Wersja z 17 kwietnia 2007 r.

Bazy Gröbnera

Jerzy Browkin

Bazy Gröbnera są to pewne bazy ideałów pierścienia $k[x_1, \ldots, x_n]$, gdzie k jest ciałem. Takie bazy pozwalają określić dzielenie z resztą w przypadku wielomianów wielu zmiennych, a także rozwiązywać układy równań wielomianowych o wielu niewiadomych.

Bazy Gröbnera zostały wprowadzone przez H. Hironakę w 1964 r. pod nazwą "standard bases" w pracy o usuwaniu osobliwości zbiorów algebraicznych. Bruno Buchberger wprowadził je niezależnie w swojej rozprawie doktorskiej w 1966 r. i nazwał je bazami Gröbnera od nazwiska swojego promotora Wolfganga Gröbnera (1899–1980). Podobne idee można znaleźć dużo wcześniej, na przykład w pracy Paula Gordana z teorii niezmienników z 1900 r.

1. Definicja bazy Gröbnera.

Niech I będzie ideałem pierścienia $k[\mathbf{x}]$, gdzie $\mathbf{x} = (x_1, \ldots, x_n)$ i niech B będzie zbiorem generatorów ideału I. Piszemy wtedy $I = \langle B \rangle$.

Mamy więc

$$I = \{a_1 b_1 + \ldots + a_r b_r \ : r \geq 0, \ \ a_j \in k[\mathbf{x}], \ b_j \in B \text{ dla } 1 \leq j \leq r\}.$$

Każdy zbiór generatorów ideału nazywamy też jego bazą.

W tej sytuacji nie możemy powiedzieć, że B jest lub nie jest bazą Gröbnera ideału I. Musimy sytuację bardziej sprecyzować.

Pierścień $k[\mathbf{x}]$ jest przestrzenią liniową nad ciałem k, jej bazą liniową jest zbiór wszystkich jednomianów $x_1^{a_1} \cdots x_n^{a_n} =: \mathbf{x}^{\mathbf{a}}$, gdzie $\mathbf{a} = (a_1, \ldots, a_n)$ i każde a_j jest nieujemne. Każdy wielomian $f \in k[\mathbf{x}]$ ma więc jednoznaczny zapis w postaci sumy

$$f = \sum_{\mathbf{a}} c_{\mathbf{a}} \mathbf{x}^{\mathbf{a}}, \qquad \text{gdzie} \quad c_{\mathbf{a}} \in k,$$

w której prawie wszystkie współczynniki $c_{\mathbf{a}}$ są równe zeru, zaś $\mathbf{a}$ przebiega elementy zbioru $\mathbb{N}_0^n$, gdzie $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Aby zapisywać składniki wielomianu f (jednomiany $c_{\mathbf{a}}\mathbf{x}^{\mathbf{a}}$) w określonej kolejności, wprowadzimy pewien porządek liniowy $<$ w zbiorze jednomianów $\mathbf{x}^{\mathbf{a}}$, lub, co na jedno wychodzi, w zbiorze $\mathbb{N}_0^n$. Żądamy, aby porządek ten spełniał warunek

$(*)$ Jeżeli $\mathbf{x}^{\mathbf{a}} < \mathbf{x}^{\mathbf{b}}$, to $\mathbf{x}^{\mathbf{a}+\mathbf{c}} < \mathbf{x}^{\mathbf{b}+\mathbf{c}}$ dla każdego $\mathbf{c} \in \mathbb{N}_0^n$.

Żądamy ponadto, aby był to porządek dobry, to znaczy, aby w każdym niepustym zbiorze jednomianów był element najmniejszy w sensie tego porządku.

Przykłady. 1. Porządek leksykograficzny $<_{\text{lex}}$:

$\mathbf{a} <_{\text{lex}} \mathbf{b}$, jeżeli *pierwszy* niezerowy wyraz ciągu $\mathbf{a} - \mathbf{b}$ jest *ujemny*.

Na przykład

$$1 <_{\text{lex}} x_n <_{\text{lex}} \cdots <_{\text{lex}} x_2 <_{\text{lex}} x_1,$$

$$x_2^k <_{\text{lex}} x_1 \qquad \text{dla każdego} \quad k \in \mathbb{N}.$$

Według porządku leksykograficznego są ustawione wyrazy w słowniku. Jeżeli przyjmiemy, że $a < b < c < \cdots < z$, to wyrazy w słowniku są uporządkowane rosnąco.

2. Porządek $<_{\text{grlex}}$ ze względu na stopień, a przy równych stopniach – leksykograficznie (graded lex order) :

Na przykład $1 < x_2 < x_1 < x_2^2 < x_1x_2 < x_1^2$ oraz $x_2^2 < x_1x_3$.

3. Porządek $<_{\text{wt}}$ wyznaczony przez wagę :

Ustalamy liczby rzeczywiste dodatnie $u_1, \ldots, u_n$ liniowo niezależne nad ciałem liczb wymiernych $\mathbb{Q}$. Określamy wagę jednomianu $\text{wt}(\mathbf{x}^{\mathbf{a}}) := a_1u_1 + \ldots + a_nu_n$. Tak więc $\text{wt}(x_j) = u_j$.

Przyjmujemy

$$\mathbf{x}^{\mathbf{a}} <_{\text{wt}} \mathbf{x}^{\mathbf{b}}, \qquad \text{jeżeli} \quad \text{wt}(\mathbf{x}^{\mathbf{a}}) < \text{wt}(\mathbf{x}^{\mathbf{b}}).$$

4. Porządek $<_{\text{grevlex}}$ (graded reverse lex order):

$\mathbf{x}^{\mathbf{a}} <_{\text{grevlex}} \mathbf{x}^{\mathbf{b}}$, jeżeli stopień $\mathbf{x}^{\mathbf{a}}$ jest mniejszy niż stopień $\mathbf{x}^{\mathbf{b}}$, lub stopnie są równe i *ostatni* niezerowy wyraz ciągu $\mathbf{a} - \mathbf{b}$ jest *dodatni*.

Na przykład

$$1 < x_n < \cdots < x_2 < x_1 \qquad \text{oraz} \quad x_1x_3 < x_2^2.$$

5. Porządek $<_{\text{invlex}}$ (inverse lexicographic) :

$\mathbf{a} <_{\text{invlex}} \mathbf{b}$, jeżeli *ostatni* niezerowy wyraz ciągu $\mathbf{a} - \mathbf{b}$ jest *ujemny*.

Na przykład

$$1 < x_1 < x_2 < \cdots < x_n \qquad \text{oraz} \quad x_1^k < x_2 \quad \text{dla każdego} \quad k \in \mathbb{N}.$$

Zadania. 1. Dowieść, że porządki $<_{\text{lex}}$, $<_{\text{grlex}}$ oraz $<_{\text{wt}}$ spełniają warunek $(*)$ i są dobrymi porządkami. Czy porządki $<_{\text{lex}}$ i $<_{\text{grlex}}$ są wyznaczone przez pewne wagi ?

2. Dowieść, że porządek liniowy $<$ spełniający warunek $(*)$ jest dobry wtedy i tylko wtedy, gdy $\mathbf{x}^{\mathbf{a}} > 1$ dla każdego $\mathbf{a} \neq \mathbf{0}$.

3. Dowieść, że liczba różnych porządków jest nieprzeliczalna.

4. Dowieść, że dla $n = 2$ porządki $<_{\text{grlex}}$ oraz $<_{\text{grevlex}}$ są równe.

W dalszym ciągu $<$ będzie ustalonym dobrym porządkiem w zbiorze jednomianów spełniającym warunek $(*)$. Pozwala to ustawić składniki każdego wielomianu w porządku malejącym:

$$f = c_0\mathbf{x}^{\mathbf{a}_0} + c_1\mathbf{x}^{\mathbf{a}_1} + \ldots + c_r\mathbf{x}^{\mathbf{a}_r}, \tag{1}$$

gdzie $c_j \in k^*$, oraz $\mathbf{x}^{\mathbf{a}_0} > \mathbf{x}^{\mathbf{a}_1} > \cdots > \mathbf{x}^{\mathbf{a}_r}$.

Jednomian $c_0\mathbf{x}^{\mathbf{a}_0}$ nazywamy najwyższym wyrazem wielomianu f i oznaczamy przez $\mathrm{LT}(f)$, (LT = leading term). Pozostałe jednomiany $c_j\mathbf{x}^{\mathbf{a}_j},\ j > 0$, nazywamy dalszymi wyrazami wielomianu f. Jeżeli $f = 0$, to symbol $\mathrm{LT}(f)$ nie jest określony.

Stopień wielomianu niezerowego f danego wzorem (1) określamy następująco: $\deg f = \mathbf{a}_0 \in \mathbb{N}_0^n$.

Zadania. 1. Dowieść, że jeżeli $f, g \in k[\mathbf{x}],\ fg \neq 0$, to $\mathrm{LT}(fg) = \mathrm{LT}(f) \cdot \mathrm{LT}(g)$.

2. Dowieść, że dla $fg \neq 0$ mamy albo $\mathrm{LT}(f) \cdot g = \mathrm{LT}(g) \cdot f$, albo

$$\mathrm{LT}\Big(\mathrm{LT}(f) \cdot g - \mathrm{LT}(g) \cdot f\Big) < \mathrm{LT}(f) \cdot \mathrm{LT}(g).$$

3. Udowodnić zwykłe własności stopnia wielomianu:

$$\deg(fg) = \deg f + \deg g,$$

$$\deg(f+g) \leq \max(\deg f, \deg g), \qquad \text{jeżeli} \quad f + g \neq 0,$$

a jeżeli $\deg f \neq \deg g$, to w tym wzorze zachodzi równość.

Potrzebne nam jeszcze będzie twierdzenie Hilberta o bazie.

Twierdzenie 1 (D. Hilbert, 1890)**.** *Każdy ideał I pierścienia wielomianów $k[\mathbf{x}]$ ma skończony zbiór generatorów.*

Dokładniej, w każdym zbiorze generatorów ideału I istnieje taki podzbiór skończony, który generuje I.

Dowód można znaleźć w każdym podręczniku algebry. □

Następne definicje i lematy nie wymagają założenia, że w zbiorze jednomianów $\mathbf{x}^{\mathbf{a}}$ jest określony porządek.

Ideał I pierścienia $k[\mathbf{x}]$ nazywamy jednomianowym, jeżeli ma on bazę złożoną z jednomianów. Na mocy twierdzenia Hilberta ma on bazę złożoną ze skończonej liczby jednomianów $I = \langle \mathbf{x}^{\mathbf{a}_1}, \dots, \mathbf{x}^{\mathbf{a}_r} \rangle$.

Mówimy, że jednomian $\mathbf{x}^{\mathbf{a}}$ jest podzielny przez jednomian $\mathbf{x}^{\mathbf{b}}$, jeżeli istnieje taki jedniomian $\mathbf{x}^{\mathbf{c}}$, że $\mathbf{x}^{\mathbf{a}} = \mathbf{x}^{\mathbf{b}} \cdot \mathbf{x}^{\mathbf{c}}$. Piszemy wtedy $\mathbf{x}^{\mathbf{b}} \,|\, \mathbf{x}^{\mathbf{a}}$. Ta relacja podzielności określa odpowiednią relację podzielności w zbiorze $\mathbb{N}_0^n$. Przyjmujemy mianowicie, że $\mathbf{b}|\mathbf{a}$, jeżeli $\mathbf{x}^{\mathbf{b}} \,|\, \mathbf{x}^{\mathbf{a}}$.

