив уколико постоји функција $f\colon V \to \{1, \ldots, m\}$ за коју важи: ако је $\{v_1, v_2\} \in E$, онда је $f(v_1) \neq f(v_2)$. Кратко речено, свако теме „бојимо" једном од m боја и суседна темена не смеју бити обојена истом бојом. Ово „кодирамо" помоћу полинома и идеала на следећи начин.

Посматрамо прстен полинома са n неодређених, где је n број елемената у скупу V, са коефицијентима у пољу комплексних бројева: $\mathbb{C}[X_1, \ldots, X_n]$. Идеал I има за генераторе полиноме $X_1^3 - 1, \ldots, X_n^3 - 1$, као и полиноме $X_i^2 + X_i X_j + X_j^2$ за оне $1 \leqslant i < j \leqslant n$ за које је $\{v_i, v_j\} \in E$. Са $V(I)$ означимо скуп свих нула овог идеала, тј.

$$V(I) = \{(z_1, \ldots, z_n) : f(z_1, \ldots, z_n) = 0 \text{ за све } f \in I\}.$$

Наиме, наша идеја је да је $V(I) \neq \emptyset$ акко је граф Γ 3-обојив. Није тешко уверити се зашто је ово тачно. Наиме, уколико је $(z_1, \ldots, z_n) \in V(I)$, онда најпре имамо да је $z_i^3 = 1$ за све i, те је z_i један од ТРИ различита корена из јединице. Та три корена су нам као три боје. А, уколико је $z_i^2 + z_i z_j + z_j^2 = 0$, онда мора бити $z_i \neq z_j$ – у супротном је $z_i^2 + z_i z_j + z_j^2 = 3z_i^2 \neq 0$, јер $z_i \neq 0$, те су темена v_i и v_j обојена различитим бојама.

Дакле, једино што нам недостаје је критеријум за испитивање када је $V(I) \neq \emptyset$. Но, овде „улази у игру" чињеница да су ово полиноми са коефицијентима у $\mathbb{C}$ пошто важи следећа теорема, коју нећемо доказивати.

Теорема 88. Ако је $I \lhd \mathbb{C}[X_1, \ldots, X_n]$ онда је $V(I) = \emptyset$ акко $1 \in I$.

Дакле, све што треба да урадимо је да нађемо редуковану Гребнерову базу G за I и да проверимо да ли $1 \in G$. Нећемо улазити у детаље, али овде треба користити lex поредак.

Пример 89. Нека је $\Gamma = (V, E)$, где је $V = \{v_1, \ldots, v_8\}$ и

$$E = \{\{v_1, v_2\}, \{v_1, v_5\}, \{v_1, v_6\}, \{v_2, v_3\}, \{v_2, v_4\}, \{v_2, v_8\}, \{v_3, v_4\}, \{v_3, v_8\}, \\ \{v_4, v_5\}, \{v_4, v_7\}, \{v_5, v_6\}, \{v_5, v_7\}, \{v_6, v_7\}, \{v_7, v_8\}\}.$$

Ако посматрамо lex поредак за који је $X_1 \succ \cdots \succ X_8$, добијамо редуковану Гребнерову базу

$$G = \{X_1 - X_7, X_2 + X_7 + X_8, X_3 - X_7, X_4 - X_8, \\ X_5 + X_7 + X_8, X_6 - X_8, X_7^2 + X_7X_8 + X_8^2, X_8^3 - 1\}$$

Како $1 \notin G$ закључујемо да је дати граф Γ 3-обојив. Заправо, можемо наћи и како да га обојимо у три боје. Најпре бирамо боју за v_8, јер се X_8 самостално налази у елементу Гребнерове базе. Потом видимо да v_4 мора имати исту боју као и v_8, док v_7 мора бити друге боје. И тако даље. Нацртајте дати граф и обојите га како ова Гребнерова база сугерише. ♣

Напомена 90. У случају да граф има више различитих бојења, Гребнерова база ће бити компликованија и неће нам дати оволико лако начин да то бојење извршимо. ♢

Овим се завршава материјал за други колоквијум.