Mamy oczywiście

$$(b_1, \dots, b_n) \,|\, (a_1, \dots, a_n) \quad \Leftrightarrow \quad b_j \le a_j \quad \text{dla} \quad 1 \le j \le n.$$

Relacja podzielności określa częściowy porządek w zbiorze jednomianów i w zbiorze $\mathbb{N}_0^n$. Jeżeli w zbiorze jednomianów jest określony również porządek $<$ spełniający warunek $(*)$, to relacja podzielności jest słabsza niż relacja porządku :

$$\text{Jeżeli} \quad \mathbf{x}^{\mathbf{b}} \,|\, \mathbf{x}^{\mathbf{a}}, \quad \text{to} \quad \mathbf{x}^{\mathbf{b}} \le \mathbf{x}^{\mathbf{a}}.$$

Za pomocą relacji podzielności można określić największy wspólny dzielnik (gcd) i najmniejszą wspólną wielokrotność (lcm) dwóch jednomianów.

Mianowicie, $\gcd(\mathbf{x}^{\mathbf{a}}, \mathbf{x}^{\mathbf{b}}) = \mathbf{x}^{\mathbf{c}}$, jeżeli

$$(i) \quad \mathbf{x}^{\mathbf{c}} \,|\, \mathbf{x}^{\mathbf{a}} \quad \text{i} \quad \mathbf{x}^{\mathbf{c}} \,|\, \mathbf{x}^{\mathbf{b}},$$
$$(ii) \quad \mathbf{x}^{\mathbf{d}} \,|\, \mathbf{x}^{\mathbf{a}} \quad \text{i} \quad \mathbf{x}^{\mathbf{d}} \,|\, \mathbf{x}^{\mathbf{b}} \quad \Rightarrow \quad \mathbf{x}^{\mathbf{d}} \,|\, \mathbf{x}^{\mathbf{c}}.$$

Podobnie określa się najmniejszą wspólną wielokrotność.

Zadania. 1. Udowodnić, że jeżeli $\mathbf{a} = (a_1, \dots, a_n)$, $\mathbf{b} = (b_1, \dots, b_n)$, to

$$\gcd(\mathbf{x}^{\mathbf{a}}, \mathbf{x}^{\mathbf{b}}) = \mathbf{x}^{\mathbf{c}}, \quad \text{gdzie} \quad \mathbf{c} = (\min(a_1, b_1), \dots, \min(a_n, b_n)),$$
$$\operatorname{lcm}(\mathbf{x}^{\mathbf{a}}, \mathbf{x}^{\mathbf{b}}) = \mathbf{x}^{\mathbf{d}}, \quad \text{gdzie} \quad \mathbf{d} = (\max(a_1, b_1), \dots, \max(a_n, b_n)).$$

2. Udowodnić implikacje

$$\mathbf{x}^{\mathbf{a}} \,|\, \mathbf{x}^{\mathbf{b}} \quad \text{i} \quad \mathbf{x}^{\mathbf{b}} \,|\, \mathbf{x}^{\mathbf{c}} \quad \Rightarrow \quad \mathbf{x}^{\mathbf{a}} \,|\, \mathbf{x}^{\mathbf{c}},$$
$$\mathbf{x}^{\mathbf{a}} \,|\, \mathbf{x}^{\mathbf{b}} \quad \text{i} \quad \mathbf{x}^{\mathbf{b}} \,|\, \mathbf{x}^{\mathbf{a}} \quad \Rightarrow \quad \mathbf{x}^{\mathbf{a}} = \mathbf{x}^{\mathbf{b}}.$$

Lemat 1. *Jeżeli wielomian* $f = \sum_j c_j \mathbf{x}^{\mathbf{b}_j}$, *gdzie* $c_j \in k^*$, *należy do ideału jednomianowego* $I = \langle \mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_r} \rangle$, *to każdy jednomian* $\mathbf{x}^{\mathbf{b}_j}$ *występujący w wielomianie* f *jest podzielny przez pewien jednomian* $\mathbf{x}^{\mathbf{a}_i}$.

Dowód wymagający trochę wyobraźni. Z założenia mamy

$$f(\mathbf{x}) = \sum_{m=1}^{r} h_m(\mathbf{x}) \cdot \mathbf{x}^{\mathbf{a}_m},$$

gdzie $h_m(\mathbf{x}) \in k[\mathbf{x}]$ dla $1 \leq m \leq r$. Zatem strona prawa tej równości, po wymnożeniu, jest sumą jednomianów, z których każdy jest podzielny przez pewne $\mathbf{x}^{\mathbf{a}_m}$. Po lewej stronie występuje jednomian $\mathbf{x}^{\mathbf{b}_j}$. Taki jednomian musi więc wystąpić również po stronie prawej, być może wielokrotnie i z różnymi współczynnikami. Biorąc pod uwagę jeden taki składnik po prawej stronie otrzymujemy tezę. □

Wniosek 1. *Jeżeli* I *jest ideałem jednomianowym pierścienia* $k[\mathbf{x}]$, *to bazą przestrzeni liniowej* $k[\mathbf{x}]/I$ *jest zbiór wszystkich jednomianów nie należących do* I.

Dowód. Niech $I = \langle \mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_r} \rangle$. Z lematu 1 wynika, że wielomian należy do I wtedy i tylko wtedy, gdy każdy występujący w nim jednomian jest podzielny przez pewien jednomian $\mathbf{x}^{\mathbf{a}_j}$, $1 \leq j \leq r$. Zatem zbiór wszystkich jednomianów podzielnych przez co najmniej jeden jednomian $\mathbf{x}^{\mathbf{a}_j}$ jest bazą przestrzeni I.

Bazą przestrzeni $k[\mathbf{x}]$ jest zbiór wszystkich jednomianów. Wynika stąd, że bazą przestrzeni $k[\mathbf{x}]/I$ jest zbiór tych jednomianów, które nie należą do I. □

Bazę $\mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_r}$ ideału jednomianowego nazywamy minimalną, jeżeli $\mathbf{x}^{\mathbf{a}_i}$ nie dzieli $\mathbf{x}^{\mathbf{a}_j}$ dla $1 \leq i, j \leq r,\ i \neq j$.

Oczywiście każda baza $\mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_r}$ ideału jednomianowego zawiera bazę minimalną.

Wniosek 2. *Baza minimalna ideału jednomianowego jest tylko jedna z dokładnością do porządku.*

Dowód. Niech $\mathbf{x}^{\mathbf{a}_1}, \ldots, \mathbf{x}^{\mathbf{a}_r}$ oraz $\mathbf{x}^{\mathbf{b}_1}, \ldots, \mathbf{x}^{\mathbf{b}_s}$ będą bazami minimalnymi pewnego ideału jednomianowego. Udowodnimy, że każdy element pierwszej bazy występuje w drugiej bazie i naodwrót.

Weźmy element $\mathbf{x}^{\mathbf{a}_i}$ z pierwszej bazy. Na mocy lematu 1 otrzymujemy $\mathbf{x}^{\mathbf{b}_j} \mid \mathbf{x}^{\mathbf{a}_i}$ dla pewnego j i podobnie $\mathbf{x}^{\mathbf{a}_k} \mid \mathbf{x}^{\mathbf{b}_j}$ dla pewnego k. Zatem $\mathbf{x}^{\mathbf{a}_k} \mid \mathbf{x}^{\mathbf{a}_i}$ i z minimalności pierwszej bazy otrzymujemy, że $k = i$.

Mamy więc $\mathbf{x}^{\mathbf{b}_j} \mid \mathbf{x}^{\mathbf{a}_i}$ oraz $\mathbf{x}^{\mathbf{a}_i} \mid \mathbf{x}^{\mathbf{b}_j}$. Stąd $\mathbf{x}^{\mathbf{a}_i} = \mathbf{x}^{\mathbf{b}_j}$. Oczywiście też elementy każdej z tych baz są różne. □

Niech I będzie ideałem niezerowym pierścienia $k[\mathbf{x}]$ i niech $<$ będzie ustalonym dobrym porządkiem w zbiorze jednomianów spełniającym warunek $(*)$. Określamy ideał

$$\mathrm{LT}(I) := \langle \mathrm{LT}(f) \ : \ f \in I, \ f \neq 0 \rangle.$$

Na mocy twierdzenia Hilberta ma on bazę skończoną:

$$\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r) \rangle, \quad \text{gdzie} \quad g_j \in I, \quad \text{dla} \quad 1 \leq j \leq r.$$

Twierdzenie 2. *Jeżeli I jest ideałem niezerowym pierścienia $k[\mathbf{x}]$ oraz $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r) \rangle$ dla pewnych $g_j \in I$, to $g_1, \ldots, g_r$ jest bazą ideału I.*

Dowód. Oczywiście $\langle g_1, \ldots, g_r \rangle \subset I$. Udowodnimy inkluzję odwrotną.

Przypuśćmy, że istnieje wielomian $f \in I$, który nie należy do $\langle g_1, \ldots, g_r \rangle$. W zbiorze takich wielomianów istnieje wielomian najniższego stopnia, ponieważ porządek w zbiorze jednomianów jest dobry.

Z określenia ideału I wynika, że jest to ideał jednomianowy oraz $\mathrm{LT}(f) \in \mathrm{LT}(I)$. Stąd na mocy lematu 1 jednomian $\mathrm{LT}(f)$ jest podzielny przez jednomian $\mathrm{LT}(g_i)$ dla pewnego i. Mamy więc $\mathrm{LT}(f) = c\mathbf{x}^{\mathbf{b}}\mathrm{LT}(g_i)$, gdzie $c \in k^*, \ \mathbf{b} \in \mathbb{N}_0$.

Ponieważ mnożenie przez jednomian zachowuje porządek składników wielomianu, więc

$$\mathrm{LT}(c\,\mathbf{x}^{\mathbf{b}}\, g_i) = c\,\mathbf{x}^{\mathbf{b}}\,\mathrm{LT}(g_i) = \mathrm{LT}(f).$$

Wobec tego najwyższe wyrazy wielomianów f oraz $c\,\mathbf{x}^{\mathbf{b}}\, g_i$ są równe, a zatem $\deg(f - c\,\mathbf{x}^{\mathbf{b}}\, g_i) < \deg f$. Ponadto $f - c\,\mathbf{x}^{\mathbf{b}}\, g_i \notin \langle g_1, \ldots, g_r \rangle$, ponieważ wielomian f nie należy do ideału $\langle g_1, \ldots, g_r \rangle$, i oczywiście $f - c\,\mathbf{x}^{\mathbf{b}}\, g_i \in I$.

Tak więc wielomian $f - c\,\mathbf{x}^{\mathbf{b}}\, g_i$ ma te same własności co wielomian f i ma niższy od niego stopień. Uzyskana sprzeczność dowodzi, że taki wielomian f nie istnieje. Wynika stąd teza twierdzenia. □

Definicja. Niech I będzie ideałem niezerowym pierścienia $k[\mathbf{x}]$. Skończony zbiór wielomianów $g_1, \ldots, g_r \in I$ nazywamy bazą Gröbnera tego ideału, jeżeli $\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_r) \rangle$.

Powyższe twierdzenie uzasadnia użycie tu wyrazu "baza". Jak stwierdziliśmy wyżej, każdy niezerowy ideał pierścienia $k[\mathbf{x}]$ ma bazę Gröbnera.

Baza Gröbnera ideału nie jest wyznaczona jednoznacznie, ponieważ dołączając do niej dowolny niezerowy element tego ideału otrzymamy znów bazę Gröbnera.

2. Algorytm dzielenia z resztą.

Nadal zakładamy, że w zbiorze jednomianów jest określony dobry porządek spełniający warunek $(*)$.

Mamy skończony ciąg niezerowych wielomianów $F = (f_1, \dots, f_t)$ oraz wielomian $f \in k[\mathbf{x}]$. Określimy następujący algorytm dzielenia f przez F.

Rozważamy równości postaci:

$$f = a_1 f_1 + \ldots + a_t f_t + (r + s), \tag{2}$$

gdzie $a_j, r, s \in k[\mathbf{x}],\ \deg(a_j f_j) \leq \deg f$ dla $1 \leq j \leq t$, $\deg s \leq \deg f,\ \deg r \leq \deg f$.

Sytuacja początkowa: $a_1 = \ldots = a_t = r = 0,\ s = f$.

Sytuacja końcowa: $s = 0$ oraz ($r = 0$ lub żaden jednomian wielomianu r nie jest podzielny przez żaden jednomian $\mathrm{LT}(f_j)$ dla $1 \leq j \leq t$).

Algorytm prowadzący od sytuacji początkowej do końcowej:

1) Jeżeli jednomian $\mathrm{LT}(s)$ jest podzielny przez pewien jednomian $\mathrm{LT}(f_j)$, to bierzemy najmniejsze j o tej własności. Mamy więc $\mathrm{LT}(s) = c\mathbf{x}^{\mathbf{b}} \cdot \mathrm{LT}(f_j)$. Dokonujemy następujących zmian we wzorze (2):

$$a_j := a_j + c\mathbf{x}^{\mathbf{b}},$$

$$s := s - c\mathbf{x}^{\mathbf{b}} \cdot f_j.$$

Pozostałe a_i oraz r nie ulegają zmianie.

Mamy $\deg(s - c\mathbf{x}^{\mathbf{b}} \cdot f_j) = \deg(s - \mathrm{LT}(s)) < \deg s$. Zatem stopień wielomianu s się zmniejszył, lub $s = 0$.

Mamy też $\deg((a_j + c\mathbf{x}^{\mathbf{b}}) \cdot f_j) = \deg(a_j f_j + c\mathbf{x}^{\mathbf{b}} \cdot f_j) \leq \deg f$, ponieważ $\deg(c\mathbf{x}^{\mathbf{b}} \cdot f_j) = \deg s \leq \deg f$.

2) Jeżeli jednomian $\mathrm{LT}(s)$ nie jest podzielny przez żaden jednomian $\mathrm{LT}(f_j)$ dla $1 \leq j \leq t$, to dokonujemy następujących zmian we wzorze (2):

$$s := s - \mathrm{LT}(s),$$

$$r := r + \mathrm{LT}(s).$$

Żadne a_i nie ulega zmianie. Oczywiście stopień wielomianu s się zmniejszył, a wielomiany $a_j f_j$ pozostały bez zmian.

Ponieważ w każdym kroku algorytmu stopień wielomianu s się zmniejsza, więc po skończonej liczbie kroków dojdziemy do sytuacji końcowej.

Udowodniliśmy więc

Lemat 2. *Jeżeli $F = (f_1, \dots, f_t)$ jest skończonym ciągiem wielomianów niezerowych i $f \in k[\mathbf{x}]$, to istnieją takie wielomiany $a_1, \dots, a_t, r$ że*

(i) $f = a_1 f_1 + \ldots + a_t f_f + r$,

(ii) $\deg(a_j f_j) \leq \deg f$ *dla* $1 \leq j \leq t$, $\deg r \leq \deg f$,

(iii) $r = 0$ *lub żaden jednomian wielomianu r nie jest podzielny przez żaden z jednomianów* $\mathrm{LT}(f_j)$, $1 \leq j \leq t$.

Wielomian r otrzymany w wyniku zastosowania tego algorytmu nazywamy resztą z dzielenia wielomianu f przez ciąg wielomianów $F = (f_1, \dots, f_t)$ i oznaczamy przez f^F.

Ten algorytm dzielenia jest niedoskonały z następujących względów:

1) Jeżeli F' jest permutacją ciągu F, to reszty z dzielenia wielomianu f przez F i przez F' mogą być różne.

2) Jeżeli wielomian f należy do ideału $I = \langle f_1, \dots, f_t \rangle$ generowanego przez wyrazy ciągu $F = (f_1, \dots, f_t)$, to reszta z dzielenia f przez F może być różna od zera, choć oczywiście $f \equiv 0 \pmod{I}$.

Zadanie. Znaleźć przykłady ilustrujące 1) i 2).

Udowodnimy, że jeżeli F jest bazą Gröbnera, to dzielenie przez F nie ma tych wad, a nawet ma jeszcze szereg zalet.

Twierdzenie 3. *Jeżeli $F = (f_1, \dots, f_t)$ oraz $F' = (f'_1, , \dots, f'_u)$ są bazami Gröbnera ideału I, to dla każdego wielomianu $f \in k[\mathbf{x}]$ reszty z dzielenia f przez F i przez F' są równe. W szczególności reszta nie ulega zmianie przy permutowaniu wyrazów bazy Gröbnera.*

Ponadto $f \in I$ wtedy i tylko wtedy, gdy reszta z dzielenia f przez F jest równa zeru.

Dowód. Wykonując algorytm dzielenia f przez F i przez F' otrzymujemy równości

$$\begin{aligned} f &= a_1 f_1 + \ldots + a_t f_t + r, \\ f &= a'_1 f'_1 + \ldots + a'_u f'_u + r', \end{aligned} \tag{3}$$

gdzie żaden z jednomianów wielomianu r nie jest podzielny przez żaden z jednomianów $\mathrm{LT}(f_j)$ lub $r = 0$ i podobnie żaden z jednomianów wielomianu r' nie jest podzielny przez żaden z jednomianów $\mathrm{LT}(f'_j)$ lub $r' = 0$.

Odejmując stronami równości (3) otrzymamy, że $r - r' \in I$. Przypuśćmy, że $r \neq r'$. Wtedy jednomian $\mathrm{LT}(r - r')$ występuje w wielomianie r lub w wielomianie r', być może z innym niezerowym współczynnikiem.

Dla ustalenia uwagi przyjmijmy, że jednomian podobny do $\mathrm{LT}(r - r')$ występuje w wielomianie r.

Mamy więc

$$\mathrm{LT}(r - r') \in \mathrm{LT}(I) = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t) \rangle,$$

ponieważ $f_1, \ldots, f_t$ jest bazą Gröbnera ideału I. Ideał $\mathrm{LT}(I)$ jest jednomianowy, a zatem jednomian $\mathrm{LT}(r - r')$ jest podzielny przez pewien jednomian $\mathrm{LT}(f_j)$. Wobec tego pewien jednomian wielomianu r też jest podzielny przez $\mathrm{LT}(f_j)$.

Reszta z dzielenia nie może mieć tej własności. Uzyskana sprzeczność dowodzi, że $r = r'$.

Dla dowodu ostatniej części twierdzenia zauważmy, że jeżeli $f \in I = \langle f_1, \ldots, f_t \rangle$ oraz r jest resztą z dzielenia f przez $F = (f_1, \ldots, f_t)$, to $r \in I$.

Jeżeli $r \neq 0$, to $\mathrm{LT}(r) \in \mathrm{LT}(I) = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t) \rangle$. Zatem jednomian $\mathrm{LT}(r)$ jest podzielny przez pewien jednomian $\mathrm{LT}(f_j)$. Przeczy to określeniu reszty z dzielenia. Zatem $r = 0$. □

3. Warunek Buchbergera.

Podamy warunek równoważny temu, że $F = (f_1, \ldots, f_t)$ jest bazą Gröbnera ideału I generowanego przez F. Warunek ten pozwala rozstrzygnąć w skończonej liczbie kroków, czy dany skończony zbiór generatorów ideału jest jego bazą Gröbnera.

Na mocy określenia zbiór wielomianów $f_1, \ldots, f_t$ jest bazą Gröbnera ideału $I = \langle f_1, \ldots, f_t \rangle$ wtedy i tylko wtedy, gdy $\mathrm{LT}(I) = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t) \rangle$. Z lematu 1 wynika, że ta równość zachodzi wtedy i tylko wtedy, gdy dla każdego $f \in I,\ f \neq 0$, jednomian $\mathrm{LT}(f)$ jest podzielny przez pewien jednomian $\mathrm{LT}(f_j)$.

Jeszcze inny równoważny warunek podaje następujący

Lemat 3. *Niech $I = \langle f_1, \ldots, f_t \rangle$. Jeżeli dla każdego $f \in I$ istnieją takie wielomiany $a_1, \ldots, a_t \in k[\mathbf{x}]$, że*

$$f = a_1 f_1 + \ldots + a_t f_t, \quad \textit{gdzie} \quad \deg(a_j f_j) \leq \deg f \quad \textit{dla} \quad 1 \leq j \leq t, \tag{4}$$

to $f_1, \ldots, f_t$ jest bazą Gröbnera ideału I.

Na odwrót, każda baza Gröbnera ma tę własność.

Dowód. Z (4) wynika, że $\mathrm{LT}(f) = \mathrm{LT}(a_j f_j)$ dla pewnego j. Zatem $\mathrm{LT}(f_j) \,|\, \mathrm{LT}(f)$. Wobec tego, na mocy powyższej uwagi, $f_1, \ldots, f_t$ jest bazą Gröbnera ideału I.

Na odwrót, jeżeli $F = (f_1, \ldots, f_t)$ jest bazą Gröbnera ideału I, to algorytm dzielenia f przez F daje wzór (4). □

Niestety, ten lemat jest mało użyteczny, ponieważ wymaga zbadania wszystkich wielomianów $f \in I$. Będziemy chcieli nieco osłabić warunek (4), dbając jednak o to, aby $f_1, \ldots, f_t$ było nadal bazą Gröbnera.

`Krok 1.`

Przypuśćmy więc, że $I = \langle f_1, \ldots, f_t \rangle$ oraz, że wielomian $f \in I$ ma przedstawienie $f = a_1 f_1 + \ldots + a_t f_f$, które nie spełnia warunku (4). To znaczy $\deg(a_j f_j) > \deg f$ dla pewnego j.

Permutując odpowiednio ciąg $(f_1, \ldots, f_t)$ możemy założyć bez zmniejszenia ogólności, że $\deg(a_1 f_1) > \deg f$, a nawet dokładniej, że

$$\mathbf{w} := \deg(a_1 f_1) = \ldots = \deg(a_m f_m) > \deg(a_j f_j) \quad \text{dla} \quad j > m \quad \text{oraz} \quad \mathbf{w} > \deg f.$$

Niech $\mathrm{LT}(a_j) = c_j \mathbf{x}^{\mathbf{u}_j}$, $\mathrm{LT}(f_j) = d_j \mathbf{x}^{\mathbf{v}_j}$ dla $1 \leq j \leq m$. Wtedy $\mathbf{w} = \mathbf{u}_j + \mathbf{v}_j > \deg f$ dla $1 \leq j \leq m$ i wobec tego

$$c_1 d_1 + \ldots + c_m d_m = 0. \tag{5}$$

Przyjmijmy $g := \mathrm{LT}(a_1) f_1 + \ldots + \mathrm{LT}(a_m) f_m$. Wtedy wielomian

$$(a_1 f_1 + \ldots + a_m f_m) - g = (a_1 - \mathrm{LT}(a_1)) f_1 + \ldots + (a_m - \mathrm{LT}(a_m)) f_m$$

jest sumą składników stopni mniejszych od $\deg(a_1 f_1) = \mathbf{w}$. Wobec tego

$$f = g + \sum_{j=1}^{t} a'_j f_j, \qquad \text{gdzie} \quad \deg(a'_j f_j) < \mathbf{w}.$$

Na mocy przyjętych oznaczeń mamy

$$\begin{aligned} g &= c_1 \mathbf{x}^{\mathbf{u}_1} f_1 + \ldots + c_m \mathbf{x}^{\mathbf{u}_m} f_m = c_1 d_1 \cdot \mathbf{x}^{\mathbf{u}_1} f_1 / d_1 + \ldots + c_m d_m \mathbf{x}^{\mathbf{u}_m} f_m / d_m \\ &= c_1 d_1 \cdot g_1 + \ldots + c_m d_m \cdot g_m, \end{aligned} \tag{6}$$

gdzie $g_j = \mathbf{x}^{\mathbf{u}_j} f_j / d_j$.

Zastosujemy tożsamość Abela:

$$X_1Y_1+\ldots+X_mY_m$$
$$= X_1(Y_1-Y_2)+(X_1+X_2)(Y_2-Y_3)+(X_1+X_2+X_3)(Y_3-Y_4)$$
$$+\ldots+(X_1+X_2+\ldots+X_{m-1})(Y_{m-1}-Y_m)+(X_1+X_2+\ldots+X_m)Y_m.$$

Podstawiając w niej $X_i = c_id_i,\ Y_i = g_i$ na mocy (5) i (6) otrzymamy

$$g = c_1d_1(g_1-g_2)+(c_1d_1+c_2d_2)(g_2-g_3)+\ldots+(c_1d_1+\ldots+c_{m-1}d_{m-1})(g_{m-1}-g_m).$$

Tak więc udowodniliśmy, że jeżeli wielomian $f \in I = \langle f_1, \ldots, f_t\rangle$ ma przedstawienie

$$f = a_1f_1+\ldots+a_tf_t,$$

gdzie $\mathbf{w} = \max\deg(a_jf_j) > \deg f$, to f ma też przedstawienie

$$f = \sum_{1\le i<j\le t} c_{ij}(g_i-g_j)+(a'_1f_1+\ldots+a'_tf_t), \tag{7}$$

gdzie $c_{ij} \in k$ oraz $\max_j \deg(a'_jf_j) < \mathbf{w}$, a wielomiany $g_j = \mathbf{x}^{\mathbf{u}_j} f_j/d_j$ należą do ideału I.

`Krok 2.`

Zasadniczą trudność przedstawiają tu wielomiany $g_i - g_j$. Przyjrzyjmy się im dokładniej.

Przy powyższych oznaczeniach mamy

$$g_j = \mathbf{x}^{\mathbf{u}_j} f_j/d_j = \mathbf{x}^{\mathbf{u}_j+\mathbf{v}_j} f_j/d_j\mathbf{x}^{\mathbf{v}_j} = \mathbf{x}^{\mathbf{W}} f_j/\mathrm{LT}(f_j).$$

Wobec tego

$$g_i - g_j = \mathbf{x}^{\mathbf{W}}\Big(f_i/\mathrm{LT}(f_i) - f_j/\mathrm{LT}(f_j)\Big), \tag{8}$$

gdzie $\mathrm{LT}(f_i) \,|\, \mathbf{x}^{\mathbf{W}}$ oraz $\mathrm{LT}(f_j) \,|\, \mathbf{x}^{\mathbf{W}}$, zatem $\mathrm{lcm}(\deg f_i,\ \deg f_j) \,|\, \mathbf{w}$.

Ogólniej, dla dowolnej pary niezerowych wielomianów $f', f'' \in k[\mathbf{x}]$ określamy wielomian $S(f', f'')$, zwany ich S-wielomianem, albo ich syzygią.

[Wyraz "syzygia" w astronomii oznacza koniunkcję lub opozycję dwóch ciał niebieskich względem Słońca. Na przykład Ziemia i Księżyc tworzą syzygię w czasie nowiu lub pełni Księżyca].

Mianowicie przyjmujemy

$$S(f', f'') = \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(f')} \cdot f' - \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(f'')} \cdot f'',$$

gdzie $\mathbf{a} = \mathrm{lcm}(\deg f', \deg f'')$. Mamy $S(f', f'') \in \langle f', f'' \rangle$ oraz $\deg S(f', f'') < \mathbf{a}$, ponieważ $S(f', f'')$ jest różnicą dwóch wielomianów o tym samym najwyższym wyrazie $x^{\mathbf{a}}$.

Wobec tego z (8) otrzymujemy

$$g_i - g_j = \mathbf{x}^{\mathbf{w}-\mathbf{a}_{ij}} S(f_i, f_j), \qquad \text{gdzie} \quad \mathbf{a}_{ij} = \mathrm{lcm}(\deg f_i, \deg f_j).$$

Stąd

$$\deg(g_i - g_j) = (\mathbf{w} - \mathbf{a}_{ij}) + \deg S(f_i, f_j) < (\mathbf{w} - \mathbf{a}_{ij}) + \mathbf{a}_{ij} = \mathbf{w}.$$

`Krok 3.`

Załóżmy, że jest spełniony

Warunek Buchbergera (dotyczący bazy $F = (f_1, \ldots, f_t)$ ideału I)**.** *Dla dowolnych i, j, gdzie $1 \leq i < j \leq t$, reszta z dzielenia wielomianu $S(f_i, f_j)$ przez F jest równa zeru:*

$$S(f_i, f_j)^F = 0 \qquad \textit{dla} \quad 1 \leq i < j \leq t.$$

Z lematu 3 wyprowadzimy

Lemat 4. *Jeżeli $I = \langle f_1, \ldots, f_t \rangle$ oraz $f \in I$ ma postać*

$$f = a_1 f_1 + \ldots + a_t f_t, \qquad \textit{gdzie} \quad \mathbf{w} := \max_j \deg(a_j f_j) > \deg f$$

oraz ciąg $F = (f_1, \ldots, f_t)$ spełnia warunek Buchbergera, to f ma też postać

$$f = b_1 f_1 + \ldots + b_t f_t, \qquad \textit{gdzie} \quad \max_j \deg(b_j f_j) < \mathbf{w}.$$

Dowód. Jak wiemy, zachodzi wzór (7):

$$f = \sum_{1 \leq i < j \leq t} c_{ij}(g_i - g_j) + \sum_{k=1}^{t} a'_k f_k, \tag{7}$$

gdzie $c_{ij} \in k$ oraz $\max_k \deg(a'_k f_k) < \mathbf{w}$.

Ponadto z założenia mamy $S(f_i, f_j)^F = 0$, a więc na mocy algorytmu dzielenia

$$S(f_i, f_j) = q_1^{(ij)} f_1 + \ldots + q_t^{(ij)} f_t,$$

gdzie

$$\deg(q_k^{(ij)} f_k) \leq \deg S(f_i, f_j) < \operatorname{lcm}(\deg f_i, \deg f_j) = \mathbf{a}_{ij}.$$

Wobec tego

$$g_i - g_j = \mathbf{x}^{\mathbf{w}-\mathbf{a}_{ij}} S(f_i, f_j) = \mathbf{x}^{\mathbf{w}-\mathbf{a}_{ij}} \sum_{k=1}^{t} q_k^{(ij)} f_k,$$

gdzie $\deg\left(\mathbf{x}^{\mathbf{w}-\mathbf{a}_{ij}} q_k^{(ij)} f_k\right) < \deg \mathbf{w}$.

Z (7) otrzymujemy więc

$$f = \sum_{k=1}^{t} \left(\sum_{1 \leq i < j \leq t} c_{ij} \mathbf{x}^{\mathbf{w}-\mathbf{a}_{ij}} q_k^{(ij)} + a'_k \right) f_k =: \sum_{k=1}^{t} b_k f_k$$

i stopień każdego wielomianu

$$b_k = \sum_{1 \leq i < j \leq t} c_{ij} \mathbf{x}^{\mathbf{w}-\mathbf{a}_{ij}} q_k^{(ij)} + a'_k$$

jest mniejszy od $\mathbf{w}$. □

Stosując najpierw wielokrotnie lemat 4 dla zmniejszenia wartości liczby $\mathbf{w} := \max_j \deg(a_j f_j)$, a następnie, po osiągnięciu $\mathbf{w} \leq \deg f$, stosując lemat 3, otrzymujemy

Twierdzenie 4 (Kryterium Buchbergera)**.** *Jeżeli $F = (f_1, \ldots, f_t)$, $I = \langle F \rangle$ i spełniony jest warunek Buchbergera*

$$S(f_i, f_j)^F = 0 \qquad dla \quad 1 \leq i < j \leq t,$$

to F jest bazą Gröbnera ideału I.

Na odwrót, każda baza Gröbnera spełnia warunek Buchbergera.

Dowód. Niech $f \in I$. Jak stwierdziliśmy wyżej, wielokrotne zastosowanie lematu 4 daje przedstawienie

$$f = p_1 f_1 + \ldots + p_t f_t, \qquad \text{gdzie} \quad \max_j \deg(p_j f_j) \leq \deg f.$$

Wobec tego z lematu 3 wynika, że F jest bazą Gröbnera ideału I.

Na odwrót, jeżeli F jest bazą Gröbnera ideału I, to na mocy twierdzenia 3 z $S(f_i, f_j) \in \langle f_i, f_j \rangle \subset I$ wynika, że $S(f_i, f_j)^F = 0$. Spełniony jest więc warunek Buchbergera. □

Przykład. W pierścieniu $k[x_1, x_2]$ rozpatrzmy porządek $<_{\text{grlex}}$ spełniający $x_2 < x_1$. Niech I będzie ideałem generowanym przez zbiór wszystkich wielomianów symetrycznych. Mamy więc $I = \langle x_1 + x_2, x_1x_2 \rangle$.

1) Czy $f_1 = x_1 + x_2,\ f_2 = x_1x_2$ jest bazą Gröbnera ideału I?

Mamy $x_1, x_1x_2 \in \mathrm{LT}(I)$. Ponadto $x_2^2 = x_2(x_1+x_2) - x_1x_2 \in I$. Zatem $x_2^2 \in \mathrm{LT}(I)$.

Jednak $x_2^2 \notin \langle x_1, x_1x_2 \rangle = \langle \mathrm{LT}(f_1), \mathrm{LT}(f_2) \rangle$. Wobec tego f_1, f_2 nie jest bazą Gröbnera ideału I.

2) Czy $f_1 = x_1 + x_2, f_3 = x_2^2$ jest bazą Gröbnera ideału I?

Sprawdzimy, czy $F = (f_1, f_3)$ spełnia warunek Buchbergera. Mamy

$$\mathbf{a} := \mathrm{lcm}(\deg f_1, \deg f_3) = \mathrm{lcm}(\,(1,0),\,(0,2)\,) = (1,2).$$

Wobec tego

$$S(f_1, f_3) = \mathbf{x}^{\mathbf{a}} \left(\frac{f_1}{\mathrm{LT} f_1} - \frac{f_3}{\mathrm{LT} f_3} \right) = x_1x_2^2 \left(\frac{x_1 + x_2}{x_1} - \frac{x_2^2}{x_2^2} \right) = x_2^3.$$

Stosując algorytm dzielenia wielomianu $S(f_1, f_3) = x_2^3$ przez ciąg $F = (f_1, f_3) = (x_1 + x_2, x_2^2)$ otrzymujemy resztę zero, ponieważ $f_3 = x_2^2$ dzieli $S(f_1, f_3) = x_2^3$.

Zatem spełniony jest warunek Buchbergera i na mocy twierdzenia 4 f_1, f_3 jest bazą Gröbnera ideału I.

Wynika stąd, że $\mathrm{LT}(I) = \langle \mathrm{LT}(f_1), \mathrm{LT}(f_3) \rangle = \langle x_1, x_2^2 \rangle$.

Zadania. Niech I będzie ideałem z powyższego przykładu.

1. Znaleźć wszystkie bazy Gröbnera ideału I złożone z dwóch wielomianów.

2. Dla każdego porządku w zbiorze jednomianów opisać ideał $\mathrm{LT}(I)$. Ile jest takich ideałów ?

3. Wskazać skończony zbiór generatorów ideału I, który jest bazą Gröbnera przy każdym porządku w zbiorze generatorów. [Jest to tak zwana uniwersalna baza Gröbnera].

4. Algorytm Buchbergera.

Algorytm ten pozwala uzupełnić dowolny skończony zbiór generatorów ideału do jego bazy Gröbnera.

Mamy ideał I oraz ciąg skończony jego generatorów $F = (f_1, \ldots, f_t)$. Jeżeli $S(f_i, f_j)^F = 0$ dla każdej pary (i, j), gdzie $1 \le i < j \le t$, to, jak wiemy, F jest bazą Gröbnera ideału I.

W przeciwnym razie ustalamy taką parę (i,j), że $S(f_i,f_j)^F \neq 0$ i przyjmujemy $f_{t+1} := S(f_i,f_j)^F$. Ponieważ $S(f_i,f_j) \in I$, więc również reszta $S(f_i,f_j)^F$ z dzielenia $S(f_i,f_j)$ przez F należy do I. Mamy więc $I = \langle f_1,\dots,f_t,f_{t+1}\rangle$.

W następnym kroku algorytmu przyjmujemy $F = (f_1,\dots,f_t,f_{t+1})$ i postępujemy podobnie.

Twierdzenie 5. *Algorytm Buchbergera po skończonej liczbie kroków daje bazę Gröbnera ideału.*

W dowodzie twierdzenia wykorzystamy następujący lemat, który nie zakłada istnienia porządku w zbiorze jednomianów.

Przypomnijmy, że ciąg $\mathbf{b} = (b_1,\dots,b_n) \in \mathbb{N}_0^n$ jest wielokrotnością ciągu $\mathbf{a} = (a_1,\dots,a_n) \in \mathbb{N}_0^n$, jeżeli $a_j \leq b_j$ dla każdego $1 \leq j \leq n$.

Lemat 5. *Każdy ciąg $\mathbf{a}^{(1)}$, $\mathbf{a}^{(2)},\dots$ elementów zbioru $\mathbb{N}_0^n$ spełniający warunek*
(§) *Żaden wyraz ciągu nie jest wielokrotnością żadnego wyrazu wcześniejszego, jest skończony.*

Dowód. Zastosujemy indukcję względem n. Dla $n=1$ mamy $\mathbf{a}^{(j)} = (a_1^{(j)})$. Warunek (§) oznacza w tym przypadku, że ciąg liczb $a_1^{(j)}$ jest malejący. Oczywiście każdy ciąg malejący o wyrazach z $\mathbb{N}_0$ jest skończony.

Z kolei niech $n > 1$ i załóżmy, że lemat zachodzi dla $n-1$. Przypuśćmy, że istnieje ciąg nieskończony $\mathbf{a}^{(j)}$ o wyrazach z $\mathbb{N}_0^n$ spełniający warunek (§).

Zauważmy, że każdy ciąg nieskończony o wyrazach z $\mathbb{N}_0$ zawiera podciąg nieskończony niemalejący. Mianowicie, jeżeli nieskończenie wiele wyrazów tego ciągu jest równych, to te wyrazy tworzą poszukiwany podciąg. W przeciwnym razie jest tylko skończenie wiele wyrazów równych 1, skończenie wiele wyrazów równych 2, itd. Istnieje więc podciąg nieskończony rosnący.

Rozpatrzmy ciąg $a_1^{(j)}$ pierwszych współrzędnych wyrazów ciągu $\mathbf{a}^{(j)}$. Na mocy powyższej uwagi ciąg $a_1^{(j)}$ zawiera podciąg nieskończony niemalejący

$$a_1^{(j_1)} \leq a_1^{(j_2)} \leq \dots \tag{8}$$

Zauważmy, że każdy podciąg ciągu spełniającego warunek (§) też spełnia ten warunek. W szczególności podciąg $(\mathbf{a}^{(j_k)})$ spełnia warunek (§).

Dla $\mathbf{a} \in \mathbb{N}_0^n$ oznaczmy przez $\sigma(\mathbf{a}) \in \mathbb{N}_0^{n-1}$ ciąg powstający z $\mathbf{a}$ przez opuszczenie pierwszej współrzędnej. Ponieważ ciąg $\mathbf{a}^{(j_k)}$ spełnia warunek (§), więc $\mathbf{a}^{(j_k)}$ nie jest

wielokrotnością żadnego $\mathbf{a}^{(j_i)}$ dla $i < k$. Mamy więc

$$\bigwedge_{i<k} \bigvee_{1\le m\le n} a_m^{(j_k)} < a_m^{(j_i)}.$$

Jednak na mocy (8) mamy $a_1^{(j_k)} \ge a_1^{(j_i)}$. Zatem

$$\bigwedge_{i<k} \bigvee_{2\le m\le n} a_m^{(j_k)} < a_m^{(j_i)}.$$

Oznacza to, że ciąg $\sigma(\mathbf{a}^{(j_k)})$ spełnia warunek (§). Jest to ciąg nieskończony o wyrazach z $\mathbb{N}_0^{n-1}$. Przeczy to założeniu indukcyjnemu.

Uzyskana sprzeczność dowodzi tezy lematu. □

Dowód twierdzenia. Ponieważ $f_{t+1} = S(f_i, f_j)^F$ jest niezerową resztą z dzielenia $S(f_i, f_j)$ przez $F = (f_1, \dots, f_t)$, więc z algorytmu dzielenia wynika, że żaden jednomian wielomianu f_{t+1} nie jest podzielny przez żaden z jednomianów $\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_t)$. W szczególności jednomian $\mathrm{LT}(f_{t+1})$ ma tę własność, to znaczy, $\mathrm{LT}(f_{t+1})$ nie jest wielokrotnością żadnego z jednomianów $\mathrm{LT}(f_1), \dots, \mathrm{LT}(f_t)$.

Gdyby algorytm Buchbergera nie zakończył się po skończonej liczbie kroków, to otrzymalibyśmy ciąg nieskończony jednomianów

$$\mathrm{LT}(f_t),\ \mathrm{LT}(f_{t+1}),\ \mathrm{LT}(f_{t+2}),\ \dots,$$

w którym żaden wyraz nie jest wielokrotnością żadnego wyrazu wcześniejszego.

Na mocy lematu 5 jest to niemożliwe. □

5. Baza Gröbnera zredukowana.

Lemat 6. *Niech $f_1, \dots, f_t$ będzie bazą Gröbnera ideału I i niech na przykład $\mathrm{LT}(f_2) \mid \mathrm{LT}(f_1)$. Wtedy $(f_2, \dots, f_t)$ również jest bazą Gröbnera ideału I.*

Dowód. Z założenia wynika, że ideały $\langle \mathrm{LT}(f_1), \dots, \mathrm{LT}(f_t)\rangle$ oraz $\langle \mathrm{LT}(f_2), \dots, \mathrm{LT}(f_t)\rangle$ są równe. Zatem na mocy definicji bazy Gröbnera z twierdzenia 2 otrzymujemy tezę. □

Bazę Gröbnera $(f_1, \dots, f_t)$ ideału I nazywamy minimalną, jeżeli żadne $\mathrm{LT}(f_i)$ nie jest podzielne przez żadne $\mathrm{LT}(f_j)$ dla $j \ne i$ i jeżeli każdy jednomian $\mathrm{LT}(f_i)$ ma współczynnik 1, $\mathrm{LT}(f_i) = \mathbf{x}^{\mathbf{a}_i}$.

Z lematu 6 wynika, że każdą bazę Gröbnera można doprowadzić do postaci minimalnej usuwając odpowiednie wielomiany, a pozostałe mnożąc przez odpowiednie elementy ciała k.

Ideał może mieć kilka różnych minimalnych baz Gröbnera. Dlatego nałożymy na bazy jeszcze jeden warunek:

(α) Żaden wyraz wielomianu f_j nie jest podzielny przez żadne $\mathrm{LT}(f_i)$ dla $i \neq j$.

Bazę Gröbnera minimalną spełniającą warunek (α) nazywamy bazą Gröbnera zredukowaną.

Twierdzenie 6. *Każdy ideał niezerowy I ma dokładnie jedną (z dokładnością do permutacji) bazę Gröbnera zredukowaną.*

Dowód. Istnienie. Niech $f_1, \ldots, f_t$ będzie pewną minimalną bazą Gröbnera ideału I. Wtedy jednomiany $\mathrm{LT}(f_j) = \mathbf{x}^{\mathbf{a}_j}$, $1 \leq j \leq t$, są różne. Możemy przyjąć, że

$$\mathbf{x}^{\mathbf{a}_1} > \mathbf{x}^{\mathbf{a}_2} > \cdots > \mathbf{x}^{\mathbf{a}_t}.$$

Wtedy w wielomianie f_j składniki dalsze (prócz najwyższego) mogą być podzielne przez $\mathbf{x}^{\mathbf{a}_i}$ tylko dla $i > j$. Zastępując f_1 resztą z dzielenia f_1 przez $(f_2, \ldots, f_t)$, następnie f_2 resztą z dzielenia f_2 przez $(f_3, \ldots, f_t)$, itd. otrzymamy bazę Gröbnera zredukowaną ideału I.

Jednoznaczność. Przypuśćmy, że $f_1, \ldots, f_t$ oraz $g_1, \ldots, g_u$ są zredukowanymi bazami Gröbnera ideału I. Wtedy

$$\mathrm{LT}(I) = \langle \mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t) \rangle = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_u) \rangle.$$

Z minimalności tych baz Gröbnera wynika, że $\mathrm{LT}(f_i) \nmid \mathrm{LT}(f_j)$ dla $i \neq j$ i podobnie $\mathrm{LT}(g_i) \nmid \mathrm{LT}(g_j)$ dla $i \neq j$. To znaczy, że bazy $\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t)$ oraz $\mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_u)$ ideału jednomianowego $\mathrm{LT}(I)$ są minimalne.

Z wniosku 2 otrzymujemy więc, że $t = u$ oraz po odpowiedniej permutacji $\mathrm{LT}(f_j) = \mathrm{LT}(g_j)$ dla $1 \leq j \leq t$.

Przypuśćmy, że $f_i \neq g_i$ dla pewnego i. Wtedy jednomian $\mathrm{LT}(f_i - g_i)$ występuje w wielomianie f_i lub g_i z niezerowym współczynnikiem. Na przykład niech jednomian podobny do $\mathrm{LT}(f_i - g_i)$ występuje w wielomianie f_i. Mamy oczywiście $\mathrm{LT}(f_i - g_i) < \mathrm{LT}(f_i)$.

Z drugiej strony jednomian $\mathrm{LT}(f_i - g_i)$ należy do ideału jednomianowego $\mathrm{LT}(I)$, jest więc podzielny przez pewien jednomian z bazy tego ideału:

$$\mathrm{LT}(f_j) \mid \mathrm{LT}(f_i - g_i) \qquad \text{dla pewnego} \quad 1 \leq j \leq t.$$

Zatem $\mathrm{LT}(f_j)$ dzieli pewnien wyraz wielomianu f_i różny od $\mathrm{LT}(f_i)$. Przeczy to definicji zredukowanej bazy Gröbnera.

Uzyskana sprzeczność dowodzi, że $f_j = g_j$ dla $1 \leq j \leq t$. $\square$

6. Modyfikacje algorytmu Buchbergera.

Tak więc z punktu widzenia teorii wszystko jest jasne. Każdy niezerowy ideał pierścienia wielomianów $k[\mathbf{x}]$ ma bazę Gröbnera o dobrych własnościach, a nawet dokładnie jedną zredukowaną bazę Gröbnera. Znamy też algorytm, który pozwala rozszerzyć dowolną bazę ideału do pewnej jego bazy Gröbnera, a następnie tę bazę zredukować.

Natomiast z praktycznego punktu widzenia pewne istotne pytania pozostają otwarte. Na przykład:

1) Czy można tak zmodyfikować algorytm Buchbergera, aby go istotnie uprościć ?
2) Jak wybrać porządek w zbiorze jednomianów, aby baza Gröbnera danego ideału była możliwie prosta ?
3) Jak zależy algorytm Buchbergera od porządku w zbiorze jednomianów ? Jak wybrać porządek, aby dla danego ideału, a nawet jego ustalonej bazy, algorytm Buchbergera był możliwie prosty ?

Już nawet w przypadku wielomianów dwóch lub trzech zmiennych nie widać prostych odpowiedzi na te pytania, choć jest sporo prac na ten temat.

Niech $F = (f_1, \dots, f_t)$. Będziemy pisali $f \to_F 0$, jeżeli istnieje taki układ wielomianów $a_1, \dots, a_t$, że

$$f = a_1 f_1 + \ldots + a_t f_t \qquad \text{oraz} \quad \deg(a_j f_j) \leq \deg f \quad \text{dla} \quad 1 \leq j \leq t.$$

Z własności algorytmu dzielenia wynika implikacja

$$f^F = 0 \qquad \Longrightarrow \qquad f \to_F 0. \tag{9}$$

Implikacja odwrotna nie zachodzi, czego dowodzi następujący

Przykład. W zbiorze jednomianów z $k[x, y]$ rozpatrzmy porządek leksykograficzny, gdzie $x > y$.

Przyjmijmy $F = (xy+1,\ y^2-1)$, $\quad f = xy^2 - x$. Dzieląc f przez F otrzymujemy

$$xy^2 - x = y(xy + 1) - x - y.$$

Zatem resztą z dzielenia jest $f^F = -x - y$.

Mamy też $xy^2 - x = x(y^2 - 1)$, a więc $f \to_F 0$.

Twierdzenie 7. *W kryterium Buchbergera warunek* $S(f_i, f_j)^F = 0$ *można zastąpić przez warunek słabszy* $S(f_i, f_j) \to_F 0$.

Dowód. Z warunku Buchbergera korzystaliśmy tylko w dowodzie lematu 4 i tam z $S(f_i, f_j)^F = 0$ wnosiliśmy, że

$$S(f_i, f_j) = q_1^{(ij)} f_1 + \ldots + q_t^{(ij)} f_t,$$

gdzie $\deg(q_k^{(ij)} f_k) \leq \deg S(f_i, f_j)$ dla $1 \leq k \leq t$.

Na mocy implikacji (9) do wyciągnięcia tego wniosku wystarczyłoby założenie, że $S(f_i, f_j) \to_F 0$.

W dowodzie twierdzenia 4 odwoływaliśmy się tylko do lematu 4. □

Następujący lemat wskazuje, że warunek $S(f_i, f_j) \to_F 0$ czasem łatwiej jest sprawdzać niż warunek $S(f_i, f_j)^F = 0$.

Lemat 7. *Jeżeli* $F = (f_1, \ldots, f_t)$ *i dla pewnych* $i, j,\ i \neq j$, *mamy*

$$\gcd(\mathrm{LT}(f_i),\ \mathrm{LT}(f_j)) = 1,$$

to $S(f_i, f_j) \to_F 0$.

Dowód. Dla upraszczenia zapisu oznaczmy $f = f_i,\ g = f_j$. Ponadto niech

$$f = c\mathbf{x}^{\mathbf{a}} + f',\ g = d\mathbf{x}^{\mathbf{b}} + g', \qquad \text{gdzie} \quad c\mathbf{x}^{\mathbf{a}} = \mathrm{LT}(f), \quad d\mathbf{x}^{\mathbf{b}} = \mathrm{LT}(g).$$

Mamy więc

$$S(f, g) = d\mathbf{x}^{\mathbf{b}} f - c\mathbf{x}^{\mathbf{a}} g = (g - g')f - (f - f')g = f'g - g'f.$$

Jeżeli $f' = 0$ lub $g' = 0$, to teza jest oczywista. Niech więc $f'g' \neq 0$. Mamy

$$\mathrm{LT}(f'g) = d\mathbf{x}^{\mathbf{b}}\mathrm{LT}(f'), \quad \mathrm{LT}(g'f) = c\mathbf{x}^{\mathbf{a}}\mathrm{LT}(g').$$

Przypuśćmy, że $\mathrm{LT}(f'g) = \mathrm{LT}(g'f)$. Wtedy, na mocy założenia

$$\gcd(\mathrm{LT}(f),\ \mathrm{LT}(g)) = \gcd(c\mathbf{x}^{\mathbf{a}}, d\mathbf{x}^{\mathbf{b}}) = 1,$$

wnosimy, że $c\mathbf{x}^{\mathbf{a}} \,|\, \mathrm{LT}(f')$, co nie może mieć miejsca.

Zatem $\mathrm{LT}(f'g) \neq \mathrm{LT}(g'f)$ i stąd

$$\deg S(f, g) = \max(\deg(f'g), \deg(g'f)).$$

Wobec tego $S(f,g) \to_F 0$. $\square$

Niech $F = (f_1, \ldots, f_t)$ oraz $\mathrm{LT}(F) := (\mathrm{LT}(f_1), \ldots, \mathrm{LT}(f_t))$. Określimy moduł syzygii $S(F)$ układu F.

[syzygia ($\sigma\acute{\upsilon}\zeta\upsilon\gamma o\zeta$) – związek małżeński, jarzmo wiążące woły w uprzęży].

Mianowicie

$$S(F) := \{S = (h_1, \ldots, h_t) \in k[\mathbf{x}]^t \ : \ \sum_{j=1}^{t} h_j \mathrm{LT}(f_j) = 0\}.$$

Jest to moduł nad $k[\mathbf{x}]$.

Oznaczając przez $\mathbf{e}_j$ wersor j-tej osi w $k[\mathbf{x}]^t$ możemy zapisać $S = \sum_{j=1}^{t} h_j \mathbf{e}_j$. Tak więc S jest syzygią dla F, jeżeli $S \circ \mathrm{LT}(F) = 0$.

Mówimy, że syzygia $S = (h_1, \ldots, h_t)$ dla F jest jednorodna stopnia $\mathbf{a}$, jeżeli S jest układem jednomianów $S = (c_1\mathbf{x}^{\mathbf{a}_1}, \ldots, c_t\mathbf{x}^{\mathbf{a}_t})$ oraz

$$\deg(h_j f_j) = \mathbf{a} \qquad \text{lub} \quad h_j f_j = 0 \quad \text{dla} \quad 1 \le j \le t.$$

Jeżeli więc $\mathrm{LT}(f_j) = d_j\mathbf{x}^{\mathbf{b}_j}$ dla $1 \le j \le t$ oraz $S = (c_1\mathbf{x}^{\mathbf{a}_1}, \ldots, c_t\mathbf{x}^{\mathbf{a}_t})$, to S jest syzygią jednorodną stopnia $\mathbf{a}$ dla F, jeżeli

$$c_1 d_1 + \ldots + c_t d_t = 0 \qquad \text{oraz} \quad \mathbf{a}_1 + \mathbf{b}_1 = \ldots = \mathbf{a}_t + \mathbf{b}_t = \mathbf{a}.$$

Lemat 8. *Każda syzygia S dla $F = (f_1, \ldots, f_t)$ jest sumą syzygii jednorodnych dla F.*

Dowód wymagający nieco wyobraźni.

Niech $\mathrm{LT}(f_j) = d_j\mathbf{x}^{\mathbf{b}_j}$ dla $1 \le j \le t$ i niech $S = (h_1, \ldots, h_t)$. Mamy więc

$$h_1 d_1 \mathbf{x}^{\mathbf{b}_1} + \ldots + h_t d_t \mathbf{x}^{\mathbf{b}_t} = 0.$$

Każdy wielomian h_j jest sumą jednomianów. Wymnóżmy i zgrupujmy jednomiany ustalonego stopnia $\mathbf{a}$. Ich suma jest równa zeru. Mamy więc

$$c_1\mathbf{x}^{\mathbf{a}-\mathbf{b}_1} \cdot d_1\mathbf{x}^{\mathbf{b}_1} + \ldots + c_t\mathbf{x}^{\mathbf{a}-\mathbf{b}_t} \cdot d_t\mathbf{x}^{\mathbf{b}_t} = 0.$$

Zatem $S_{\mathbf{a}} := (c_1\mathbf{x}^{\mathbf{a}-\mathbf{b}_1}, \ldots, c_t\mathbf{x}^{\mathbf{a}-\mathbf{b}_t})$ jest syzygią jednorodną dla F stopnia $\mathbf{a}$ i oczywiście $S = \sum_{\mathbf{a}} S_{\mathbf{a}}$. $\square$

Przykład. Niech $F = (f_1, \ldots, f_t)$ i niech $\mathbf{x}^{\mathbf{a}} = \mathrm{lcm}(\mathrm{LT}(f_i), \mathrm{LT}(f_j))$ dla pewnych $i \ne j,\ 1 \le i, j \le t$. Wtedy

$$S_{ij} := \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(f_i)}\mathbf{e}_i - \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(f_j)}\mathbf{e}_j$$

jest syzygią dla F. Jest to syzygia jednorodna stopnia $\mathbf{a}$. Mamy też $S(f_i, f_j) = S_{ij} \circ F$.

Lemat 9. *Niech $F = (f_1, \dots, f_t)$, gdzie $t \geq 2$. Wtedy każda syzygia S dla F ma postać*

$$S = \sum_{1 \leq i < j \leq t} u_{ij} S_{ij}, \qquad \text{gdzie} \quad u_{ij} \in k[\mathbf{x}].$$

Dowód. Wystarczy udowodnić lemat dla syzygii jednorodnych. Oczywiście S ma co najmniej dwie niezerowe współrzędne:

$$c_i \mathbf{x}^{\mathbf{a}_i} \quad \text{oraz} \quad c_j \mathbf{x}^{\mathbf{a}_j}, \quad \text{gdzie} \quad c_i, c_j \in k^*, \ i \neq j.$$

Niech $\mathrm{LT}(f_k) = d_k \mathbf{x}^{\mathbf{b}_k}$ dla $1 \leq k \leq t$. Z jednorodności S wynika, że $\mathbf{a}_i + \mathbf{b}_i = \mathbf{a}_j + \mathbf{b}_j =: \mathbf{a}$. Mamy więc

$$\mathbf{x}^{\mathbf{b}} := \mathrm{lcm}(\mathrm{LT}(f_i), \mathrm{LT}(f_j)) = \mathrm{lcm}(\mathbf{x}^{\mathbf{b}_i}, \mathbf{x}^{\mathbf{b}_j}) \,|\, \mathbf{x}^{\mathbf{a}}.$$

Z określenia syzygii S_{ij} wynika, że i-ta współrzędna syzygii

$$S' := S - c_i d_i \mathbf{x}^{\mathbf{b}-\mathbf{a}} S_{ij}$$

jest równa

$$c_i \mathbf{x}^{\mathbf{a}_i} - c_i d_i \mathbf{x}^{\mathbf{b}-\mathbf{a}} \cdot \frac{\mathbf{x}^{\mathbf{a}}}{\mathrm{LT}(f_i)} = c_i \mathbf{x}^{\mathbf{a}_i} - c_i \mathbf{x}^{\mathbf{b}-\mathbf{b}_i} = 0.$$

Ponadto współrzędne o numerach różnych od i oraz j w obu syzygiach S i S' są odpowiednio równe.

Tak więc S' jest syzygią jednorodną dla F i ma mniej niezerowych współrzędnych niż syzygia S. Po skończonej liczbie kroków otrzymamy więc syzygię zerową. Wynika stąd teza lematu. □

Wniosek. *Moduł $S(F)$ syzygii dla F jest skończenie generowany. Jego zbiór generatorów jest zawarty w zbiorze syzygii S_{ij}, gdzie $1 \leq i < j \leq t$.*

Lemat 10. *Niech $F = (f_1, \dots, f_t)$ i niech $\mathcal{S}$ będzie bazą modułu syzygii $S(F)$ zawartą w zbiorze $\{S_{ij} \ : \ 1 \leq i < j \leq t\}$. Jeżeli dla pewnych różnych wskaźników $1 \leq i, j, k \leq t$ zachodzi*

$$\mathrm{LT}(f_k) \mid lcm(\mathrm{LT}(f_i), \mathrm{LT}(f_j)) \tag{10}$$

oraz $S_{ij}, S_{jk}, S_{ik} \in \mathcal{S}$, to $\mathcal{S} \setminus \{S_{ij}\}$ też jest bazą modułu $S(F)$.

Dowód. Niech $\mathbf{x}^{\mathbf{a}_{pq}} := \mathrm{lcm}(\mathrm{LT}(f_p), \mathrm{LT}(f_q))$ dla $1 \leq p, q \leq t, \ p \neq q$.

Mamy więc

$$\mathrm{LT}(f_p) \,|\, \mathbf{x}^{a_{pq}} \quad \text{oraz} \quad \mathrm{LT}(f_q) \,|\, \mathbf{x}^{a_{pq}}. \tag{11}$$

Wobec tego

$$\begin{array}{ll} \mathrm{LT}(f_k) \mid \mathbf{x}^{\mathbf{a}_{ij}} & \text{na mocy (10)}, \\ \mathrm{LT}(f_i) \mid \mathbf{x}^{\mathbf{a}_{ij}} & \text{na mocy (11)}, \\ \mathrm{LT}(f_j) \mid \mathbf{x}^{\mathbf{a}_{ij}} & \text{na mocy (11)}. \end{array}$$

Zatem

$$\begin{aligned} \mathbf{x}^{\mathbf{a}_{ik}} &= \mathrm{lcm}(\mathrm{LT}(f_i), \mathrm{LT}(f_k)) \mid \mathbf{x}^{\mathbf{a}_{ij}} \\ \mathbf{x}^{\mathbf{a}_{jk}} &= \mathrm{lcm}(\mathrm{LT}(f_j), \mathrm{LT}(f_k)) \mid \mathbf{x}^{\mathbf{a}_{ij}} \end{aligned}$$

Z określenia mamy

$$S_{ij} = \frac{\mathbf{x}^{\mathbf{a}_{ij}}}{\mathrm{LT}(f_i)} \cdot \mathbf{e}_i - \frac{\mathbf{x}^{\mathbf{a}_{ij}}}{\mathrm{LT}(f_j)} \cdot \mathbf{e}_j,$$

$$S_{ik} = \frac{\mathbf{x}^{\mathbf{a}_{ik}}}{\mathrm{LT}(f_i)} \cdot \mathbf{e}_i - \frac{\mathbf{x}^{\mathbf{a}_{ik}}}{\mathrm{LT}(f_k)} \cdot \mathbf{e}_k,$$

$$S_{jk} = \frac{\mathbf{x}^{\mathbf{a}_{jk}}}{\mathrm{LT}(f_j)} \cdot \mathbf{e}_j - \frac{\mathbf{x}^{\mathbf{a}_{jk}}}{\mathrm{LT}(f_k)} \cdot \mathbf{e}_k.$$

Jak dowiedliśmy, $\mathbf{x}^{\mathbf{a}_{ik}} \,|\, \mathbf{x}^{\mathbf{a}_{ij}}$, $\mathbf{x}^{\mathbf{a}_{jk}} \,|\, \mathbf{x}^{\mathbf{a}_{ij}}$, więc obliczamy

$$\mathbf{x}^{\mathbf{a}_{ij}-\mathbf{a}_{ik}} S_{ik} - \mathbf{x}^{\mathbf{a}_{ij}-\mathbf{a}_{jk}} S_{jk} = S_{ij}.$$

Wynika stąd teza lematu. □

7. Zastosowania baz Gröbnera.

Podamy najpierw kilka oczywistych zastosowań baz Gröbnera. Niech dana będzie baza Gröbnera $F = (f_1, \ldots, f_t)$ ideału I.

1. *Pytanie*: Czy wielomian f należy do ideału I?
   Odpowiedź: Należy wykonać algorytm dzielenia f przez F. Jeżeli reszta z tego dzielenia f^F jest równa 0, to $f \in I$, i naodwrót.

2. *Pytanie*: Dany jest drugi ideał I' i jego baza Gröbnera $F' = (f'_1, \ldots, f'_s)$. Czy $I = I'$?
   Odpowiedź: Należy obie bazy Gröbnera F i F' zredukować. Jeżeli te bazy zredukowane są równe (z dokładnością do porządku), to $I = I'$, i naodwrót.

Przejdziemy teraz do zastosowania baz Gröbnera do rozwiązywania równań wielomianowych o wielu niewiadomych.

Mamy więc układ równań $f_1 = \ldots = f_t = 0$, gdzie $f_j \in k[\mathbf{x}]$ dla $1 \leq j \leq t$. Jeżeli $I = \langle f_1, \ldots, f_t \rangle$ oraz $f'_1, \ldots, f'_s$ jest inną bazą ideału I, to oczywiście zbiory rozwiązań układów równań

$$f_1 = \ldots = f_t = 0 \qquad \text{oraz} \qquad f'_1 = \ldots = f'_s = 0$$

są równe. Tak więc zbiór rozwiązań danego układu równań nie zależy od wyboru bazy ideału I.

Potrzebne nam jeszcze będzie twierdzenie Hilberta o zerach.

Twierdzenie 8 (D. Hilbert)**.** *Niech $I = \langle f_1, \ldots, f_t \rangle$, gdzie $f_j \in k[\mathbf{x}]$ dla $1 \leq j \leq t$, i niech $\overline{k}$ będzie algebraicznym domknięciem ciała k.*

Jeżeli wielomian $f \in k[\mathbf{x}]$ spełnia warunek:

$$\text{Dla każdego } \mathbf{a} \in \overline{k}^n, \text{ jeżeli } f_j(\mathbf{a}) = 0 \text{ dla } 1 \leq j \leq t, \text{ to } f(\mathbf{a}) = 0,$$

to $f^r \in I$ dla pewnego $r \in \mathbb{N}$.

Inaczej mówiąc, jeżeli wielomian f znika w każdym zerze ideału I należącym do $\overline{k}^n$, to $f^r \in I$ dla pewnego $r \geq 1$.

Dowód można znaleźć w każdym podręczniku geometrii algebraicznej. □

Układ równań $f_1 = \ldots = f_t = 0$, gdzie $f_j \in k[\mathbf{x}]$ dla $1 \leq j \leq t$, nazywamy sprzecznym, jeżeli nie ma on rozwiązań w $\overline{k}^n$.

Z twierdzenia Hilberta o zerach wynika, że układ równań $f_1 = \ldots = f_t = 0$ jest sprzeczny wtedy i tylko wtedy, gdy $1 \in \langle f_1, \ldots, f_t \rangle$.

Lemat 11. *Układ równań $f_1 = \ldots = f_t = 0$ jest sprzeczny wtedy i tylko wtedy, gdy bazą Gröbnera zredukowaną ideału $I = \langle f_1, \ldots, f_t \rangle$ jest* (1).

Dowód. Jak wiemy, układ równań $f_1 = \ldots = f_t = 0$ jest sprzeczny wtedy i tylko wtedy, gdy $I := \langle f_1, \ldots, f_t \rangle = k[\mathbf{x}]$. Bazą tego ideału jest (1). Jest to baza Gröbnera zredukowana. □

Twierdzenie 9. *Jeżeli $F = (f_1, \ldots, f_t)$ jest bazą Gröbnera ideału I pierścienia wielomianów $k[x_1, \ldots, x_n]$ z porządkiem leksykograficznym spełniającym $x_1 > x_2 > \cdots > x_n$, to dla każdego m, $1 \leq m \leq n$ zbiór*

$$F_m := F \cap k[x_{m+1}, \ldots, x_n]$$

jest bazą Gröbnera ideału

$$I_m := I \cap k[x_{m+1}, \ldots, x_n].$$

Dowód. Dokonując odpowiedniej permutacji zbioru F możemy przyjąć, że $F_m = (f_1, \ldots, f_r)$.

Mamy oczywiście $\langle f_1, \ldots, f_r\rangle \subset I_m$. Udowodnimy inkluzję odwrotną. Niech $f \in I_m$. Dzieląc f przez F otrzymamy

$$f = a_1 f_1 + \ldots + a_t f_t + 0,$$

ponieważ F jest bazą Gröbnera ideału I oraz $f \in I$.

Zauważmy, że dla $r < j \leq t$ jednomian $\mathrm{LT}(f_j)$ jest podzielny przez pewne x_i, gdzie $i \leq m$, ponieważ $f_j \notin k[x_{m+1}, \ldots, x_n]$. Zatem żaden jednomian wielomianu f nie jest podzielny przez $\mathrm{LT}(f_j)$. Wobec tego przy wykonywaniu algorytmu dzielenia wielomian f_j nigdy nie był wykorzystany. Wynika stąd, że $a_j = 0$. Tak więc

$$f = a_1 f_1 + \ldots + a_r f_r + 0,$$

czyli $f^{F_m} = 0$.

Udowodniliśmy więc, że $F_m = (f_1, \ldots, f_r)$ jest bazą ideału I_m. Na mocy lematu 3 jest to baza Gröbnera, ponieważ $f^{F_m} = 0$ dla każdego $f \in I_m$. □

Twierdzenie 10. *Układ równań $f_1 = \ldots = f_t = 0$ ma skończoną liczbę rozwiązań w $\overline{k}^n$ wtedy i tylko wtedy, gdy ideał $I = \langle f_1, \ldots, f_t\rangle$ spełnia warunek*

$$\mathrm{LT}(I) = \langle x_1^{k_1}, \ldots, x_n^{k_n}, \ldots\rangle$$

dla pewnych $k_1, \ldots, k_n \in \mathbb{N}_0$.

Dowód. $\Rightarrow$ Niech $\mathbf{a}^{(j)} = (a_1^{(j)}, \ldots, a_n^{(j)})$, $1 \leq j \leq s$ będą wszystkimi rozwiązaniami danego układu równań w $\overline{k}^n$. Ponieważ element $a_i^{(j)}$ jest algebraiczny względem ciała k, więc istnieje taki niezerowy wielomian $h_i^{(j)} \in k[\mathbf{x}]$, że $h_i^{(j)}(a_i^{(j)}) = 0$.

Wtedy wielomian

$$h_i(x_i) := h_i^{(1)}(x_i) \cdots h_i^{(s)}(x_i)$$

znika we wszystkich zerach $\mathbf{a}^{(j)}$, $1 \leq j \leq s$ ideału I.

Z twierdzenia Hilberta o zerach otrzymujemy więc, że $h_i^{r_i} \in I$ dla pewnego $r_i > 0$. Ponieważ h_i jest wielomianem jednej zmiennej x_i, więc $\mathrm{LT}\,(h_i^{r_i}) = c x_i^{k_i}$ dla pewnego $k_i \geq 0$. Stąd $x_i^{k_i} \in \mathrm{LT}(I)$.

$\Leftarrow$ Z założenia wynika, że istnieje wielomian $g_i \in I$ spełniający $\mathrm{LT}(g_i) = x_i^{k_i}$, $1 \leq i \leq n$. Z algorytmu dzielenia dowolnego wielomianu $f \in k[\mathbf{x}]$ przez układ $G := (g_1, \ldots, g_n)$ otrzymujemy taką resztę r, w której żaden jednomian nie jest podzielny przez żadne $\mathrm{LT}(g_i) = x_i^{k_i}$ dla $1 \leq i \leq n$.

Zatem r jest kombinacją liniową jednomianów postaci

$$x_i^{m_1} \cdots x_n^{m_n}, \qquad \text{gdzie} \quad 0 \leq m_i < k_i \quad \text{dla} \quad 1 \leq i \leq n.$$

Takich jednomianów jest $d := k_1 \cdots k_n$. Zatem przestrzeń liniowa $k[\mathbf{x}]/I$ ma wymiar $\leq d$.

Wynika stąd, że zbiór $d+1$ wielomianów $1, x_i, x_i^2, \ldots, x_i^d$ jest liniowo zależny modulo I. To znaczy, że istnieje niezerowy wielomian $h_i \in k[x_i]$ stopnia $\leq d$ spełniający $h_i \in I$.

Zatem i-ta współrzędna dowolnego zera ideału I jest pierwiastkiem wielomianu h_i. Wynika stąd, że liczba zer ideału I w $\overline{k}^n$ nie przekracza d^n. □

Wniosek 4. *Dany jest układ równań $f_1 = \ldots = f_t = 0$. Niech $g_1, \ldots, g_m$ będzie bazą Gröbnera ideału $I = \langle f_1, \ldots, f_t \rangle$.*

Ten układ równań ma skończoną liczbę rozwiązań w $\overline{k}^n$ wtedy i tylko wtedy, gdy

$$\bigwedge_{1 \leq i \leq n} \bigvee_{1 \leq j \leq m} \mathrm{LT}(g_j) = x_i^{r_i} \qquad \textit{dla pewnego} \quad r_i \geq 0.$$

Dowód. Z definicji bazy Gröbnera mamy

$$\mathrm{LT}(I) = \langle \mathrm{LT}(g_1), \ldots, \mathrm{LT}(g_m) \rangle.$$

Teza wniosku wynika więc z twierdzenia 10. □

Wniosek 5. *Jeżeli układ równań $f_1 = \ldots = f_t = 0$ ma skończoną liczbę rozwiązań w $\overline{k}^n$, to istnieje równoważny mu układ $g_1 = \cdots = g_m = 0$ w postaci "trójkątnej", tzn. spełniający $m \geq n$ oraz dla $1 \leq k \leq n$*

$$g_k = x_k^{r_k} + g_k' \qquad \textit{dla pewnego} \quad r_k > 0,$$

gdzie wielomian g_k' nie zawiera zmiennych $x_1, \ldots, x_{k-1}$.

Dowód. Rozpatrzmy dowolny porządek w zbiorze jednomianów spełniający $x_1 > x_2 > \cdots > x_n$. Niech $g_1, \ldots, g_m$ będzie bazą Gröbnera ideału $I = \langle f_1, \ldots, f_t \rangle$.

Dokonując odpowiedniej permutacji tej bazy na mocy wniosku 4 można przyjąć, że $\mathrm{LT}(g_k) = x_k^{r_k}$ dla $1 \leq k \leq n$.

Określając $g_k' = g_k - x_k^{r_k}$ otrzymamy

$$\mathrm{LT}(g_k') < \mathrm{LT}(g_k) = x_k^{r_k} < x_j \qquad \text{dla} \quad 1 \leq j \leq k.$$

Wobec tego wielomian g_k' nie zawiera zmiennych $x_1, \ldots, x_{k-1}$. □

8. Przykłady.

8.1. Twierdzenie Pappusa.

Twierdzenie 11 (Pappus z Aleksandrii, ok. 320 r.n.e.)**.** *Na płaszczyźnie dane są dwie proste L i M i na każdej z nich po trzy punkty*: $A, B, C \in L$ *oraz* $A', B', C' \in M$.

Rozpatrzmy następujące proste $K_j,\ K'_j,\ j = 1, 2, 3$, *wyznaczone przez pary tych punktów*

$$A, B' \in K_1, \qquad A', B \in K'_1,$$

$$B, C' \in K_2, \qquad B', C \in K'_2,$$

$$C, A' \in K_3, \qquad C', A \in K'_3.$$

Rozważmy punkty przecięcia odpowiednich par prostych:

$$P \in K_1 \cap K'_1, \quad Q \in K_2 \cap K'_2, \quad R \in K_3 \cap K'_3.$$

Wtedy punkty P, Q, R są współliniowe.

[Czytelnik zechce wykonać odpowiedni rysunek].

Dowód. Oznaczmy przez $x_1, \ldots, x_{18}$ współrzędne dziewięciu rozważanych punktów

$$A, B, C; \quad A', B', C'; \quad P, Q, R.$$

W założeniu mamy, że na każdej z ośmiu prostych

$$L,\ M,\ K_1, K'_1,\ K_2, K'_2,\ K_3, K'_3$$

są po trzy dane punkty.

Warunek współliniowości trzech punktów

$$T = (t_1, t_2), \quad U = (u_1, u_2), \quad W = (w_1, w_2)$$

ma postać

$$f(T, U, W) := \det \begin{pmatrix} 1 & t_1 & t_2 \\ 1 & u_1 & u_2 \\ 1 & w_1 & w_2 \end{pmatrix} = 0.$$

Zatem założenia twierdzenia Pappusa można zapisać jako układ ośmiu równań kwadratowych o niewiadomych $x_1, \ldots, x_{18}$:

$$f(A, B, C) = 0, \quad f(A', B', C') = 0, \quad f(A, B', P) = 0, \quad f(A', B, P) = 0,$$

$$f(B,C',Q)=0,\quad f(B',C,Q)=0,\quad f(A,C',R)=0,\quad f(A',C,R)=0.$$

Natomiast teza ma postać $f(P,Q,R)=0$.

Przypuśćmy, że teza nie zachodzi. Można to zapisać wprowadzając jeszcze jedną niewiadomą x_{19} następująco: $x_{19}\,f(P,Q,R)-1=0$.

Dla dowodu twierdzenia wystarczy wykazać, że układ złożony z ośmiu początkowych równań i ostatniego równania jest sprzeczny. W tym celu wystarczy stwierdzić, że zredukowana baza Gröbnera ideału generowanego przez wielomiany występujące po lewych stronach tych dziewięciu równań jest równa (1).

Tę bazę znajduje komputer, jest to łatwe ćwiczenie. □

8.2. Twierdzenie Erdősa.

Niech $f\in k[x]$ spełnia $f(0)\neq 0$, gdzie k jest ciałem charakterystyki 0. Pytamy, czy wielomian f^2 może mieć "dużo mniej" niezerowych współczynników niż wielomian f?

Dokładniej, niech $nz(g)$ będzie liczbą niezerowych współczynników wielomianu g i niech dla $N=1,2,\ldots$

$$Q(N):=\min\{nz(f^2)\ :\ nz(f)=N\}.$$

W 1949 r, P. Erdős udowodnił, że istnieją stałe dodatnie C_1,C_2 spełniające

$$Q(N)<C_1\,N^{1-C_2}\qquad\text{dla każdego}\quad N\geq 1.$$

Zatem

$$\inf_f\big(nz(f^2)/nz(f)\big)=0.$$

Można rozpatrywać analogiczne pytanie dla wielomianów o wszystkich współczynnikach niezerowych. Niech więc

$$\mathbb{Q}'(N):=\min\{nz(f^2)\ :\ nz(f)=\deg f+1,\ \deg f=N\}.$$

Również w 1949 r. W. Verdenius udowodnił, że istnieje liczba dodatnia C spełniająca

$$Q'(N)\leq C\,N^{0.81072}\qquad\text{dla każdego}\quad N\geq 1.$$

Badano też liczby $Q'(N)$ dla małych wartości N. Podano przykłady wielomianów, z których wynikają następujące oszacowania:

A. Renyi (1947): $Q'(28) < 28$.

R. Freud (1973); A. Choudry (1988) : $Q'(17) < 17$.

D. Coppersmith, J. Davenport (Acta Arithmetica 58 (1991), 79–87) : $Q'(12) \leq 12$. Podali oni mianowicie następujący wielomian stopnia 12 o niezerowych współczynnikach

$$P_{12}(x) := (1 + 2x - 2x^2 + 4x^3 - 10x^4 + 50x^5 + 125x^6)(1 - 110x^6),$$

którego kwadrat ma tylko 12 niezerowych współczynników.

W pracy tej używając baz Gröbnera udowodniono też, że $Q'(d) > d$ dla $d \leq 7$.

Objaśnimy to na przykładzie wielomianów stopnia 3.

Niech więc wielomian

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3$$

ma wszystkie współczynniki różne od zera. Bez zmniejszenia ogólności można przyjąć, że $a_0 = a_3 = 1$. Wtedy

$$f^2(x) = 1 + 2a_1x + (2a_2 + a_1^2)x^2 + 2(1 + a_1a_2)x^3 + (2a_1 + a_2^2)x^4 + 2a_2x^5 + x^6.$$

Chcemy udowodnić, że wielomian f^2 ma co najwyżej dwa współczynniki równe zeru. Mogą to być jedynie współczynniki przy x^2, x^3 i x^4.

Przypuśćmy, że wszystkie te współczynniki znikają. Prowadzi to do układu równań (o niewiadomych a_1, a_2, b_1, b_2) :

$$2a_2 + a_1^2 = 0, \quad 1 + a_1a_2 = 0, \quad 2a_1 + a_2^2 = 0, \quad a_1b_1 - 1 = 0, \quad a_2b_2 - 1 = 0.$$

Znajdując zredukowaną bazę Gröbnera ideału generowanego przez wielomiany występujące po lewych stronach tych równań otrzymujemy (1). Zatem układ równań jest sprzeczny. Wynika stąd, że $Q'(3) \geq 5$.

Copperfield i Davenport udowodnili w ten sposób, że $Q'(d) > d$ dla $d \leq 7$. Problem, czy $Q'(d) > d$ również dla $d = 8, 9, 10, 11$ pozostaje otwarty. Stosując bazy Gröbnera można go oczywiście rozstrzygnąć, choć może to wymagać rozpatrzenia dużej liczby układów równań.

Dygresja. Analogiczne pytanie można sformułować też dla liczb naturalnych zapisanych na przykład w układzie dziesiętnym. Rozpatrujemy liczby naturalne m

niepodzielne przez 10. Niech $nz(m)$ będzie liczbą cyfr liczby m różnych od zera. Określamy analogicznie

$$Q(N) := \min\{nz(m^2) \ : \ nz(m) = N\}$$

$$Q'(N) := \{nz(m^2) \ : \ m \quad \text{ma } N+1 \text{ cyfr i wśrod nich nie występuje } 0\}.$$

Nie znam żadnych nietrywialnych oszacowań liczb $Q(N)$ i $Q'(N)$, choć nietrudno znajdować przykłady liczb naturalnych niepodzielnych przez 10, których kwadraty mają dużo zer.

Na przykład

$$\begin{aligned} 32^2 &= 1024, \\ 317^2 &= 100489, \\ 3163^2 &= 10004569. \end{aligned}$$

Rekordowy znany mi wynik jest następujący. Liczba

$$m = 4472135954999579392819$$

ma 22 cyfry, a liczba m^2 ma 44 cyfry, z których 26 jest równych 0.

Zatem $Q(22) \leq 18, \ Q'(21) \leq 18.$

Tutaj nie widać, jak zastosować bazy Gröbnera, ponieważ cyfry liczby m^2 nie są wielomianami od cyfr liczby m.

Nie wiadomo, czy dla liczb naturalnych zachodzą twierdzenia analogiczne do twierdzeń Erdősa i Verdeniusa.